paloalto
TECHDOCS

Strata Cloud Manager – AIOps

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

February 3, 2025

Table of Contents

AIOps for NGFW

Basierend auf Daten, die durch die PAN-OS-Gerätetelemetrie gesammelt wurden, gibt Ihnen AIOps for NGFW einen Überblick über den Zustand und die Sicherheit Ihrer Firewall-Bereitstellung der nächsten Generation (Next Generation Firewall, NGFW), um Ihnen dabei zu helfen, Bereiche für Verbesserungen zu erkennen und Sicherheitslücken zu schließen. AIOps for NGFW leitet Zustandsinformationen aus Gerätetelemetriemetriken ab, die sich auf den Betriebsstatus Ihrer Geräte beziehen. Für Sicherheitsinformationen analysiert AIOps for NGFW die Konfiguration Ihrer Geräte anhand der Best Practices von Palo Alto Networks, um mögliche Lücken in Ihrem Sicherheitsstatus aufzuzeigen.

AIOps für NGFW Premium und Strata Cloud Manager

Strata Cloud Manager *bietet einheitliche Verwaltung und Betrieb ausschließlich für NGFWs, die die AIOps-Lizenz für NGFW Premium verwenden.*

- ***NGFWs (PAN-OS und von Panorama verwaltet)*** → *Verwenden Sie für PAN-OS- und von Panorama verwaltete NGFWs mit einer AIOps für NGFW Premium-Lizenz Strata Cloud Manager, um die Integrität und den Sicherheitsstatus Ihrer Bereitstellung zu überwachen.*
- ***NGFWs (von der Cloud verwaltet)*** → *Mit einer AIOps für NGFW-Lizenz können Sie Strata Cloud Manager auch zur* Cloud-Verwaltung für NGFWs *verwenden.*

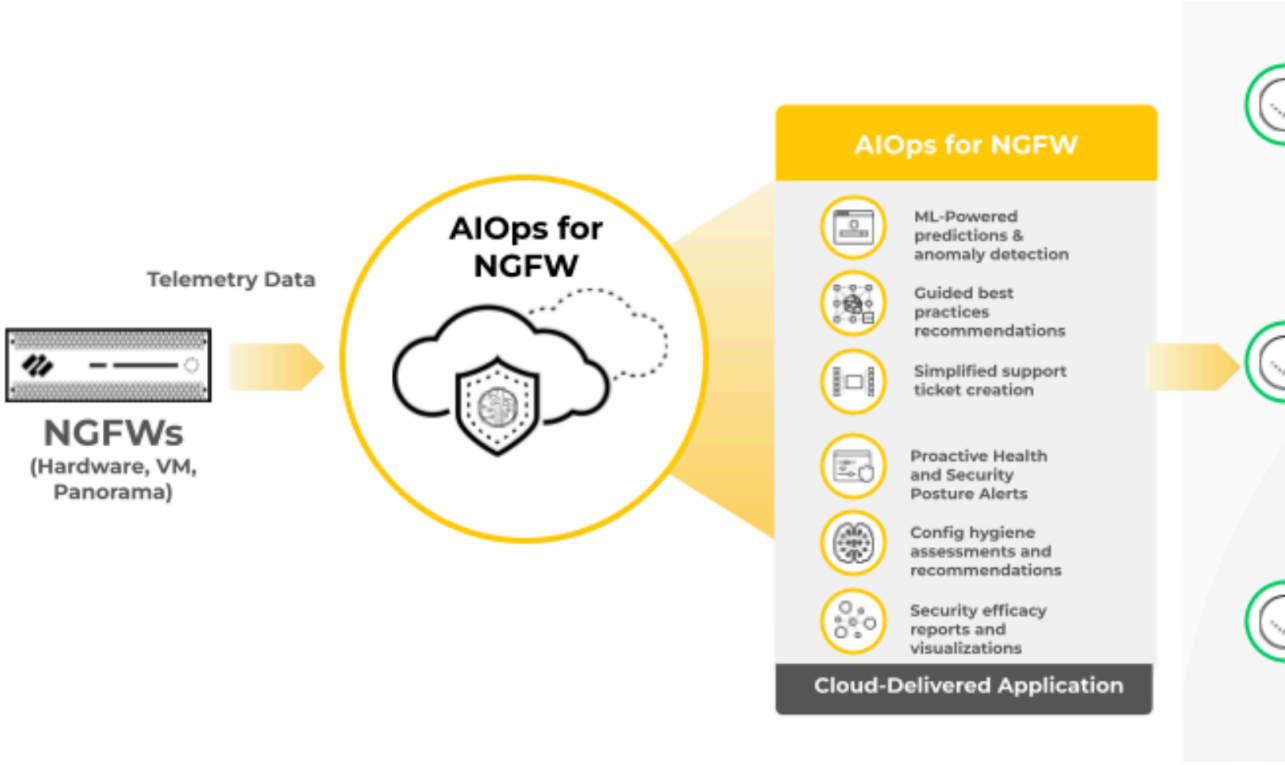
Seit Oktober 2024 gibt es für Strata Cloud Manager zwei Lizenzstufen: Strata Cloud Manager Essentials und Strata Cloud Manager Pro. Diese vereinheitlichte Struktur sorgt für eine optimierte Bereitstellung von Netzwerksicherheitsangeboten, einschließlich AIOps für NGFW, Autonomous Digital Experience Management (ADEM), Cloud-Verwaltungsfunktionalität und Strata-Protokollierungsdienst. Siehe Strata Cloud Manager-Lizenz*.*

Wenn Sie bereits die kostenlose App ***AIOps für NGFW Free*** *oder Strata Cloud Manager mit einer* ***AIOps für NGFW Premium****-Lizenz verwenden, sind Ihre vorhandenen Lizenzen davon nicht betroffen und Sie können diese weiterhin ändern, verlängern oder erneuern.*

Erste Schritte:

- AIOps für NGFW – Free und Premium
- Aktivieren Sie AIOps für NGFW
- Beginnen Sie mit dem Senden von Gerätetelemetriedaten an AIOps für NGFW
- Neue Eigenschaften

- On-Demand-BPA-Bericht
- AIOps für NGFW – Vorfälle und Benachrichtigungen



Regionen für AIOps für NGFW

Wo kann ich das verwenden?	Was brauche ich?
• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ☐ AIOps for NGFW Free oder Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro

Die Region, die Sie beim Aktivieren von AIOps for NGFW auswählen, bestimmt den physischen Standort, an dem AIOps Ihre Daten verarbeitet.

AIOps for NGFW ist nicht in allen Regionen verfügbar, in denen die Strata Logging Service-(SLS-)Infrastruktur unterstützt wird. Die AIOps for NGFW-Bereitstellung wird bald auf zusätzliche Regionen ausgeweitet, um den Zielen der Telemetriedaten zu entsprechen. Wenn Sie Ihre Telemetriedaten derzeit in eine Region senden, in der die AIOps-Anwendung nicht unterstützt wird, werden Ihre Daten von einer AIOps for NGFW-Instanz in der Region „Vereinigte Staaten – Amerika“ verarbeitet.

Wenn Sie AIOps for NGFW aktivieren, werden diese Einschränkungen automatisch angewendet. Wenn Sie beispielsweise Deutschland als Region auswählen, in der eine Instanz von AIOps for NGFW aktiviert werden soll, können dieser Instanz nur in Deutschland ansässige SLS-Mandanten zugeordnet werden.

Regionen, die AIOps für NGFW unterstützen, unterstützen auch NGFWs in Strata Cloud Manager.

Informationen zur AIOps-Datenverarbeitung für die verschiedenen Telemetriezielregionen finden Sie in der folgenden Tabelle.

Region für den Strata Logging Service	Unterstützte Region für eine AIOps for NGFW-Instanz zur Datenverarbeitung
Deutschland	Deutschland
Vereinigtes Königreich	Vereinigtes Königreich
Niederlande – Europa	Niederlande – Europa
Italien – Europa	Italien – Europa
Spanien – Europa	Spanien – Europa
Schweiz – Europa	Schweiz – Europa

Region für den Strata Logging Service	Unterstützte Region für eine AIOps for NGFW-Instanz zur Datenverarbeitung
Frankreich – Europa	Frankreich – Europa
Polen – Europa	Polen – Europa
Korea	Korea
Indonesien	Indonesien
Israel	Israel
Taiwan	Taiwan
Katar	Katar
Singapur	Singapur
Australien	Australien
Indien	Indien
Japan	Japan
Kanada	Kanada
Verbleibende SLS-Regionen	Vereinigte Staaten – Amerika

Free- und Premium-Funktionen

Wo kann ich das verwenden?	Was brauche ich?
• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ☐ AIOps for NGFW Free oder Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro

AIOps für NGFW ist mit zwei Lizenzstufen verfügbar: Free und Premium.

Mithilfe der AIOps for NGFW Free-Funktionen können Sie sich mit Ihrer Firewall-Implementierung besser vertraut machen.

Free-Funktionen:

- Bewertung der Firewall-Konfiguration und Bestimmen von Bereichen mit Verbesserungspotenzial
- Einfacher Zugriff auf Laufzeit- und historische Telemetriedaten von Firewalls
- Erkennen von Systemproblemen (unabhängig von der Erkennungsmethode)
- Schnellere Problemlösung durch Alarm-/Benachrichtigungs-Workflows
- Bereitstellen dynamischer Dashboards und Visualisierungen für mehrere Sicherheitsabonnements

Mit einer Premium-Lizenz haben Sie Zugriff auf kostenlose (Free) und Premium-Funktionen. Die Premium-Funktionen konzentrieren sich darauf, ein optimales Nutzungs- und Sicherheitsergebnis für ihre Firewalls zu gewährleisten.

Premium-Funktionen:

- Cloud-Verwaltung für NGFWs

  Wenden Sie sich an Ihr Account-Team, um Cloud-Verwaltung für NGFWs mithilfe von Strata Cloud Manager zu aktivieren.
- Verwenden fortschrittlicher ML-Techniken, um einen stets optimalen Sicherheitsstatus zu fördern, der auf die sich ändernden Bedrohungs- und Netzwerklandschaften reagiert und so die Angriffsfläche reduziert
- Bereitstellen dynamischer Dashboards und Visualisierungen für WildFire und IOC-Suche
- Interaktion mit Daten und Visualisierung der Beziehungen zwischen Ereignissen im Netzwerk im Strata Cloud Manager Command Center, um Anomalien aufzudecken oder Möglichkeiten zur Verbesserung Ihrer Netzwerksicherheit zu finden

Für Strata Cloud Manager gibt es zwei Lizenzstufen: Strata Cloud Manager Essentials und Strata Cloud Manager Pro. Diese vereinheitlichte Struktur sorgt für eine optimierte Bereitstellung von Netzwerksicherheitsangeboten, einschließlich AIOps für NGFW, Autonomous Digital Experience Management (ADEM), Cloud-Verwaltungsfunktionalität und Strata-Protokollierungsdienst. Siehe Strata Cloud Manager-Lizenz.

*Wenn Sie bereits die kostenlose App **AIOps für NGFW Free** oder Strata Cloud Manager mit einer **AIOps für NGFW Premium**-Lizenz verwenden, sind Ihre vorhandenen Lizenzen davon nicht betroffen und Sie können diese weiterhin ändern, verlängern oder erneuern.*

Funktionsumfang	Free	Premium (Verwendung von Strata Cloud Manager)
Stärkung des Sicherheitsstatus	**Teilweise**	**Ja**
• Einblicke in den Sicherheitsstatus	Ja	Ja
• Funktionsannahme	Ja	Ja
• Einstellungen für den Sicherheitsstatus	Nein	Ja
• Empfehlungen zum Software-Upgrade	Nein	Ja
• Einführung von CDSS	Ja	Ja
• Richtlinienanalyse	Nein	Ja
• On-Demand-BPA-Bericht	Ja	Ja
• Panorama CloudConnector-Plug-in	Nein	Ja
• Kapazitätsanalyse	Nein	Ja
• Dashboard „NGFW-SDWAN“	Nein	Ja
• Dashboard „Zusammenfassung der Konformität“	Nein	Ja
Proaktives Beheben von Firewall-Störungen	**Teilweise**	**Ja**
• Benachrichtigungen und Vorfälle	Teilweise	Ja
• Dashboard „PAN-OS-CVEs“	Ja	Ja
• Analyse der wahrscheinlichen Ursache für Benachrichtigungen	Nein	Ja

Funktionsumfang	Free	Premium (Verwendung von Strata Cloud Manager)
Fehlerbehebung mit Protokollen	**Ja**	**Ja**
• Anzeigen, Abfragen und Exportieren von Protokollen im Protokoll-Viewer Prüfen Sie *Lizenzen und andere Anforderungen für die Verwendung des Protokoll-Viewers.*	Ja	Ja
• Exportieren von Metadaten zur Fehlerbehebung	Ja	Ja
• Anzeigen des Auditierungslogs	Ja	Ja
Optimieren Ihrer Sicherheitsinvestition	**Teilweise**	**Ja**
• Geräte-Ranking auf der Grundlage des Zustands und des Sicherheitsstatus	Ja	Ja
• Alle Dashboards und Berichte außer dem Dashboard „Bedrohungseinblicke“	Ja	Ja
• Dashboard „Bedrohungseinblicke“ und Bericht	Nein	Ja
• Suchen nach Sicherheitsartefakten	Nein	Ja
• Erstellen eines benutzerdefinierten Dashboards	Nein	Ja
• Strata Cloud Manager Command Center	Nein	Ja
Benachrichtigungen	**Teilweise**	**Ja**
• E-Mail-Benachrichtigungen	Ja	Ja
• ServiceNow-Integration	Nein	Ja
Engagement und Unterstützung	**Nein**	**Ja**

Funktionsumfang	Free	Premium (Verwendung von Strata Cloud Manager)
• Für die Erstellung von produktinternen Support-Tickets bei Betriebsproblemen *ist Platinum Tier Support auf der Firewall erforderlich (gilt nicht für Benachrichtigungen zu Stromversorgungsausfällen)*	Nein	Ja

Neue Funktionen im Produkt in allen Funktionskategorien werden den Lizenzstufen „Free“ und „Premium“ ausschließlich nach Ermessen von Palo Alto Networks zugewiesen.

So aktivieren Sie AIOps für NGFW

Wo kann ich das verwenden?	Was brauche ich?
• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ☐ AIOps for NGFW Free oder Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro

Im Folgenden sind die verschiedenen Szenarien für die Aktivierung von AIOps for NGFW aufgeführt:

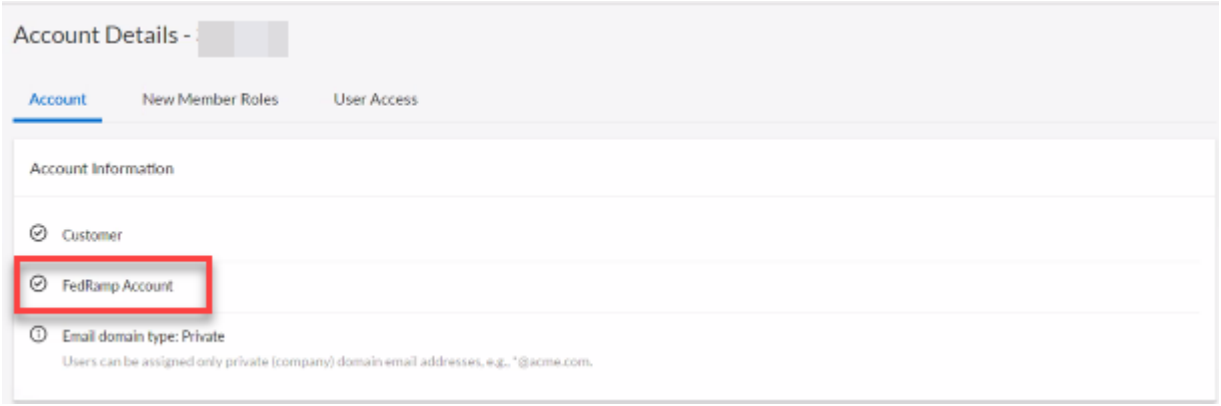
Szenario	Planen
Aktivieren von AIOps for NGFW Free	Aktivieren von AIOps for NGFW (Free)
Aktivieren von AIOps for NGFW Premium (Verwenden der Strata Cloud Manager-App)	Aktivieren von AIOps für NGFW über gemeinsame Dienste
Einbinden neuer Geräte in die aktivierte AIOps for NGFW Free-Instanz	Zuordnen von Geräten zu einem Mandanten Aktivieren von Telemetrie auf Geräten
Einbinden neuer Geräte in die aktivierte AIOps for NGFW Premium-Instanz (Verwenden der Strata Cloud Manager-App)	Zuordnen von Geräten zu einem Mandanten Zuordnen von Geräten im Mandanten zur App Aktivieren von Telemetrie auf Geräten
Aktivieren von ELA AIOps for NGFW Premium	Aktivieren von Enterprise License Agreement (ELA) AIOps für NGFW Premium
Verwenden von Strata Cloud Manager (AIOps für NGFW Premium) zur Verwaltung von VM-Series	Aktivieren einer Lizenzvereinbarung für Software NGFW Credits
Verwenden von Strata Cloud Manager (AIOps für NGFW Premium) für die von Panorama verwaltete VM-Series	Aktivieren einer Software NGFW Credits-Lizenz für die von Panorama verwaltete VM-Series
Umwandeln der AIOps für NGFW Premium-Testlizenz in eine Produktionslizenz	Umwandeln einer Testlizenz in eine Produktionslizenz
Aktivieren von Strata Cloud Manager Essentials und Strata Cloud Manager Pro	• Aktivieren von Strata Cloud Manager Essentials

Szenario	Planen
Strata Cloud Manager Essentials und Strata Cloud Manager Pro können in Konten des Customer Support Portal (CSP) aktiviert werden, wenn in diesen Folgendes nicht verfügbar ist: Strata-Protokollierungsdienst mit dimensioniertem Speicher, AIOps für NGFW Free bzw. Premium oder Prisma Access.	• Aktivieren von Strata Cloud Manager Pro

Strata Cloud Manager bietet einheitliche Verwaltung und Betrieb ausschließlich für NGFWs, die die AIOps-Lizenz für NGFW Premium verwenden. Verwenden Sie weiterhin die AIOps für NGFW Free-App für die in AIOps für NGFW Free eingebundenen NGFWs.

Strata Cloud Manager ist verfügbar und bietet zwei Lizenzstufen: Strata Cloud Manager Essentials und Strata Cloud Manager Pro. Diese vereinheitlichte Struktur sorgt für eine optimierte Bereitstellung von Netzwerksicherheitsangeboten, einschließlich AIOps für NGFW, Autonomous Digital Experience Management (ADEM), Cloud-Verwaltungsfunktionalität und Strata-Protokollierungsdienst. Wenn Sie Strata Cloud Manager vor der Einführung dieser neuen Lizenzstufen verwendet haben, werden Ihre vorhandenen Lizenzen für AIOps für NGFW Premium und AIOps für NGFW Free weiterhin unterstützt. Sie können diese Lizenzen weiterhin ändern, verlängern oder erneuern.

*FedRAMP-Konten können AIOps for NGFW nicht verwenden. Um zu überprüfen, ob dies auf Sie zutrifft, melden Sie sich bei Ihrem Konto beim Customer Support Portal an und wählen Sie **Kontoverwaltung** > **Kontodetails** aus. Wenn in der Liste ein **FedRamp-Konto** enthalten ist, können Sie AIOps for NGFW nicht verwenden.*



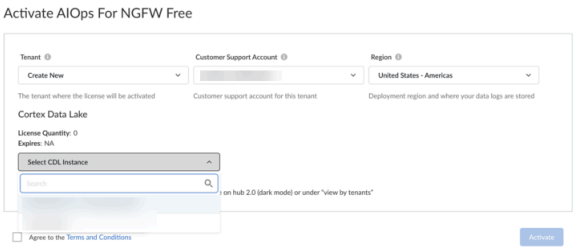
Aktivieren von AIOps for NGFW (Free)

Für die Aktivierung ist die Rolle des Kontoadministrators oder App-Administrators erforderlich.

1. Melden Sie sich beim Hub mit der mandantenorientierten Ansicht an.

   Deaktivieren Sie **Anzeigen nach Support-Konto**, wenn Sie sich in der Support-Konto-Ansicht befinden.

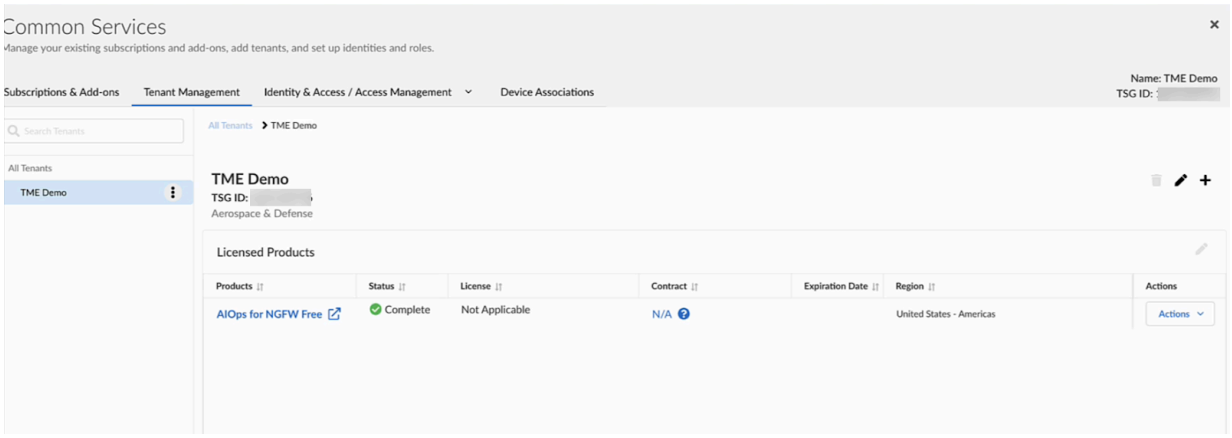
   Wenn Sie keinen bestehenden Mandanten haben, melden Sie sich mit der Support-Kontoansicht beim Hub an.
2. Suchen Sie nach AIOps for NGFW Free und wählen Sie **Aktivieren** aus.
3. Füllen Sie das Formular aus.



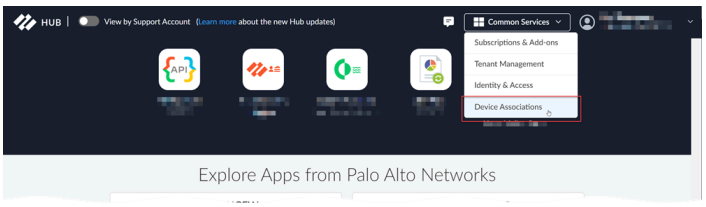
Mandant	Wählen Sie den Mandanten aus, in dem Sie die AIOps für NGFW Free-Instanz aktivieren möchten. Wenn Sie keinen bestehenden Mandanten haben, wählen Sie **Neu erstellen** aus.
Konto beim Kundensupport	Ihre Konto-ID für das Customer Support Portal.
Region	Die Bereitstellungsregion und die Region, in der Ihre Datenprotokolle gespeichert werden. Siehe Regionen für AIOps für NGFW.
Strata-Protokollierungsdienst	Der Strata Logging Service, von dem Sie Daten an AIOps für NGFW Free senden möchten. Wenn Sie über einen Strata-Protokollierungsdienst (Strata Logging Service, SLS) verfügen, können Sie diesen mit AIOps für NGFW Free verknüpfen. Andernfalls können Sie diesen Punkt überspringen.

4. **Stimmen Sie den allgemeinen Geschäftsbedingungen zu** und wählen Sie **Aktivieren** aus.

5. AIOps für NGFW Free ist bereit, sobald in der Spalte **Status** die Meldung **Abgeschlossen** angezeigt wird.



6. Ordnen Sie Geräte einem Mandanten zu, der Ihre AIOps für NGFW Free-Instanz enthält.
   1. Melden Sie sich beim Hub an.
   2. Wählen Sie **Allgemeine Dienste** > **Gerätezuordnungen** aus.



   3. Wählen Sie **Gerät hinzufügen** aus.
   4. Wählen Sie eine oder mehrere Firewalls oder Panorama-Appliances aus und klicken Sie auf **Speichern**.

Wenn Sie das Onboarding über von Panorama verwaltete Bereitstellungen vornehmen, müssen Sie Panorama dem Mandanten zuordnen, der AIOps für NGFW Free enthält. Stellen Sie sicher, dass Sie alle von Panorama verwalteten Firewalls einzeln dem Mandanten zuordnen.

Die Geräte, die Sie mit dem Mandanten verknüpft haben, werden AIOps für NGFW Free automatisch hinzugefügt. Weitere Informationen finden Sie unter Zuordnen von Geräten zu einem Mandanten.

- *Für die Aktivierung von AIOps für NGFW Free müssen Sie Apps nicht mit Geräten verknüpfen.*
- *Sie können Geräte zu Beginn der Aktivierung einem Mandanten zuordnen, wenn bereits ein Mandant vorhanden ist.*
- *Sie können Gerätezuordnungen entfernen, wenn Sie beispielsweise eine Firewall oder eine Panorama-Appliance außer Betrieb nehmen oder zurückgeben oder wenn Sie sie einer anderen Dienstgruppe für Mandanten (Tenant Service Group, TSG) zuordnen möchten.*

7. Aktivieren Sie Telemetrie auf den Geräten.
   1. Bestätigen Sie, dass das Gerät im Customer Support Portal registriert ist, indem Sie sich bei support.paloaltonetworks.com anmelden, zu Ihrem Konto wechseln (falls erforderlich) und Ihr Gerät unter **Assets** > **Geräte** identifizieren.
   2. Installieren Sie ein Gerätezertifikat auf den Geräten, die Sie einbinden möchten.
   3. Aktivieren Sie die Telemetriefreigabe auf den Geräten.

   Nachdem Sie die Geräte eingebunden und die Telemetrie aktiviert haben, dauert es einige Stunden, bis die ersten Erkenntnisse auf dem Dashboard „AIOps für NGFW“ angezeigt werden. Telemetriedaten werden auf der Geräteseite in Batches generiert und gesendet, wobei jede Metrik abgetastet und mit einer Häufigkeit erfasst wird, die für die Anwendungsfälle, für die die Metrik verwendet wird, optimiert wurde. Dieser Batch-Prozess kann zu einer Verzögerung zwischen der Einbindung der Firewall und der Verfügbarkeit der Erkenntnisse führen. Es kann mehrere Stunden dauern, bis alle Erkenntnisse zu einem neu eingebundenen Gerät auf dem Dashboard „AIOps für NGFW“ angezeigt werden.
8. Melden Sie sich bei AIOps für NGFW Free an, indem Sie im Hub auf das entsprechende Symbol klicken.

Wo sind meine AIOps für NGFW-Funktionen?

Dieser Inhalt bezieht sich auf die Cloud-Verwaltung von Next-Generation Firewalls mit AIOps for NGFW und Strata Cloud Manager. Um mit der Verwaltung von Next-Generation Firewalls mit PAN-OS zu beginnen, klicken Sie hier.

Wo kann ich das verwenden?	Was brauche ich?
• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ☐ AIOps for NGFW Free oder Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro

Palo Alto Networks Strata Cloud Manager ist eine neue, KI-gestützte, einheitliche Netzwerksicherheits-Verwaltungsplattform. Sie können jetzt Strata Cloud Manager verwenden, um AIOps for NGFW und Ihre anderen Produkte und Abonnements von Palo Alto Networks zu verwalten und mit ihnen zu interagieren.

So starten Sie Strata Cloud Manager:

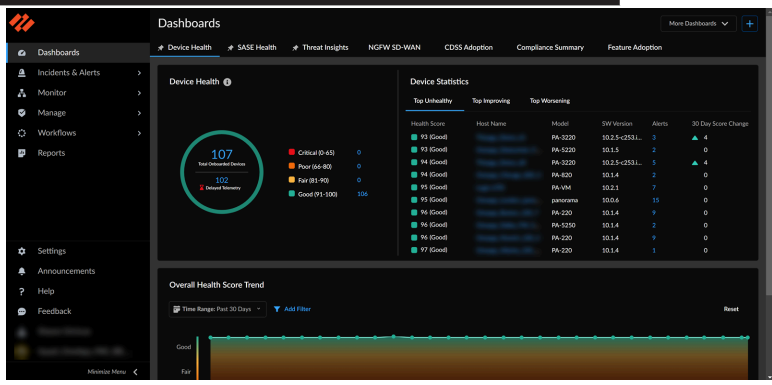
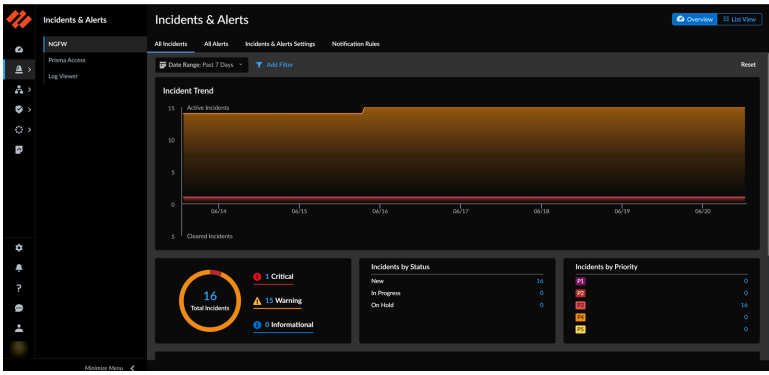
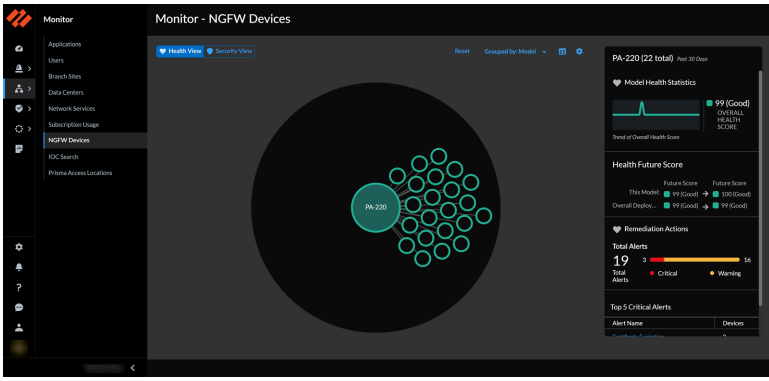
- Gehen Sie zum Hub und starten Sie die Strata Cloud Manager-App
- Gehen Sie direkt zur Strata Cloud Manager-URL

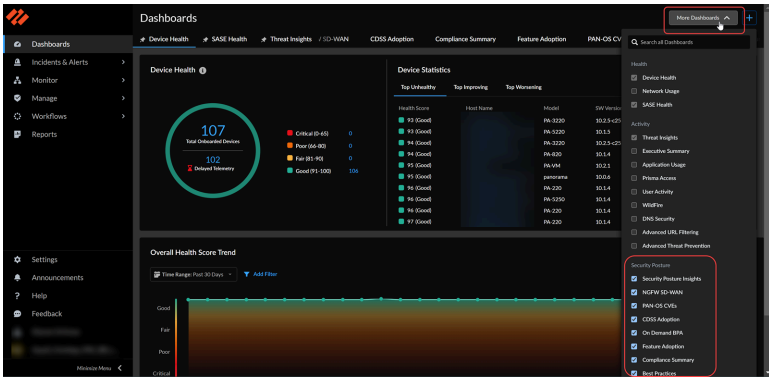
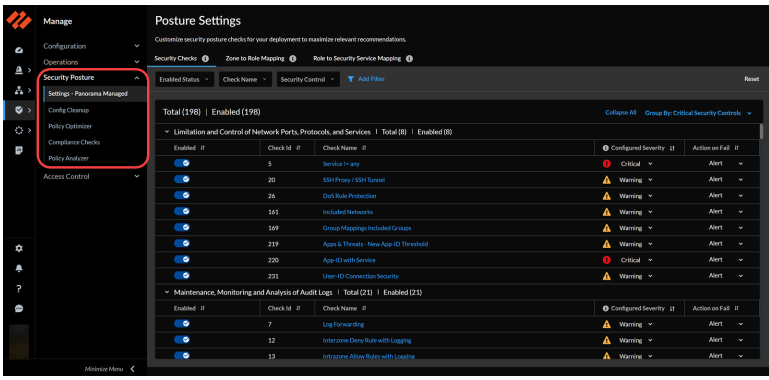
- Strata Cloud Manager *bietet einheitliche Verwaltung und Betrieb ausschließlich für NGFWs, die die AIOps-Lizenz für NGFW Premium verwenden. Der Name der Anwendungskachel auf dem Hub für AIOps für NGFW (nur die Premium-App) wurde jetzt in Strata Cloud Manager geändert. Mit diesem Update wurde auch die Anwendungs-URL in stratacloudmanager.paloaltonetworks.com geändert. Außerdem sehen Sie jetzt das Strata Cloud Manager-Logo im linken Navigationsbereich. Verwenden Sie weiterhin die AIOps für NGFW Free-App für die in AIOps für NGFW Free eingebundenen NGFWs.*
- *Wenden Sie sich an Ihr Account-Team, um Cloud-Verwaltung für NGFWs mithilfe von Strata Cloud Manager zu aktivieren.*

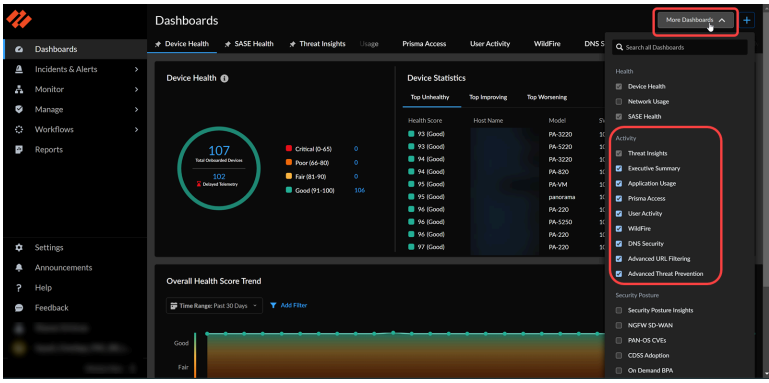
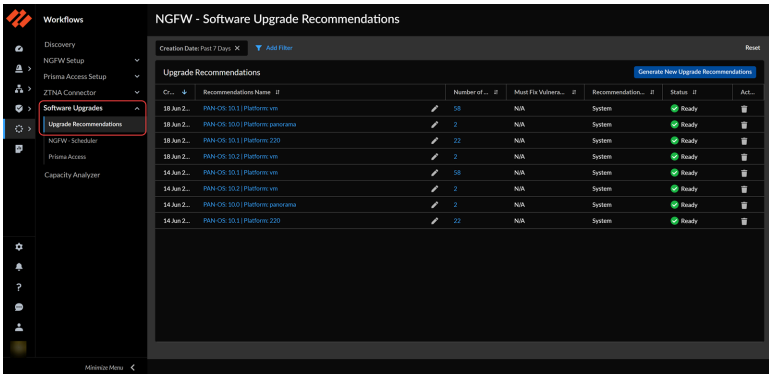
Wenn Sie zuvor die AIOps for NGFW-App verwendet haben, finden Sie Ihre Funktionen in Strata Cloud Manager wie folgt:

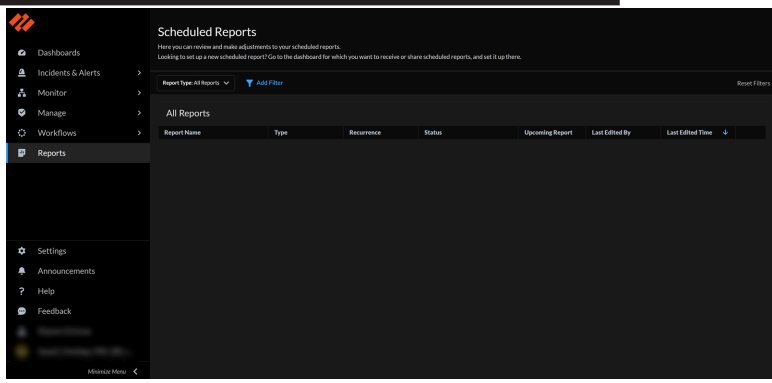
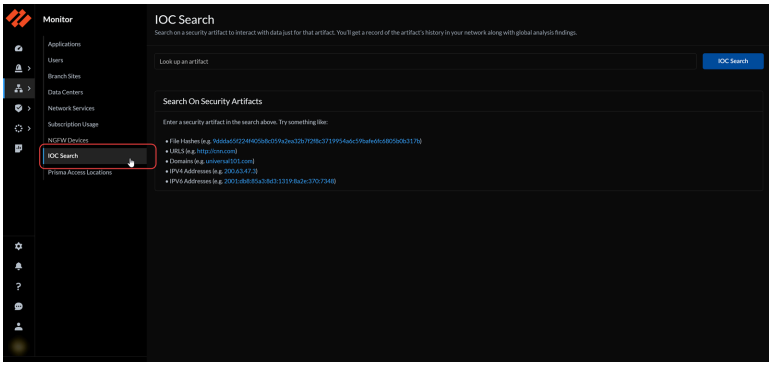
Table 1:

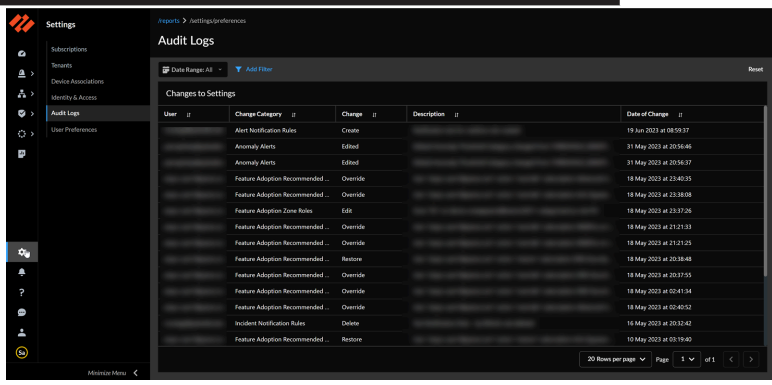
AIOps for NGFW-App	Hier finden Sie diese Funktionen in Strata Cloud Manager:
Dashboards	→ Gehen Sie zu →Dashboards →Gerätezustand

AIOps for NGFW-App	Hier finden Sie diese Funktionen in Strata Cloud Manager:
	
Benachrichtigungen	→ Gehen Sie zu →Vorfälle und Benachrichtigungen →NGFW 
Überwachen	→ Gehen Sie zu →Überwachen →Geräte →NGFW 
Status	→ Gehen Sie zu „Dashboards“, um Folgendes anzuzeigen: • Dashboard „Best Practices“ • Dashboard „Einblicke in den Sicherheitsstatus“ • Dashboard „NGFW SD-WAN“

AIOps for NGFW-App	Hier finden Sie diese Funktionen in Strata Cloud Manager:
	• Dashboard „Sicherheitsempfehlungen“ (PAN-OS-CVEs) • Dashboard „Einführung von CDSS“ • Dashboard „On-Demand-BPA“ • Dashboard „Funktionsannahme“ • Dashboard „Zusammenfassung der Konformität“  → Gehen Sie zu → Verwalten → Sicherheitsstatus, um Folgendes zu finden: • Einstellungen – Von Panorama verwaltet • Konfigurationsbereinigung • Richtlinienoptimierer • Compliance-Prüfungen • Richtlinienanalyse 
Aktivität	→ Gehen Sie zu „Dashboards“, um Folgendes anzuzeigen: • Netzwerk-Nutzung • Bedrohungseinblicke

AIOps for NGFW-App	Hier finden Sie diese Funktionen in Strata Cloud Manager:
	• Anwendungsnutzung • Advanced WildFire • DNS Security • Zusammenfassung • Benutzeraktivität  → Gehen Sie zu **Berichte**, um Berichte für unterstützte Dashboards zu generieren. → Gehen Sie zu **Vorfälle und Benachrichtigungen** für **Protokoll-Viewer**.
Workflows	→ Gehen Sie zu **Workflows** > **Software-Upgrades**, um die **Upgrade-Empfehlungen** zu nutzen. 
Berichte	→ Gehen Sie zu **Berichte**, um Berichte für unterstützte Dashboards zu planen.

AIOps for NGFW-App	Hier finden Sie diese Funktionen in Strata Cloud Manager:
	
Suche	→ Rufen Sie **Überwachen** für die **IOC-Suche** auf. 
Einstellungen	→ Gehen Sie zu **Vorfälle und Benachrichtigungen** > **NGFW** > **Einstellungen für Vorfälle und Benachrichtigungen**, um **Prognose- und Anomalievorfälle und Benachrichtigungen** anzuzeigen. → Gehen Sie zu **Vorfälle und Benachrichtigungen** > **NGFW**, um **Benachrichtigungsregeln** festzulegen. → Gehen Sie zu **Einstellungen**, um Folgendes anzuzeigen: • Auditierungslog • Benutzereinstellungen

AIOps for NGFW-App	Hier finden Sie diese Funktionen in Strata Cloud Manager:
	 → Gehen Sie zu **Verwalten** > **Sicherheitsstatus**, um **Einstellungen – Von Panorama verwaltet** anzupassen. → Gehen Sie zu **Hilfe** →**Metadaten des Mandanten exportieren**.
–	**Sie suchen nach Möglichkeiten zur Verwaltung von NGFWs mit Strata Cloud Manager?** Dies wird nur mit Strata Cloud Manager mit AIOps for NGFW Premium unterstützt und steht in der AIOps for NGFW-App nicht zur Verfügung. → Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFWs und Prisma Access** und **Workflows** > **NGFW-Setup**.

Panorama CloudConnector-Plug-in

Wo kann ich das verwenden?	Was brauche ich?
• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden	❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro

Möchten Sie Ihre Richtlinienregeln proaktiv auf die Einhaltung von Best Practices überprüfen? Wenn Sie Ihre Richtlinienregeln durchgesetzt haben, sollten Sie nicht erst auf eine Benachrichtigung warten müssen, um ein Problem zu beheben. Verbinden Sie AIOps für NGFW oder Strata Cloud Manager mit Ihrem Panorama, um Ihre Konfiguration anhand bestimmter Best Practice-Überprüfungen zu bewerten, bevor Sie sie per Push an Ihre verwalteten Firewalls übertragen. Siehe Proaktives Durchsetzen von Sicherheitsüberprüfungen.

Aktualisierungen Ihrer Sicherheitsrichtlinienregeln sind häufig zeitkritisch und erfordern schnelles Handeln. Sie möchten jedoch sicherstellen, dass alle Aktualisierungen Ihres Regelsatzes für die Sicherheitsrichtlinien Ihren Anforderungen entsprechen und keine Fehler oder Fehlkonfigurationen verursachen (z. B. Änderungen, die zu doppelten oder widersprüchlichen Regeln führen).

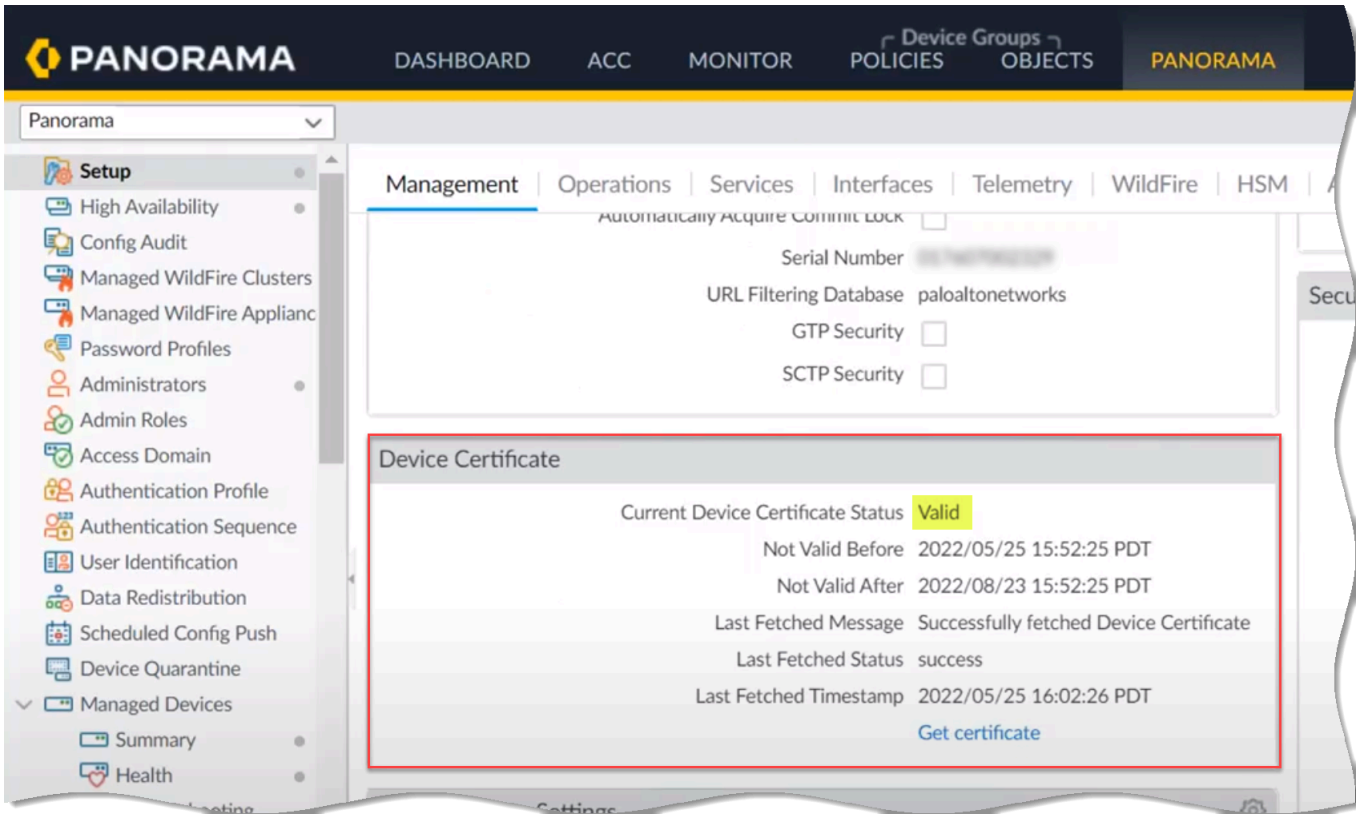
Um dies zu erreichen, ermöglicht Ihnen die Richtlinienanalyse im Strata Cloud Manager, Zeit und Ressourcen bei der Implementierung einer Änderungsanforderung zu optimieren. Die Richtlinienanalyse dient nicht nur dem Analysieren und Bereitstellen von Vorschlägen für eine mögliche Konsolidierung oder Entfernung bestimmter Regeln, um Ihren Absichten zu entsprechen, sondern sucht in Ihrem Regelsatz auch nach Anomalien wie Schatten, Redundanzen, Verallgemeinerungen, Korrelationen und Konsolidierungen.

Verbinden Sie AIOps für NGFW oder Strata Cloud Manager mit Ihrem Panorama und verwenden Sie die Richtlinienanalyse, um Ihren Regelsatz für Sicherheitsrichtlinien hinzuzufügen oder zu optimieren. Siehe Richtlinienanalyse.

Zum Herstellen einer Verbindung zwischen AIOps for NGFW und Ihrem Panorama benötigen Sie Folgendes:

- AIOps für NGFW- oder Strata Cloud Manager-Instanz: Sie benötigen keine AIOps für NGFW Premium-Lizenz, um das Panorama CloudConnector-Plug-in zu installieren. Für die Nutzung von Premium-Funktionen wie Richtlinienanalyse und proaktive Best Practice-Bewertung (BPA) ist jedoch die Premium-Lizenz erforderlich.

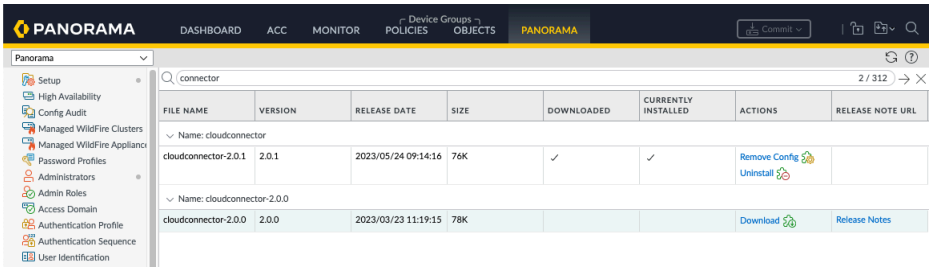
- Ein Panorama mit einem installierten Gerätezertifikat.



- Das Panorama CloudConnector-Plug-in, das auf Ihrem Panorama installiert ist, auf dem PAN OS 10.2.3 oder höher ausgeführt wird.

  Sie müssen dieses Plug-in mit dem folgenden Befehl aktivieren:

  ```
  > request plugins cloudconnector enable basic
  ```



  - *Zur Unterstützung unserer Kunden haben wir dieses Plug-in mit neueren Panorama-Versionen (11.0.1 und höher) vorinstalliert.*
  - *Wenn Sie bereits sowohl das AIOps-Plug-in als auch das CloudConnector-Plug-in installiert haben, deinstallieren Sie das AIOps-Plug-in, da die Plug-ins identisch sind und sich nur der Name geändert hat. Stellen Sie sicher, dass Sie nur ein Plug-in installiert haben. Dabei sollte es sich um die neueste Version des CloudConnector-Plug-ins handeln.*

Wenn Sie das AIOps-Plug-in auf PAN-OS 10.2.3 installiert und dann auf PAN-OS 11.0.1 oder höher aktualisiert haben, wird mit der neuen PAN-OS-Version eine Standardversion des Plug-ins installiert. Dies führt dazu, dass auf Panorama beide Plug-ins vorhanden sind. Gehen Sie in diesem Fall wie folgt vor:

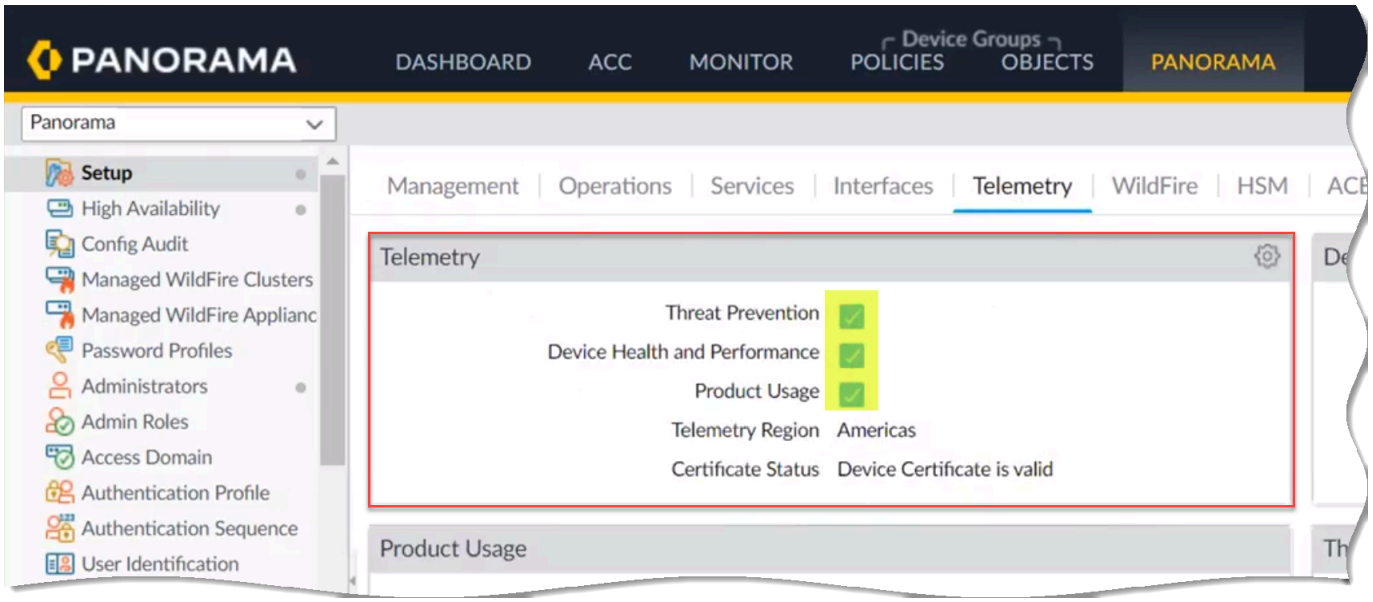
1. Wählen Sie in der Panorama-Weboberfläche **„Panorama > Plug-ins“** aus und **deinstallieren** Sie das AIOps-Plug-in.
2. Aktivieren Sie das CloudConnector-Plug-in:

   ```
   > request plugins cloudconnector enable basic
   ```

Das CloudConnector-Plug-in 2.2.0 unterstützt Proxy-Konfigurationseinstellungen von Panorama. Diese Einstellungen werden erst nach einem Commit wirksam. Es gibt folgende Szenarien:

- Konfigurieren der Proxy-Einstellungen: Wenn Sie Proxy-Einstellungen konfigurieren und ein Commit durchführen, erkennt das CloudConnector-Plug-in die neuen Proxy-Einstellungen während dieses Commits nicht. Nach dem Commit verwendet das Plug-in die Proxy-Konfiguration für zukünftige Interaktionen mit der Cloud.
- Entfernen der Proxy-Einstellungen: Wenn Sie Proxy-Einstellungen entfernen und ein Commit durchführen, erkennt das CloudConnector-Plug-in die entfernten Proxy-Einstellungen während des Commits nicht. Nach dem Commit verwendet das Plug-in die Proxy-Konfiguration nicht mehr für zukünftige Interaktionen mit der Cloud.

- Aktivierte Gerätetelemetrie auf Ihrem Panorama.



- Eine Sicherheitsrichtlinie, die die Kommunikation zwischen Panorama und dem FQDN ermöglicht, der Ihrer Strata Logging Service-Hostregion entspricht:

Amerika (americas)	https://prod.us.secure-policy.cloudmgmt.paloaltonetworks.com/
Australien (au)	https://prod.au.secure-policy.cloudmgmt.paloaltonetworks.com/
Kanada (ca)	https://prod.ca.secure-policy.cloudmgmt.paloaltonetworks.com/
Europa (europe)	https://prod.eu.secure-policy.cloudmgmt.paloaltonetworks.com/
FedRAMP (gov)	https://prod.gov.secure-policy.cloudmgmt.paloaltonetworks.com/
Deutschland (de)	https://prod.de.secure-policy.cloudmgmt.paloaltonetworks.com/
Indien (in)	https://prod.in.secure-policy.cloudmgmt.paloaltonetworks.com/
Japan (jp)	https://prod.jp.secure-policy.cloudmgmt.paloaltonetworks.com/
Singapur (sg)	https://prod.sg.secure-policy.cloudmgmt.paloaltonetworks.com/
Vereinigtes Königreich (uk)	https://prod.uk.secure-policy.cloudmgmt.paloaltonetworks.com/

Erhalten von Benachrichtigungen

Wo kann ich das verwenden?	Was brauche ich?
• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ☐ AIOps for NGFW Free oder Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro

Die Integration von Strata Cloud Manager in Ihre bestehenden Abläufe umfasst die Einrichtung proaktiver Benachrichtigungen, durch die Sie potenzielle Probleme erkennen und Gegenmaßnahmen ergreifen können, bevor sie zu schwerwiegenden Komplikationen führen. Diese Benachrichtigungen können an das Fallverwaltungsprotokoll Ihres Betriebsteams angepasst werden, beispielsweise mit den häufig verwendeten Prioritäten P1 oder P2.

Sie können beispielsweise ein Benachrichtigungssystem einrichten, bei dem kritische Benachrichtigungen zu den kritischsten Problemen sofort an Ihr Sicherheitsteam weitergeleitet werden, damit es sich umgehend darum kümmern kann. Andererseits können Warnhinweise, die weniger dringlich, aber dennoch wichtig sind, zur täglichen Überprüfung eingerichtet werden. Eine solche Regelung gewährleistet eine effiziente Vorfallverwaltung und sorgt gleichzeitig für reibungslose Betriebsabläufe.

Eine weitere Option ist die teambasierte Weiterleitung von Benachrichtigungen. Bestimmte Benachrichtigungskategorien oder selbst spezifische Benachrichtigungen können an unterschiedliche Teams weitergeleitet werden, die am besten für die Bearbeitung dieser Meldungen gerüstet sind. Sie können Benachrichtigungseinstellungen definieren, z. B. welche Alarme Benachrichtigungen auslösen, wie und wie oft Sie Benachrichtigungen erhalten, und Sie können eine Benachrichtigungsregel erstellen.

In diesem Video erfahren Sie, wie Sie eine Benachrichtigungsregel erstellen.

STEP 1 | Wählen Sie **Vorfälle und Benachrichtigungen** > **Vorfall- und Benachrichtigungseinstellungen** > **Benachrichtigungsregeln** > **Benachrichtigungsregel hinzufügen** aus.

STEP 2 | Geben Sie einen `Namen` und eine `Beschreibung` ein.

STEP 3 | Wählen Sie **Neue Bedingung hinzufügen** aus, um die `Regelbedingungen` anzugeben, die zum Auslösen der Benachrichtigung führen.

Um beispielsweise eine Benachrichtigung zur Hardware zu erstellen, wählen Sie **Unterkategorie**, **Gleich** und **Hardware** aus.

STEP 4 | Wählen Sie `Benachrichtigungstyp und Empfänger` für die Benachrichtigung aus.

1. Wenn Sie **E-Mail** auswählen, wählen Sie eine E-Mail-Gruppe aus, also eine Gruppe von Benutzern, die die E-Mail-Benachrichtigungen erhalten. Alternativ wählen Sie **Neue E-Mail-Gruppe erstellen** aus.

   1. Wenn Sie eine neue E-Mail-Gruppe erstellen, geben Sie den Namen einer E-Mail-Gruppe ein und beginnen Sie mit der Eingabe der E-Mail-Adressen derjenigen, die Sie

der Gruppe hinzufügen möchten. Drücken Sie nach der Eingabe der einzelnen E-Mail-Adressen die Eingabetaste.

2. Wählen Sie **Next (Weiter)**.
3. Wählen Sie aus, wie oft diese Benachrichtigungen gesendet werden sollen:

- Sofort
- Gruppiert und alle 4 Stunden
- Gruppiert und einmal pro Tag

2. Wenn Sie **ServiceNow** auswählen, geben Sie die `ServiceNow-URL`, die Anmeldeinformationen für den Client, die Anmeldeinformationen für ServiceNow und die `ServiceNow-API-Version` ein.
   1. **Testen** Sie Ihre Verbindung, um sicherzustellen, dass die Integration funktioniert.
   2. Wählen Sie **Next (Weiter)**.

STEP 5 | Regel speichern

Beheben von Anomalien hinsichtlich NGFW-Konnektivität und Richtliniendurchsetzung

Wo kann ich das verwenden?	Was brauche ich?
• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden	❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro ❑ Für die Protokollierung ist eine Lizenz für den Strata-Protokollierungsdienst erforderlich ❑ Wenn Sie eine Prisma Access-Lizenz besitzen, können Sie die **Ordnerverwaltung** verwenden, um Ihre vordefinierten Ordner anzuzeigen und Websicherheit für einen Ordner zu aktivieren.

Beheben Sie Probleme Ihrer NGFWs vom Strata Cloud Manager aus, ohne zwischen verschiedenen Firewall-Schnittstellen wechseln zu müssen. Wenn nach der Bereitstellung und Konfiguration Ihrer NGFWs Verbindungsprobleme auftreten, können Sie sich einen Gesamtüberblick über Ihre Routing- und Tunnelzustände verschaffen und ins Detail gehen, um Anomalien und problematische Konfigurationen zu finden.

Beheben Sie Probleme mit Ihren identitätsbasierten Richtlinienregeln und dynamisch definierten Endpunkten. Sie können den Status bestimmter NGFWs prüfen und mögliche Diskrepanzen zwischen der erwarteten Funktionsweise einer Richtlinie und ihrem tatsächlichen Durchsetzungsverhalten aufdecken.

Mithilfe der **Fehlerbehebung** können Sie Probleme, die bei diesen Netzwerk- und Identitätsfunktionen auftreten können, genauer untersuchen und Verbindungsprobleme oder Anomalien bei der Richtliniendurchsetzung aufspüren und beheben:

Fehlerbehebung: Netzwerk

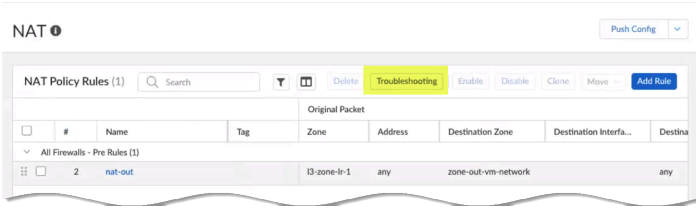
- NAT
- DNS-Proxy

Fehlerbehebung: Identitäten und Richtlinien

- Benutzergruppen
- Dynamische Adressgruppen
- Dynamische Benutzergruppen
- Benutzer-ID

Fehlerbehebung: Firewall

- Sitzungsbrowser



Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Vorgänge** > > **Fehlerbehebung** > **Sitzungsbrowser**, um mit der Fehlerbehebung Ihrer Firewalls zu beginnen.

Alternativ können Sie zu der Funktion wechseln, für die Sie Probleme beheben möchten, und durch Auswählen der Schaltfläche **Fehlerbehebung** damit beginnen.

Sie können die von Ihnen ausgeführten Fehlerbehebungsjobs anzeigen und nach Status, Aktion, Suchziel und Zeitstempel sortieren.

Merkmal	Funktionsstandort	Verfügbare Aktionen	Aktionsumfang	Jobausgabe organisiert nach:
Sitzungsbrowser (Firewall)	**Verwalten** > **Configuration (Konfiguration)** > **NGFW und Prisma Access** > **Vorgänge** > > **Fehlerbehebung** > **Sitzungsbrowser**	Filtern nach: • Firewalls • Regelname • Quellzone • Quelladresse • Quellbenutzer • Quellport • Zielzone • Zieladresse • Zielport • App-ID	Von Ihnen angegebene Firewalls	• Sitzungs-ID • Startzeit • Zonen • Quelle • Ziel • Ports • Protokoll • Anwendung • Eingang • Ausgang • Byte
DNS-Proxy (Netzwerk)	**Konfiguration verwalten** > **NGFW und Prisma Access** > **Geräteeinstellungen** > **DNS-Proxy**	• DNS-Proxy-Cache anzeigen • Durchsuchen des DNS-Proxy-Cache	Von Ihnen angegebene Firewalls	• Domänenname • IP-Adresse • Typ – IPv4-Adressdatensatz (A), IPv6-Adressdatensatz (AAAA), kanonischer Namensdatensatz (CNAME), Mail-Austausch-Datensatz (MX) und Zeiger

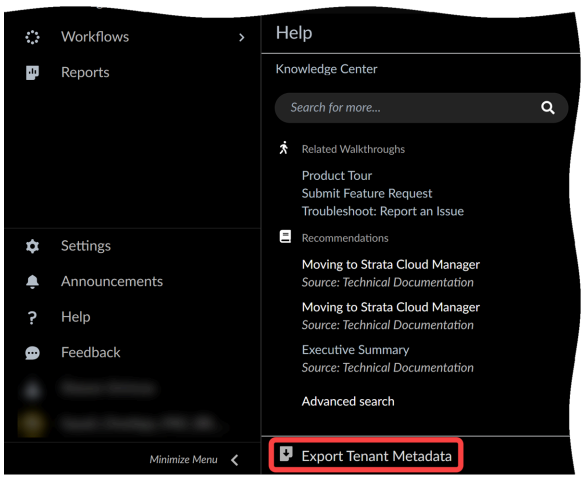
Merkmal	Funktionsstandort	Verfügbare Aktionen	Aktionsumfang	Jobausgabe organisiert nach:
				auf einen kanonischen Namen (PTR) • Klasse: Internet (IN TCP/IP), Chaos (CH) und Hesiod (HS) • Time-to-Live (TTL) in Sekunden • Treffer – Anzahl der Datensatzabfragen seit dem letzten Neustart
NAT (Netzwerk)	**Konfiguration verwalten** > **NGFW und Prisma Access** > **Netzwerkrichtlinien** > **NAT**	NAT-Regel-IP-Pool anzeigen	Von Ihnen angegebene Firewalls	• Regel • Typ • Verwendet • Verfügbar • Speichergrößenverhältnis
Benutzergruppen (Identität)	**Konfiguration verwalten** > **NGFW und Prisma Access** > **Identitätsdienste** > **Cloud Identity Engine**	• Benutzergruppe anzeigen • Benutzergruppe suchen	Von Ihnen angegebene Firewalls	• Benutzername • Gruppe
Dynamische Adressgruppen (Identität)	**Konfiguration verwalten** > **NGFW und Prisma Access** > **Objekte** > **Adresse** > **Adressgruppen**	• Alle dynamischen Adressgruppen anzeigen • Nach einer dynamischen Adressgruppe suchen (aus einer Liste ausgewählt)	Von Ihnen angegebene Firewalls	• Name • Filter • Mitglieder

Merkmal	Funktionsstandort	Verfügbare Aktionen	Aktionsumfang	Jobausgabe organisiert nach:
Dynamische Benutzergruppen (Identität)	**Konfiguration verwalten** > **NGFW und Prisma Access** > **Objekte** > **Dynamische Benutzergruppen**	• Nach dynamischer Benutzergruppe suchen • Nach Benutzernamen suchen	Von Ihnen angegebene Firewalls	• Mitglieder (Benutzername) und/oder dynamische Benutzergruppe
Benutzer-ID (Identität)	**Konfiguration verwalten** > **NGFW und Prisma Access** > **Identitätsdienste** > **Identitätsweitergabe**	• Alle Benutzer-IP-Zuordnungen anzeigen • Nach Benutzer-IP-Zuordnung suchen	Von Ihnen angegebene Firewalls	• IP • Benutzer • Von • Timeout nach Inaktivität • Max. Timeout

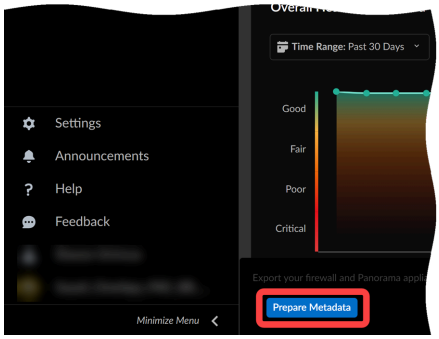
Exportieren von Metadaten zur Fehlerbehebung

Um dem technischen Support die Informationen bereitzustellen, die er benötigt, um Ihnen besser helfen zu können, ermöglicht Ihnen AIOps for NGFW, Ihre Bereitstellungsdaten auf Ihren lokalen Computer zu exportieren. Diese Daten werden als JSON-Dateien exportiert und im GZIP-Format komprimiert.

1. Wählen Sie **Hilfe > Metadaten des Mandanten exportieren** aus.



2. **Bereiten Sie die Metadaten vor**.



3. **Laden Sie Ihre Metadatendatei herunter**.

   Der Name der Metadatendatei enthält Ihre Customer Support Portal-(CSP-)ID, Ihre AIOps für NGFW-Mandanten-ID und den Zeitstempel für den Export: <*csp-tenant-timestamp*>.gzip.

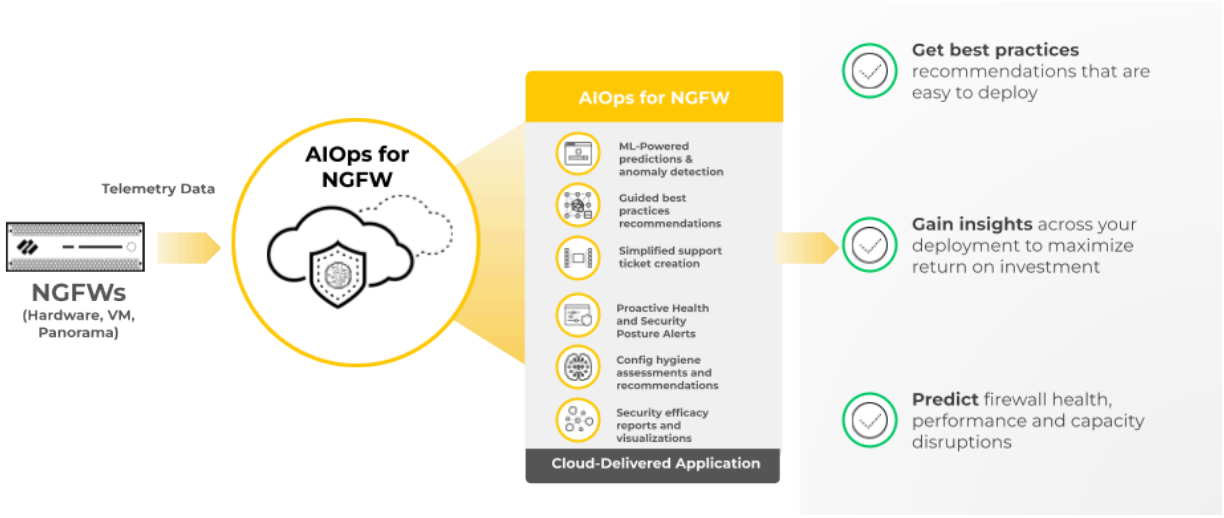
Gerätetelemetrie für AIOps for NGFW

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

AIOps for NGFW bewertet den Zustand der Firewalls in Ihrer Bereitstellung durch die Analyse von Telemetriedaten, die Ihre PAN-OS-Geräte an Strata Logging Service senden. Zum Senden dieser Daten muss auf Ihren Geräten die Gerätetelemetrie aktiviert sein.

Sobald die Telemetrie konfiguriert ist, senden Ihre Firewalls der nächsten Generation Telemetrierohdaten an Strata Logging Service in festgelegten Intervallen. Strata Logging Service analysiert und übersetzt diese Rohdaten, sodass Ihnen AIOps for NGFW Gerätestatus, Visualisierungen und Benachrichtigungen bereitstellen kann.

Binden Sie Ihre Geräte ein, um mit dem Senden von Gerätetelemetriedaten an AIOps for NGFW zu beginnen.



Aktivieren von Telemetrie auf Geräten

Befolgen Sie die nachstehenden Schritte, um AIOps for NGFW mit Ihren PAN-OS-Geräten zu verwenden.

Wenn Ihr ausgehender Datenverkehr über einen Proxy läuft, stellen Sie sicher, dass Sie die für AIOps für NGFW erforderlichen Domains zugelassen haben (siehe Für AIOps for NGFW erforderliche Domains).

Sie müssen Panorama in AIOps für NGFW einbinden, wenn Sie von Panorama verwaltete Bereitstellungen einbinden.

1. Bestätigen Sie, dass das Gerät im Customer Support Portal registriert ist, indem Sie sich bei support.paloaltonetworks.com anmelden, zu Ihrem Konto wechseln (falls erforderlich) und Ihr Gerät unter **Assets** > **Geräte** identifizieren.
2. Installieren Sie ein Gerätezertifikat auf den Geräten, die Sie einbinden möchten.
3. Aktivieren Sie die Telemetriefreigabe auf den Geräten.

Nachdem Sie die Geräte eingebunden und die Telemetrie aktiviert haben, dauert es einige Stunden, bis die ersten Erkenntnisse auf dem Dashboard „AIOps für NGFW“ angezeigt werden. Telemetriedaten werden auf der Geräteseite in Batches generiert und gesendet, wobei jede Metrik abgetastet und mit einer Häufigkeit erfasst wird, die für die Anwendungsfälle, für die die Metrik verwendet wird, optimiert wurde. Dieser Batch-Prozess kann zu einer Verzögerung zwischen der Einbindung der Firewall und der Verfügbarkeit der Erkenntnisse führen. Es kann mehrere Stunden dauern, bis alle Erkenntnisse zu einem neu eingebundenen Gerät auf dem Dashboard „AIOps für NGFW“ angezeigt werden.

Für AIOps for NGFW erforderliche Domains

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Wenn ausgehender Datenverkehr von Ihren Geräten über einen Proxy läuft, stellen Sie sicher, dass Sie die folgenden FQDNs zugelassen haben, um AIOps for NGFW erfolgreich verwenden zu können.

Domänen zum Zugriff auf AIOps for NGFW

Lassen Sie diese Domänen zu, um unabhängig von Ihrer geografischen Region auf die AIOps for NGFW-Anwendung zuzugreifen.

- *.prod.di.paloaltonetworks.cloud
- *.paloaltonetworks.com
- *.prod.di.paloaltonetworks.com
- *.prod.reporting.paloaltonetworks.com
- *.receiver.telemetry.paloaltonetworks.com
- https://storage.googleapis.com

App-IDs und Domänen zum Senden von Telemetrie

Unter Für Strata Logging Service erforderliche TCP-Ports und FQDNs sind die App-IDs und Ports aufgeführt, die Sie auf Ihren Palo Alto Networks Firewalls zulassen müssen, um Telemetriedaten erfolgreich an AIOps for NGFW zu senden.

Lassen Sie auf Ihrem Proxyserver nicht nur die erforderlichen Ports und FQDNs zu, sondern auch die Domäne, die Ihrer geografischen Region entspricht, damit Ihre Geräte Telemetriedaten an AIOps for NGFW senden können.

Region	Domäne
US	http://br-prd1.us.cdl.paloaltonetworks.com/
Europa	http://br-prd1.nl.cdl.paloaltonetworks.com/
GB	http://br-prd1.uk.cdl.paloaltonetworks.com/
Kanada	http://br-prd1.ca1.ne1.cdl.paloaltonetworks.com/

Region	Domäne
Singapur	http://br-prd1.sg1.se1.cdl.paloaltonetworks.com/
Japan	http://br-prd1.jp1.ne1.cdl.paloaltonetworks.com/
Australien	http://br-prd1.au1.se1.cdl.paloaltonetworks.com/
Deutschland	http://br-prd1.de1.ew3.cdl.paloaltonetworks.com/
Indien	http://br-prd1.in1.as1.cdl.paloaltonetworks.com/

Optimieren Sie Ihren Sicherheitsstatus

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

AIOps for NGFW trägt nicht nur dazu bei, Ihre Firewalls funktionsfähig zu halten. Sie können zudem prüfen, ob Sie von den Firewalls wirksam vor Sicherheitsbedrohungen geschützt werden.

Bewertungen des Sicherheitsstatus unterstützen derzeit nicht mehrere virtuelle Systeme, da bei der Konfigurationsverarbeitung nur das virtuelle Standardsystem (vsys1) berücksichtigt wird.

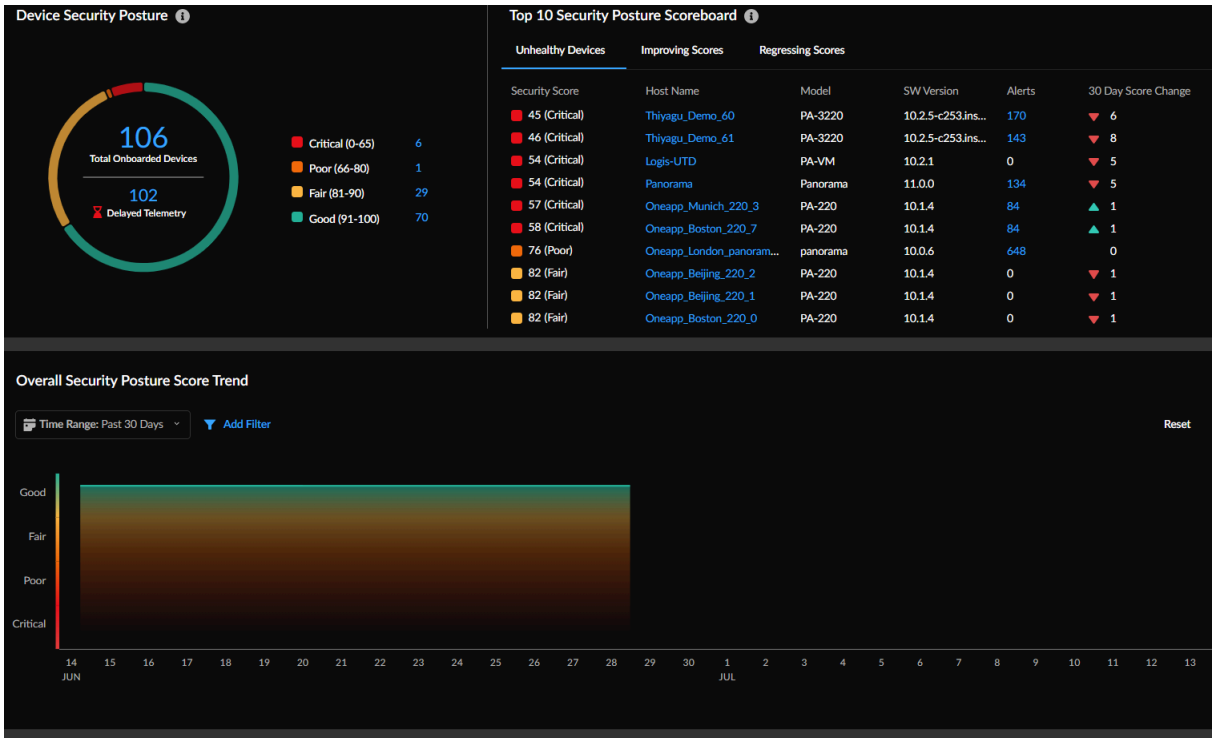
- Überwachen von Einblicken in den Sicherheitsstatus: Verschaffen Sie sich Einblick in den Sicherheitsstatus und Trend Ihrer Bereitstellung basierend auf dem Sicherheitsstatus der eingebundenen NGFW-Geräte.
- Überwachen der Funktionsannahme: Sehen Sie sich die Sicherheitsfunktionen an, die Sie in Ihrer Bereitstellung verwenden.
- Überwachen von Sicherheitsabonnements: Sehen Sie sich die empfohlenen Abonnements für die von der Cloud bereitgestellten Sicherheitsdienste (Cloud-Delivered Security Services, CDSS) und deren Verwendung auf Ihren Geräten an.
- Bewerten von Sicherheitslücken: Sehen Sie sich die Sicherheitslücken an, die sich auf eine bestimmte Firewall und PAN-OS-Version auswirken, und treffen Sie abhängig von Ihren Erkenntnissen die Entscheidung, ob ein Upgrade erforderlich ist.
- Überwachen der Konformitätszusammenfassung: Sehen Sie sich den Änderungsverlauf der Sicherheitsüberprüfungen an, die vor bis zu 12 Monaten vorgenommen wurden, zusammengefasst nach den CIS- (Center for Internet Security) und NIST-Frameworks (National Institute of Standards and Technology).
- Proaktives Durchsetzen von Sicherheitsüberprüfungen: Gehen Sie proaktiv gegen suboptimale Konfigurationen vor, indem Sie Commits blockieren, die bestimmte Best Practice-Überprüfungen nicht bestehen.
- Richtlinienanalyse: Erhalten Sie Analysen und Vorschläge für eine mögliche Konsolidierung oder Entfernung bestimmter Richtlinienregeln, um Ihrem angestrebten Sicherheitsstatus gerecht zu werden. Außerdem können Sie Ihren Regelsatz auf Anomalien wie Schatten, Redundanzen, Generalisierungen, Korrelationen und Konsolidierungen überprüfen.

Überwachen von Einblicken in den Sicherheitsstatus

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	• Eine der folgenden Komponenten: ❑ oder ❑ oder • Eine Rolle mit der Berechtigung zum Anzeigen des Dashboards

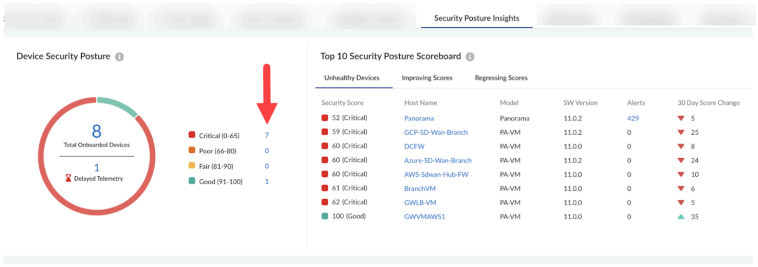
Mithilfe des Dashboards **Einblicke in den Sicherheitsstatus** können Sie sich Einblick in den Sicherheitsstatus und Trend Ihrer Bereitstellung basierend auf dem Sicherheitsstatus der eingebundenen NGFW-Geräte verschaffen. Der Schweregrad der Sicherheitsbewertung (0–100) und die entsprechende Sicherheitsstufe (gut, angemessen, schlecht, kritisch) bestimmen den Sicherheitsstatus eines Geräts. Der Sicherheitswert wird anhand von Priorität, Anzahl, Art und Status der offenen Benachrichtigungen berechnet.

1. Navigieren Sie zunächst zu **Dashboards** > **Einblicke in den Sicherheitsstatus**.



2. Zeigen Sie den Zustand Ihrer Geräte mithilfe der Option **Sicherheitsstatus des Geräts** an. Es wird Folgendes angezeigt:
   - Die Gesamtzahl der eingebundenen NGFWs.
   - Die Anzahl der Geräte, die seit über 12 Stunden keine Telemetriedaten gesendet haben.
   - Die Priorität des Sicherheitswerts für die eingebundenen Geräte in Ihrer Bereitstellung. Klicken Sie auf den Zahlenlink, um Gerätedetails und Sicherheitsstatistiken anzuzeigen.

   Beispielsweise können Sie 7 kritische Risiken für alle Geräte anzeigen.



   In diesem Fall können Sie auf die kritischen Benachrichtigungen klicken und die Geräte anzeigen, die Warnungen generieren. Wenn Sie noch tiefer ins Detail gehen, werden Sie feststellen, dass der Schutz der Benutzeranmeldeinformationen auf den Firewalls nicht aktiviert wurde. Sie können dieses Problem auf allen Geräten beheben, um Phishing-Angriffe zu vermeiden.
3. Überprüfen Sie, welche Ihrer Geräte den schlechtesten Zustand und in den letzten 30 Tagen eine rückläufige Sicherheitsbewertung aufweisen. Sie können den Zustand Ihrer Geräte anzeigen, einschließlich ihres Betriebsstatus, der Softwareversion und anderer wichtiger Metriken.

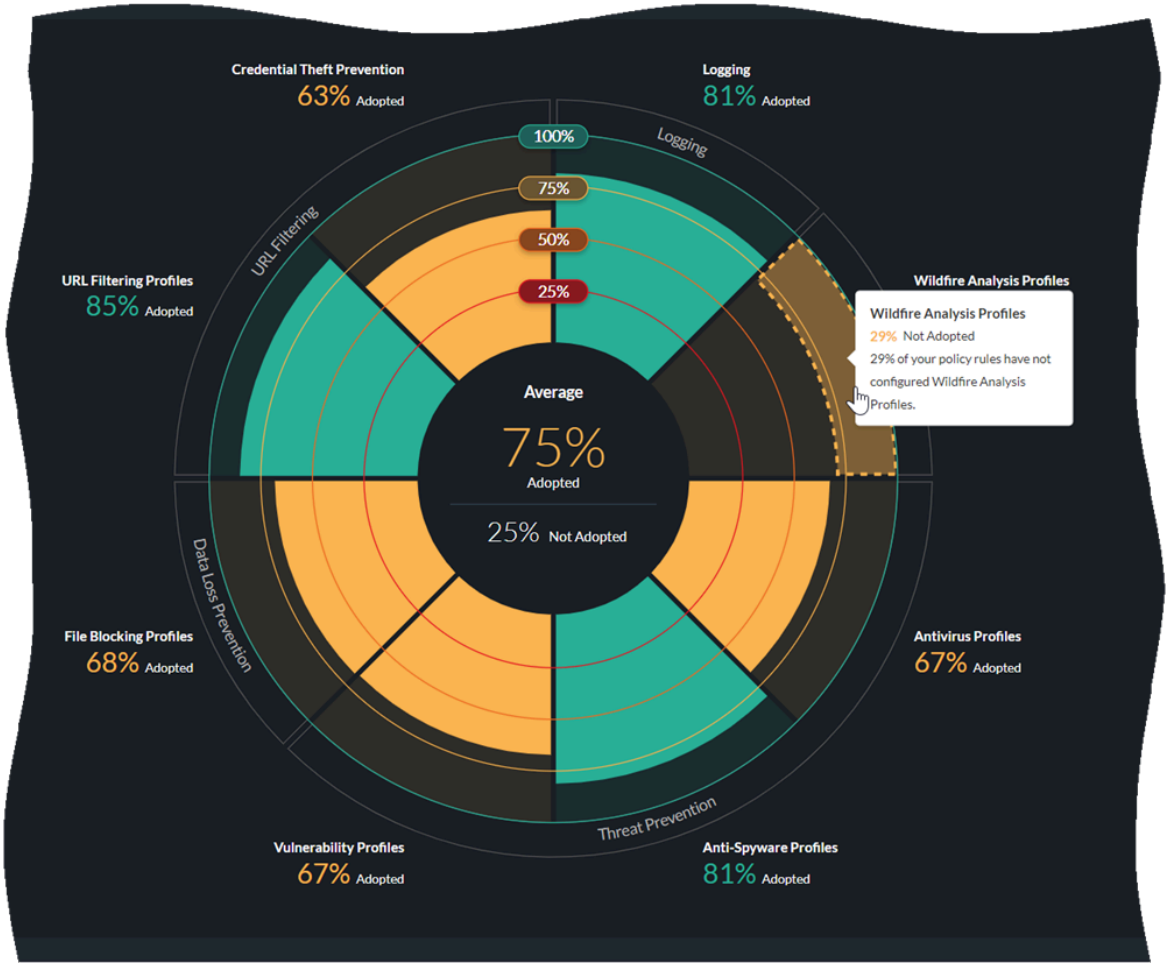
   Sie können auch feststellen, ob auf einigen Geräten veraltete Softwareversionen ausgeführt werden. In diesem Fall können Sie ein Upgrade auf die neueste empfohlene Version planen, die Sie unter Empfehlungen für Upgrade finden.
4. Überprüfen Sie den Trend zum Sicherheitsstatus Ihrer Bereitstellung für den ausgewählten Zeitraum. Bewegen Sie den Mauszeiger über den Auslösepunkt, um die Geräte und aktiven Warnungen anzuzeigen, die den Trend zum Sicherheitsstatus beeinflussen. Sie können Trends für ein Gerät oder mehrere Geräte anzeigen, gefiltert nach Hostname, Modell oder Softwareversion.

Weitere Informationen finden Sie unter Dashboard: Einblicke in den Sicherheitsstatus.

Überwachen der Funktionsannahme

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	• Eine der folgenden Komponenten: ❑ oder ❑ oder • Eine Rolle mit der Berechtigung zum Anzeigen des Dashboards

In **Dashboards** > **Funktionsannahme** können Sie die Sicherheitsfunktionen anzeigen, die Sie in Ihrer Bereitstellung verwenden. So können Sie sicherstellen, dass Sie Ihre Sicherheitsabonnements und Firewall-Funktionen von Palo Alto Networks optimal nutzen.



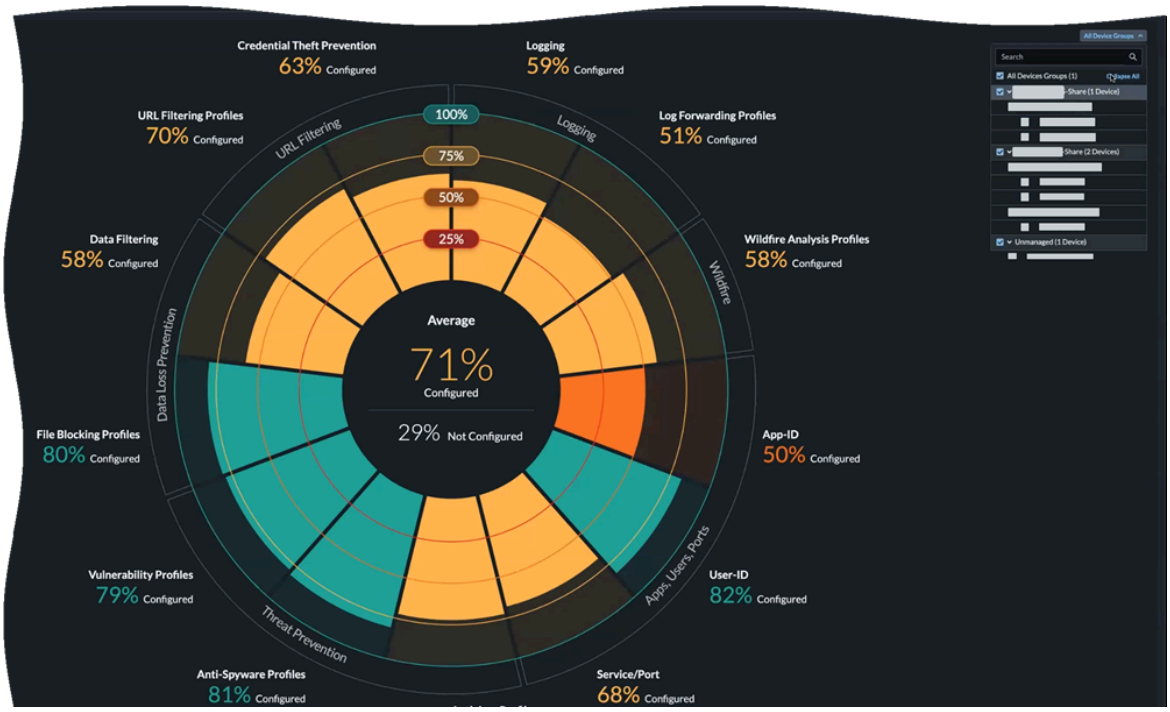
Dieses Dashboard zeigt, wo Ihre Sicherheitsrichtlinie stark ist und wo es Lücken bei der Annahme von Funktionen gibt, auf deren Verbesserung Sie sich konzentrieren können. Um maximale Transparenz im Datenverkehr und maximalen Schutz vor Angriffen zu erreichen, legen Sie Ziele für die Annahme von Sicherheitsfunktionen fest und verwenden Sie die folgenden

Empfehlungen als Grundlage für Best Practices. Bewerten Sie Ihre aktuelle Situation im Vergleich zum Ausgangszustand, um Lücken bei der Umsetzung von Sicherheitsrichtlinien zu identifizieren.

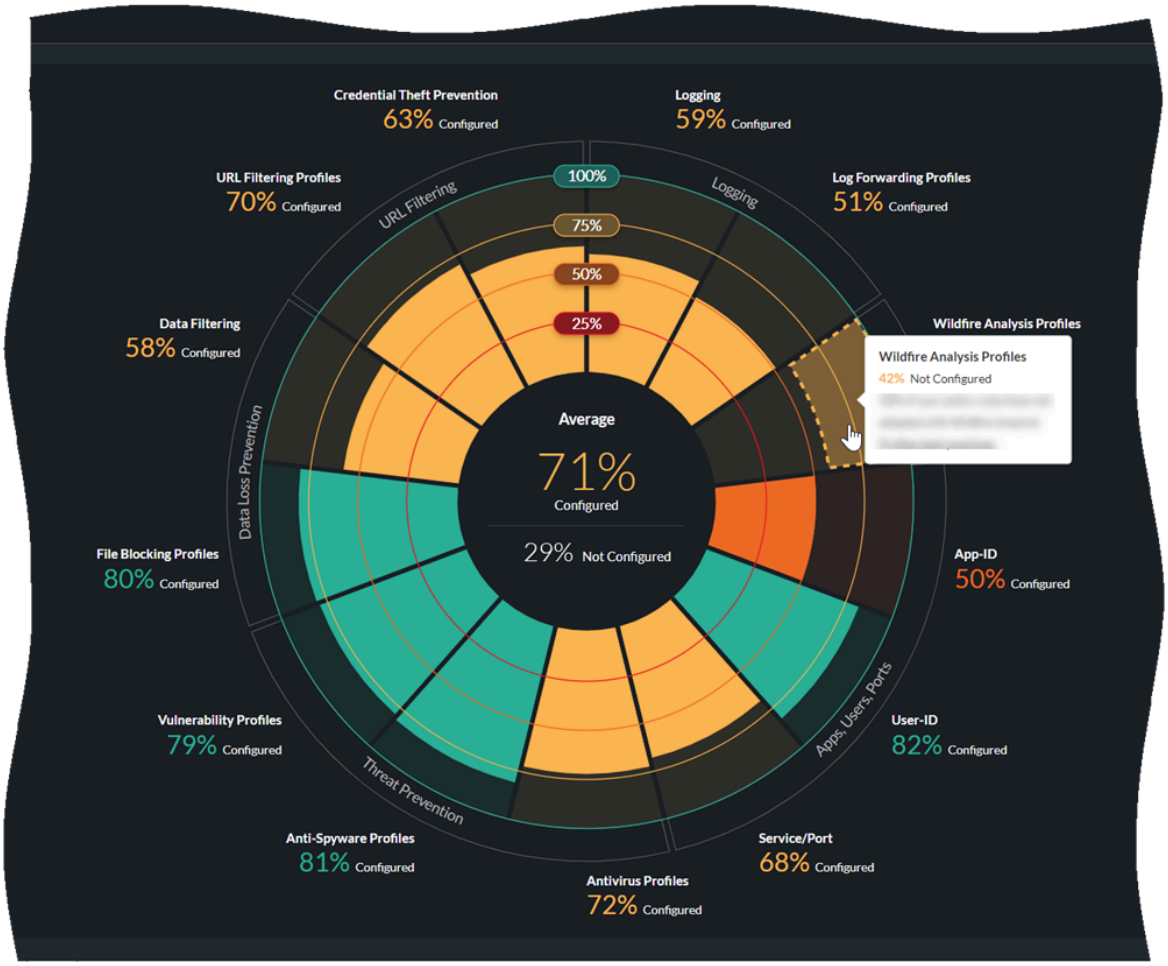
Mithilfe der Annahmeübersicht können Sie Geräte, Zonen und Bereiche identifizieren, in denen Sie die Annahme von Sicherheitsrichtlinien verbessern können. Sie können die Annahmeinformationen nach Gerätegruppe, Seriennummer und Vsys, Zonen, Architekturbereichen, Tags, Regeldetails und Zonenzuordnungen überprüfen. Filtern Sie nach „Gerätegruppe“, um den Umfang einzugrenzen und Lücken zu identifizieren.

Unter **Funktionsannahme** können Sie durch Auswahl von **Best Practices** auch sehen, ob Ihre Sicherheitsfunktionen gemäß den Best Practices von Palo Alto Networks konfiguriert sind.

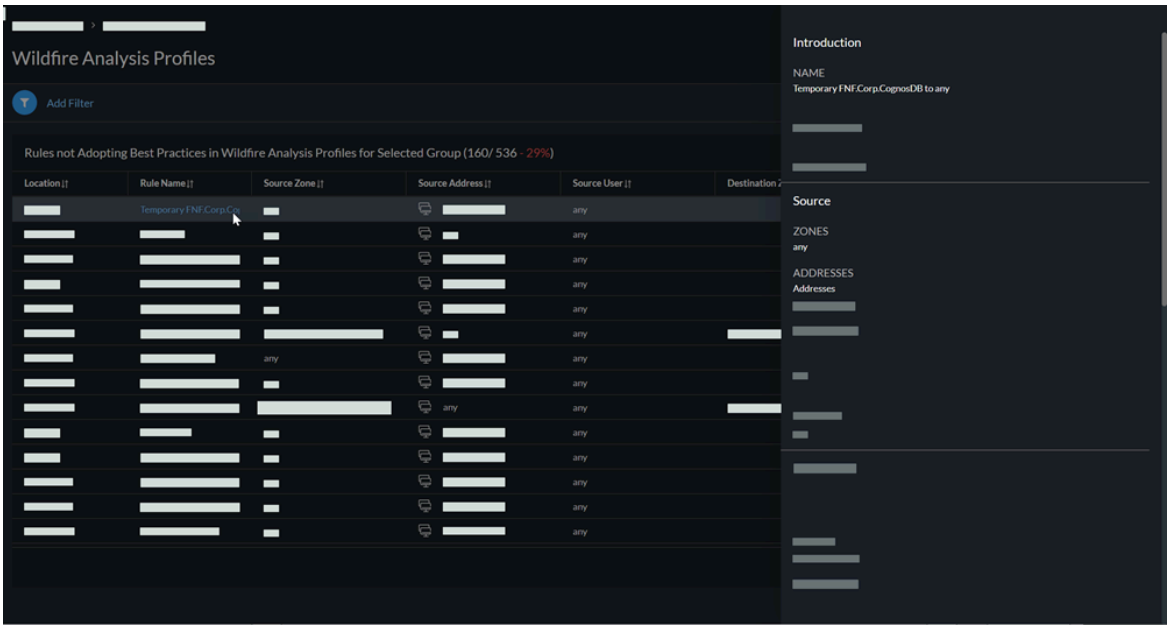
- Um sich auf die Einhaltung der Best Practices für einen bestimmten Satz von Firewalls zu konzentrieren, können Sie das Diagramm nach „Gerätegruppe“ filtern.



- Wählen Sie den Abschnitt für eine Funktion im Diagramm aus, um anzuzeigen, welche Richtlinienregeln verbessert werden können.



- Wählen Sie eine Regel aus, um ihre Details anzuzeigen, ohne die App verlassen zu müssen.



Weitere Informationen finden Sie unter Dashboard: Funktionsannahme.

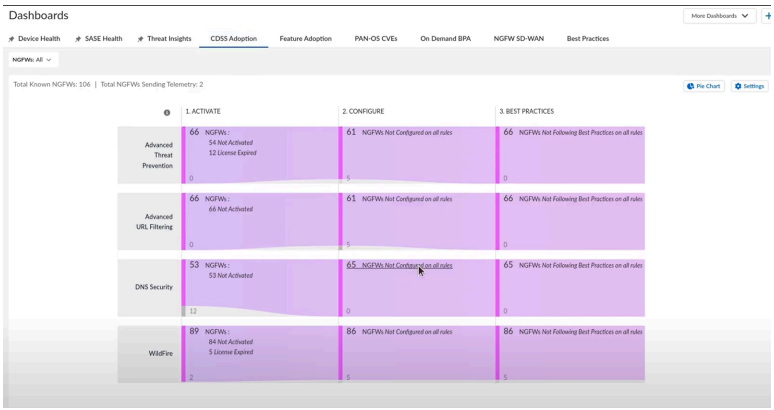
Überwachen von Sicherheitsabonnements

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	• Eine der folgenden Komponenten: ❑ oder ❑ oder • Eine Rolle mit der Berechtigung zum Anzeigen des Dashboards

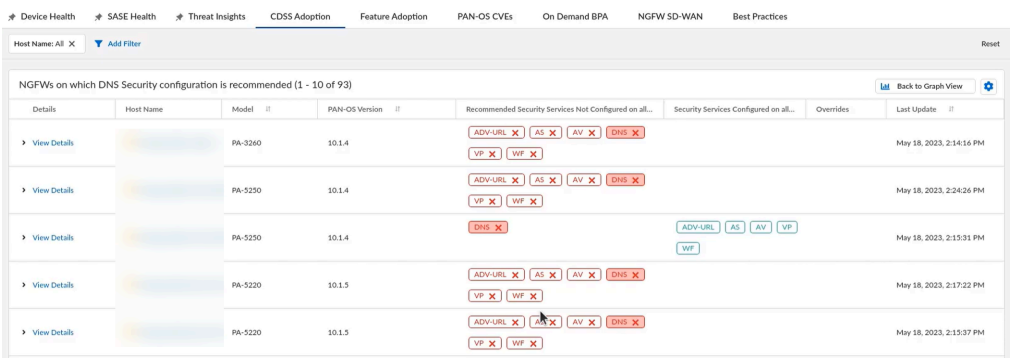
In **Dashboard** > **Status** > **Einführung von CDSS**können Sie die empfohlenen Abonnements für die von der Cloud bereitgestellten Sicherheitsdienste (Cloud-Delivered Security Services, CDSS) und deren Verwendung auf Ihren Geräten anzeigen. Dies hilft Ihnen, Sicherheitslücken zu bestimmen und den Sicherheitsstatus Ihres Unternehmens zu verbessern. Auf dieser Seite wird ein Pop-up-Fenster angezeigt, in dem Sie aufgefordert werden, Ihre Zonenrollen in NGFWs zu bestätigen oder zu aktualisieren, um genaue Empfehlungen zu Sicherheitsdiensten zu erhalten. Sie können dem Link in diesem Pop-up-Fenster folgen, um Zonen Rollen zuzuordnen.

Derzeit unterstützt dieses Dashboard nur vier Sicherheitsabonnements: „Fortschrittliche Bedrohungsabwehr“, „Erweiterte URL-Filterung“, „DNS Security“ und „WildFire“.

1. Oben auf der Seite **Einführung von CDSS** können Sie die Gesamtzahl der bekannten NGFWs und die Anzahl der NGFWs anzeigen, die in Ihrer Instanz Telemetriedaten senden.
2. Die Einführung von CDSS umfasst die schrittweise Aktivierung, Konfiguration und Einhaltung von Best Practices. Um den Fortschritt der einzelnen Abonnements zu verfolgen, klicken Sie einfach auf die Zahlen im Diagramm, um eine Liste der Geräte anzuzeigen, die im Laufe des Vorgangs aktualisiert werden müssen. In diesem Fall sollten Sie die NGFWs überprüfen, bei denen die DNS-Sicherheit nicht konfiguriert ist.



3. Überprüfen Sie NGFWs, für die eine DNS-Sicherheitskonfiguration empfehlenswert, aber nicht konfiguriert ist. Wählen Sie **Details anzeigen** aus, um die Quell- und Zielrolle zu überprüfen.

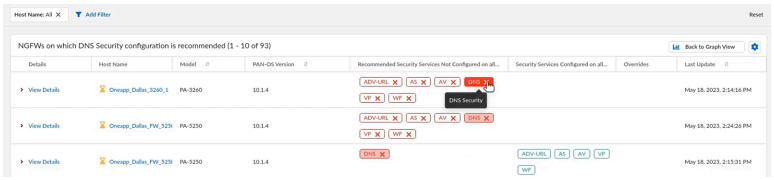


4. Wählen Sie **Richtlinien anzeigen** aus, um die Details der Regeln und der entsprechenden Quell- und Zielzonen anzuzeigen.

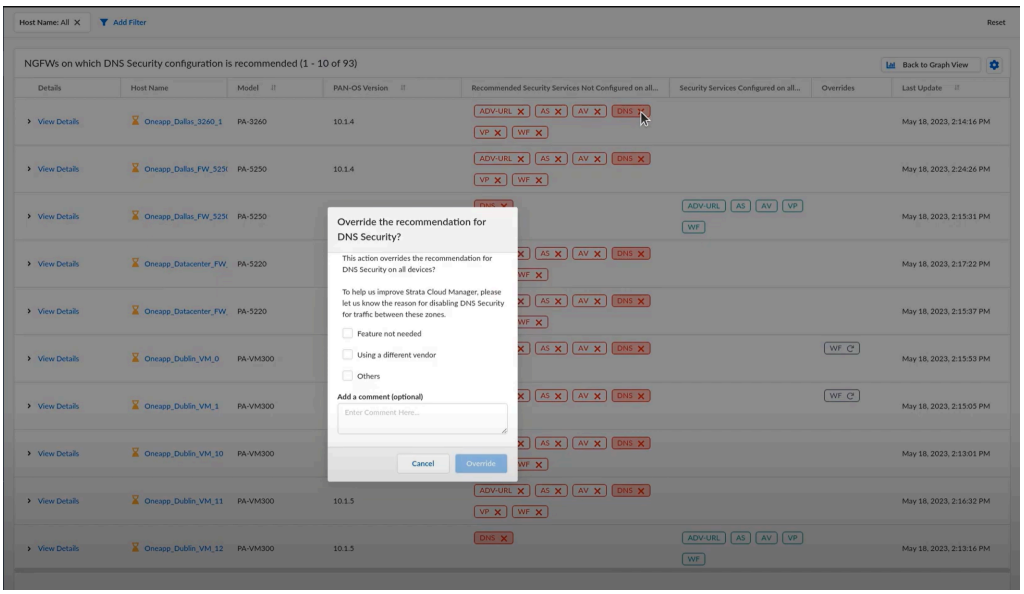
   Außerdem können Sie auf einen Regelnamen klicken, um die Details zur Regel anzuzeigen.

5. Kehren Sie zum Trichterdiagramm zurück. Sie können dieselben Informationen auch im Format eines Kreisdiagramms anzeigen.

6. Wenn Sie einen empfohlenen Sicherheitsdienst aus irgendeinem Grund nicht benötigen, können Sie ihn überschreiben. In diesem Fall ist der DNS-Sicherheitsdienst nicht erforderlich. Klicken Sie neben **DNS** auf das Abbrechen-Symbol.



7. Wählen Sie einen der Gründe für das Überschreiben der Empfehlung aus.



8. Klicken Sie auf **Überschreiben**.

   Damit legen Sie fest, wie die empfohlenen CDSS-Abonnements und ihre Verwendung auf Ihren Geräten angezeigt werden.

Weitere Informationen finden Sie unter Dashboard: Einführung von CDSS.

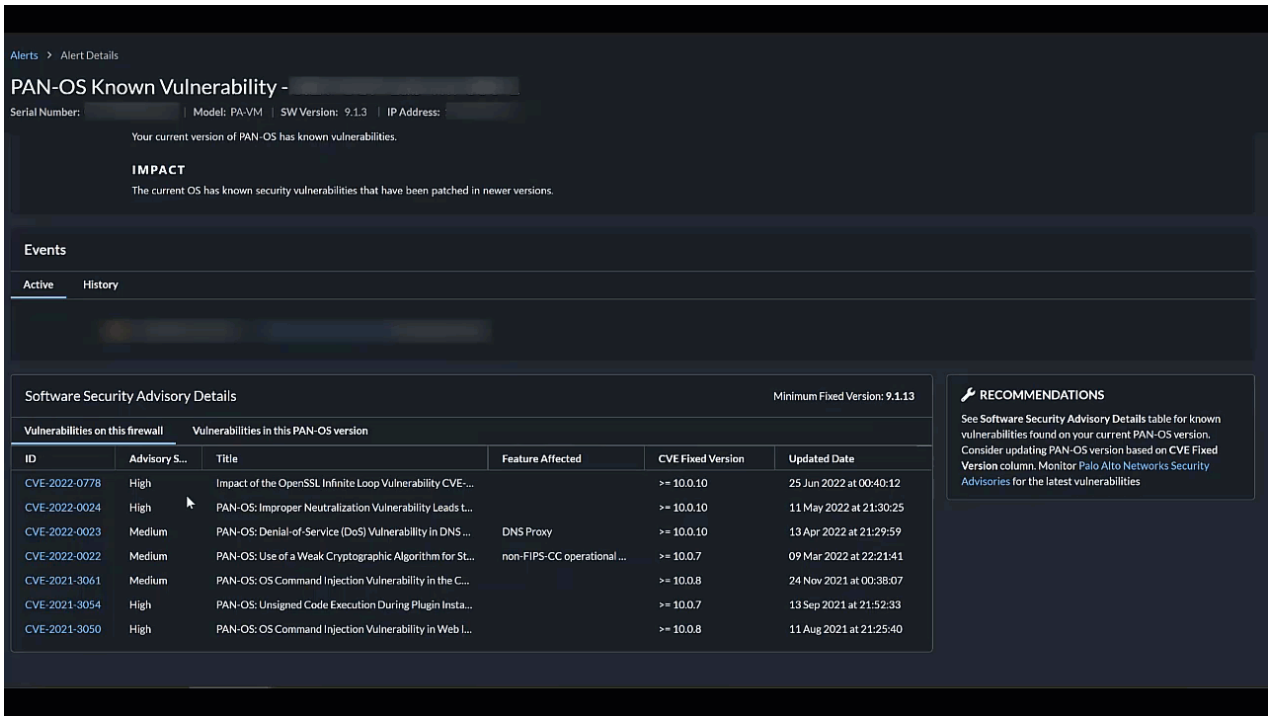
Bewerten von Sicherheitslücken

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

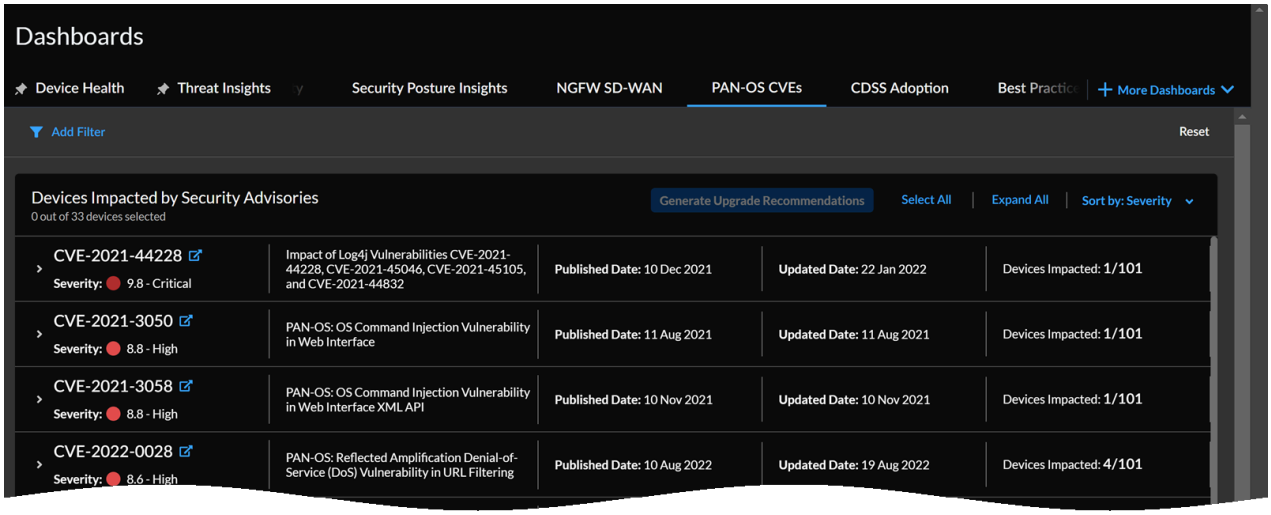
Strata Cloud Manager zeigt Ihnen, welche Sicherheitslücke eine bestimmte Firewall und PAN-OS-Version betreffen, um Ihnen bei der Entscheidung zu helfen, ob Sie ein Upgrade durchführen sollten. Navigieren Sie zu **Vorfälle und Benachrichtigungen** > **NGFW** > **Alle Alarme** und wählen Sie die Benachrichtigung **Bekannte Sicherheitslücken in PAN-OS** aus, um die neuesten Sicherheitshinweise anzuzeigen, die sich auf die Firewall auswirken, die die Benachrichtigung ausgelöst hat.

Wählen Sie **Sicherheitslücken in dieser PAN-OS-Version** aus, um die betroffene Funktion für eine Sicherheitslücke in der Spalte **Betroffene Funktion** anzuzeigen. Auf diese Weise können Sie anhand der Sicherheitslücke und ihrer Auswirkungen auf Ihre aktivierte Funktion besser entscheiden, ob eine Firewall aktualisiert werden soll. Wenn einer Funktion kein CVE zugeordnet ist, ist der Wert unter **Betroffene Funktion** leer. Dieser CVE-Typ betrifft die Firewall mit dem angegebenen Modell oder der angegebenen Version.

Standardmäßig zeigt die Benachrichtigung **Bekannte Sicherheitslücken in PAN-OS** alle Sicherheitslücken in der PAN-OS-Version auf dem Gerät an. Wenn Sie jedoch die Telemetrie zur Produktnutzung auf der Firewall aktiviert haben, können Sie festlegen, dass nur die Sicherheitslücken angezeigt werden, die die jeweilige Firewall basierend auf den aktivierten Funktionen betreffen. Auf diese Weise können Sie besser erkennen, welche Sicherheitslücken ein Problem für die Firewall darstellen, und eine fundiertere Entscheidung darüber treffen, ob ein Upgrade durchgeführt werden soll.



Sie können auch das Dashboard **PAN-OS-CVEs** verwenden, das Ihnen abhängig von den auf den Geräten aktivierten Funktionen die Anzahl der von einer bestimmten Sicherheitslücke betroffenen Geräte anzeigt. Strata Cloud Manager analysiert die aktivierten Funktionen, um die vom CVE betroffenen Geräte zu ermitteln. Die folgende Aufgabe zeigt, wie Sie Sicherheitslücken, die sich auf Geräte auswirken, bewerten und Upgrade-Empfehlungen zum Beheben der Sicherheitslücken erstellen.



Diese Aufgabe zeigt, wie Sie Sicherheitslücken, die sich auf Geräte auswirken, bewerten und Upgrade-Empfehlungen zum Beheben der Sicherheitslücken erstellen.

STEP 1 | Navigieren Sie im Strata Cloud Manager zu **Dashboards** > **PAN-OS-CVEs**.

STEP 2 | Erweitern Sie einen CVE, um die betroffenen Geräte anzuzeigen.

STEP 3 | Wählen Sie Geräte aus, die Sie aktualisieren möchten, um die Sicherheitslücken zu beheben.

STEP 4 | **Generieren von Upgrade-Empfehlungen**

STEP 5 | Klicken Sie auf den neu generierten Bericht für die Geräte.

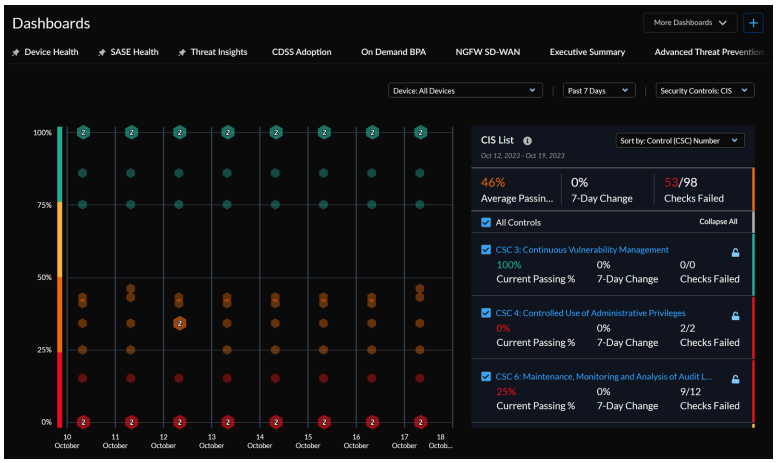
STEP 6 | Wählen Sie eine der Upgrade-Optionen aus, um Details zu **neuen Funktionen**, **bekannten Sicherheitslücken in PAN-OS**, **Verhaltensänderungen** und **bekannten Probleme in PAN-OS** anzuzeigen.

Sie können die Details in eine CSV-Datei **exportieren** und diese herunterladen.

Überwachen der Konformitätszusammenfassung

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	❑ oder ❑ Lizenz zum Anzeigen der Daten von unterstützten Produkten im Dashboard: Prisma Access

Um zum Dashboard „Zusammenfassung der Konformität“ zu gelangen, gehen Sie zu **Dashboards** und wählen Sie dann die Registerkarte **Zusammenfassung der Konformität** aus. Sie können den Änderungsverlauf der Sicherheitsüberprüfungen anzeigen, die vor bis zu 12 Monaten vorgenommen wurden, zusammengefasst nach den CIS- (Center for Internet Security) und NIST-Frameworks (National Institute of Standards and Technology). Für jedes Framework wird eine Liste mit Kontrollen sowie der Prozentsatz der aktuellen und durchschnittlichen Konformitätsrate, die Gesamtzahl der Best Practice-Überprüfungen sowie die Anzahl der fehlgeschlagenen Prüfungen für jede Kontrolle angezeigt. Interagieren Sie mit dem Diagramm und der Liste, um den Zusammenhang zwischen Kontrollen und ihren Verlaufsstatistiken zu sehen. Zeigen Sie Details zu einzelnen Kontrollen und den zugehörigen Prüfungen an, und wählen Sie eine Best Practice-Überprüfung aus, um die Firewall-Konfiguration anzuzeigen, bei der die Prüfung fehlschlägt. **Das CIS Critical Security Controls**-Framework ist eine priorisierte Reihe empfohlener Aktionen und Best Practices, die zum Schutz von Organisationen und ihrer Daten vor bekannten Cyberangriffsvektoren beitragen.



Sie können Prüfzusammenfassungen für 11 der 16 Basis- und grundlegenden CIS-Kontrollen anzeigen:

- CSC 3: Kontinuierliches Sicherheitsrisikomanagement
- CSC 4: Kontrollierte Nutzung von Administratorrechten
- CSC 6: Pflege, Überwachung und Analyse von Auditierungslogs
- CSC 7: E-Mail- und Webbrowser-Schutz
- CSC 8: Malware-Abwehr

- CSC 9: Beschränkung und Kontrolle von Netzwerkports, Protokollen und Diensten
- CSC 11: Sichere Konfiguration für Netzwerkgeräte wie Firewalls, Router und Switches
- CSC 12: Grenzverteidigung
- CSC 13: Datenschutz
- CSC 14: Kontrollierter Zugriff basierend auf dem Need-to-Know-Prinzip
- CSC 16: Kontoüberwachung und #kontrolle

Das **NIST Cybersecurity Framework SP 800-53 Controls** bietet Bundesbehörden und anderen Organisationen Leitlinien zur Implementierung und Aufrechterhaltung von Sicherheits- und Datenschutzkontrollen für ihre Informationssysteme. Sie können Prüfzusammenfassungen für acht Familien von NIST-Kontrollen anzeigen:

- SC: Zugriffssteuerung
- AU: Auditing und Rechenschaftspflicht
- CM: Verwaltung der Konfiguration
- CP: Notfallplanung
- IA: Identifizierung und Authentifizierung
- RA: Risikobewertung
- SC: System- und Kommunikationsschutz
- SI: System- und Informationsintegrität

Weitere Informationen finden Sie unter Dashboard: Zusammenfassung der Konformität.

Proaktives Durchsetzen von Sicherheitsüberprüfungen

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	❑ oder

Sie können die Sicherheitsstatusprüfungen für Ihre Bereitstellung anpassen, um mithilfe der folgenden Funktionen die relevanten Empfehlungen zu maximieren.

- **Sicherheitsprüfungen**

  Liste der Best Practice-Prüfungen, die AIOps für NGFW verwendet, um Ihre Konfiguration auszuwerten. Die Konfiguration von Firewalls und Panorama wird mit den Best Practice-Überprüfungen von Palo Alto Networks verglichen, um den Sicherheitsstatus Ihrer Geräte zu bewerten und Sicherheitsbenachrichtigungen zu generieren. Sie können eine Liste der Best Practice-Überprüfungen anzeigen, die zur Bewertung Ihrer Konfiguration verwendet werden.

  Hier haben Sie folgende Möglichkeiten:

  1. Legen Sie den Schweregrad für Prüfungen fest, um die Prüfungen zu bestimmen, die für Ihre Bereitstellung am kritischsten sind.
  2. Deaktivieren Sie Prüfungen vorübergehend.

     Wenn Sie eine Prüfung deaktivieren, können Sie angeben, wie lange sie deaktiviert bleiben soll, und einen Kommentar mit dem Grund für die Deaktivierung hinzufügen.
  3. Legen Sie die Reaktion für den Fall einer fehlgeschlagenen Prüfung fest.
- **Zone-zu-Rolle-Zuordnung**

  Ordnen Sie die Zonen in NGFWs Rollen zu, um benutzerdefinierte Empfehlungen zu erhalten.
- **Rolle-zu-Sicherheitsdienst-Zuordnung**

  Verwalten Sie die Sicherheitsdienste, die für den Datenverkehr zwischen Zonen und Rollen in allen NGFWs erforderlich sind.

Das Panorama CloudConnector-Plug-in ermöglicht Ihnen, proaktiv gegen suboptimale Konfigurationen vorzugehen, indem Sie Commits blockieren, die bestimmte Best Practice-Überprüfungen nicht bestehen. Wenn Sie in AIOps for NGFW angeben, dass für eine Prüfung der **Commit fehlschlagen** soll, blockiert Panorama automatisch Commits aller Konfigurationen, die diese Prüfung nicht bestehen. Anstatt auf eine Benachrichtigung zu einer fehlgeschlagenen Best Practice-Überprüfung zu warten, können Sie mit dem Plug-in von vornherein verhindern, dass bei Ihrer Bereitstellung Konfigurationsprobleme auftreten.

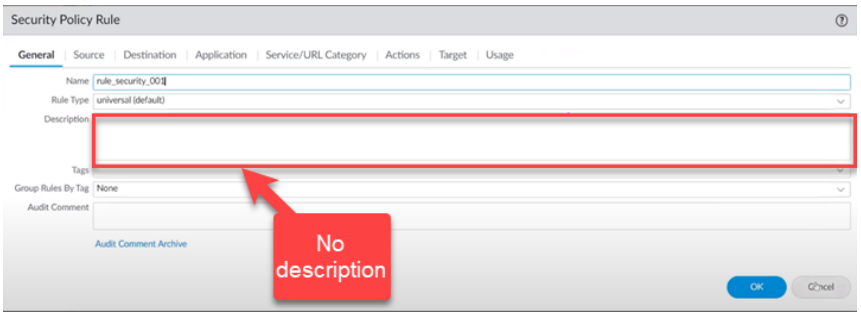
STEP 1 | Stellen Sie sicher, dass Sie alle Voraussetzungen erfüllen, und installieren Sie das Plug-in.

STEP 2 | Geben Sie die Best Practice-Überprüfungen an, die Commits bei Fehlern blockieren werden.

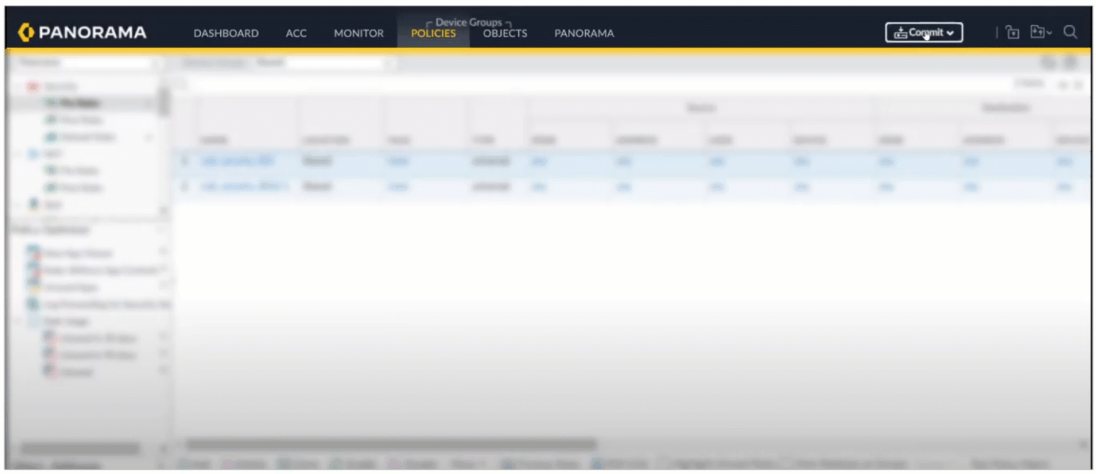
1. Wählen Sie **Verwalten** > **Sicherheitsstatus** > **Einstellungen** aus.
2. Suchen Sie die Prüfung, die Commits blockieren soll.
3. Legen Sie **Aktion bei Fehler** auf **Commit fehlgeschlagen** fest

STEP 3 | Überprüfen Sie dies, indem Sie versuchen, eine Konfiguration zu übernehmen, die die Prüfung nicht besteht.

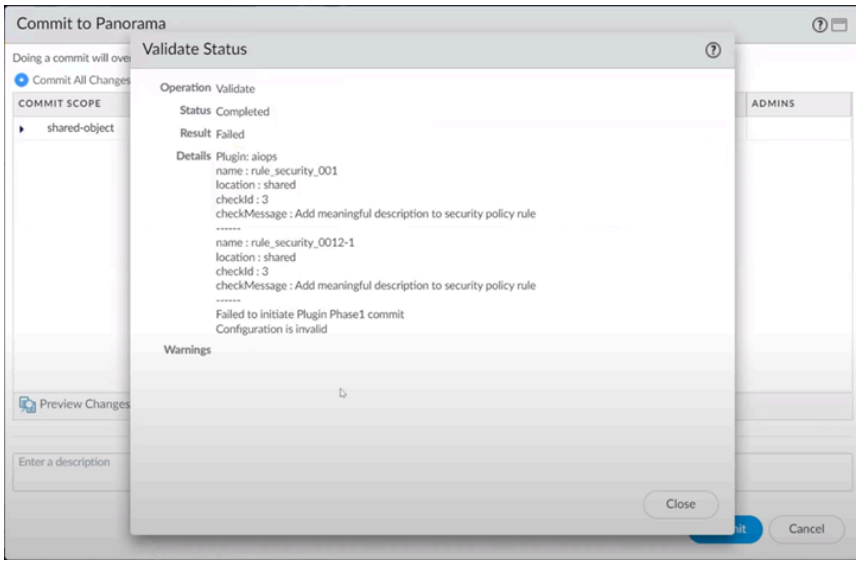
1. Melden Sie sich bei Panorama an.
2. Verletzen Sie die von Ihnen angegebene Best Practice-Überprüfung, die zum **Fehlschlagen eines Commits** führen soll.



3. Wählen Sie **Commit** > **Commit in Panorama** > **Konfiguration validieren** aus.



Es sollte ein Dialogfeld angezeigt werden, in dem Sie darüber informiert werden, dass die Validierung fehlgeschlagen ist, da die Konfiguration die Best Practice-Überprüfung nicht bestanden hat.



*Wenn Sie eine Überprüfung auf **Commit fehlgeschlagen** festlegen, schlägt sowohl die Validierung als auch der eigentliche Commit-Vorgang fehl.*

Unter Verwalten: Einstellungen für den Sicherheitsstatus finden Sie weitere Informationen.

Richtlinienanalyse

Wo kann ich das verwenden?	Was brauche ich?
• NGFW (von Panorama verwaltet) • (von Panorama verwaltet) •	❑ oder ❑ Panorama CloudConnector-Plug-in für von Panorama verwaltete Bereitstellungen

Aktualisierungen Ihrer Sicherheitsrichtlinienregeln sind häufig zeitkritisch und erfordern schnelles Handeln. Sie möchten jedoch sicherstellen, dass alle Aktualisierungen Ihres Regelsatzes für Sicherheitsrichtlinien Ihren Anforderungen entsprechen und keine Fehler oder Fehlkonfigurationen verursachen (z. B. Änderungen, die zu doppelten oder widersprüchlichen Regeln führen).

Die Richtlinienanalyse im Strata Cloud Manager ermöglicht Ihnen die Optimierung von Zeit und Ressourcen bei der Implementierung einer Änderungsanforderung. Die Richtlinienanalyse dient nicht nur dem Analysieren und Bereitstellen von Vorschlägen für eine mögliche Konsolidierung oder Entfernung bestimmter Regeln, um Ihren Absichten zu entsprechen, sondern sucht in Ihrem Regelsatz auch nach Anomalien wie Schatten, Redundanzen, Verallgemeinerungen, Korrelationen und Konsolidierungen.

Verwenden Sie die Richtlinienanalyse, um den Regelsatz Ihrer Sicherheitsrichtlinien zu ergänzen oder zu optimieren.

- **Vor dem Hinzufügen einer neuen Regel** – Prüfen Sie, ob neue Regeln hinzugefügt werden müssen. Die Richtlinienanalyse empfiehlt, wie Sie Ihre vorhandenen Sicherheitsrichtlinienregeln am besten ändern, um Ihre Anforderungen zu erfüllen und, sofern möglich, eine weitere Regel hinzuzufügen.
- **Optimierung Ihres vorhandenen Regelsatzes** – Finden Sie heraus, wo Sie Ihre Regeln aktualisieren können, um eine aufgeblähte Struktur zu vermeiden, Konflikte zu vermeiden und sicherzustellen, dass die Datenverkehrsüberwachung mit der Absicht Ihres Regelsatzes für die Sicherheitsrichtlinien übereinstimmt.

Analysieren Sie Ihre Sicherheitsrichtlinienregeln sowohl vor als auch nach dem Durchführen eines Commits für Ihre Änderungen.

- **Richtlinienanalyse vor Änderung** – Ermöglicht Ihnen, die Auswirkung einer neuen Regel zu bewerten und die Absicht der neuen Regeln im Vergleich zu den bereits vorhandenen Regeln zu analysieren, um Empfehlungen zu geben, wie die Absicht am besten erreicht werden kann.
- **Richtlinienanalyse nach Änderung** – Ermöglicht Ihnen, den vorhandenen Regelsatz zu bereinigen, indem Sie Schatten, Redundanzen und andere Anomalien identifizieren, die sich im Laufe der Zeit angesammelt haben.

- *Für die Richtlinienanalyse ist das CloudConnector-Plug-in 1.1.0 oder höher auf Ihrer Panorama-Appliance erforderlich. Sie müssen dieses Plug-in mit dem folgenden Befehl aktivieren:*

  ```
  > request plugins cloudconnector enable basic
  ```

- *Für die Richtlinienanalyse ist eine Aktualisierung von Panorama auf PAN-OS Version 10.2.3 oder eine spätere Version erforderlich.*

Von der Richtlinienanalyse erkannte Anomalietypen

Die Richtlinienanalyse erkennt die folgenden Arten von Anomalien in Ihrem Regelsatz für Sicherheitsrichtlinien:

- Schatten – Regeln, die nicht eingehalten werden, weil eine Regel weiter oben im Regelsatz denselben Datenverkehr abdeckt.

  Sicherheitsrichtlinienregeln werden im Regelsatz von oben nach unten ausgewertet, sodass Schatten erstellt werden, wenn eine im Regelsatz weiter oben stehende Regel auf denselben Datenverkehr zutrifft wie eine weiter unten stehende Regel, und die Regeln mit einer anderen Aktion konfiguriert sind. Wenn Sie die weiter unten stehende Regel entfernen, ändert sich die Sicherheitsrichtlinie nicht.
- Redundanzen – Zwei oder mehr Regeln, die auf denselben Datenverkehr zutreffen und mit derselben Aktion konfiguriert sind.
- Verallgemeinerungen – Wenn eine Regel weiter unten im Regelsatz mit dem Datenverkehr einer Regel weiter oben im Regelsatz übereinstimmt, aber nicht umgekehrt, und die Regeln jeweils eine andere Aktion ausführen. Wird die Reihenfolge der beiden Richtlinienregeln umgekehrt, wirkt sich dies auf die Sicherheitsrichtlinie aus.
- Korrelationen – Regeln, die mit einer anderen Regel korrelieren, wenn eine Regel mit einigen Paketen der anderen Regel übereinstimmt, aber zu einer anderen Aktion führt. Wird die Reihenfolge der beiden Regeln umgekehrt, hat dies Auswirkungen auf die Sicherheitsrichtlinie.
- Konsolidierungen – Regeln, die Sie zu einer einzigen Regel konsolidieren können, da die Aktion dieselbe ist und sich nur ein Attribut unterscheidet. Sie können die Regeln zu einer einzigen Regel zusammenführen, indem Sie die Attribute einer der Regeln ändern und die anderen Regeln löschen.

Richtlinienanalyse vor Änderung

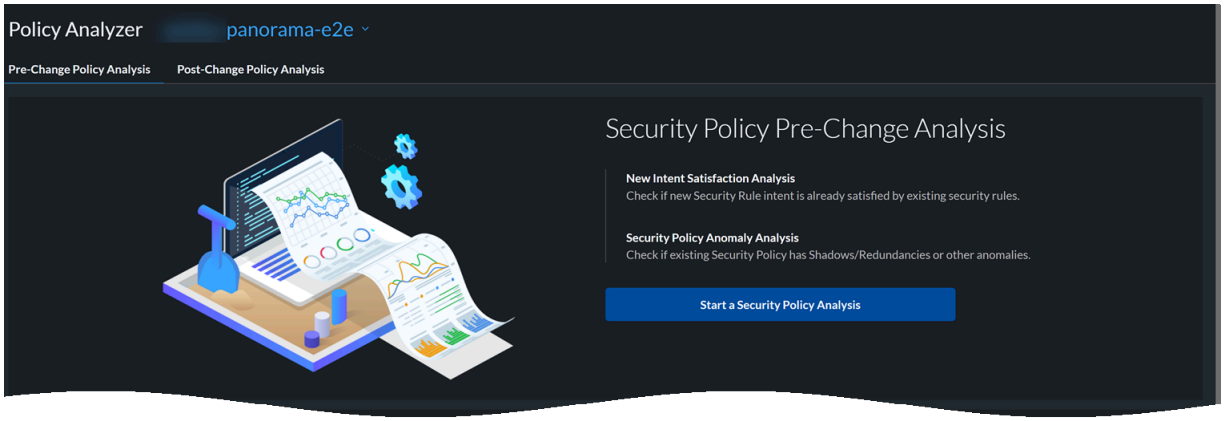
Wo kann ich das verwenden?	Was brauche ich?
• NGFW (von Panorama verwaltet) • (von Panorama verwaltet) •	❑ oder ❑ Panorama CloudConnector-Plug-in für von Panorama verwaltete Bereitstellungen

Die Richtlinienanalyse vor Änderungen führt die neue Analyse der Absichtszufriedenheit aus:

- **Neue Analyse der Absichtszufriedenheit** – Überprüft, ob die Absicht einer neuen Sicherheitsrichtlinienregel bereits von einer vorhandenen Regel abgedeckt wird.

Bevor Sie beginnen:

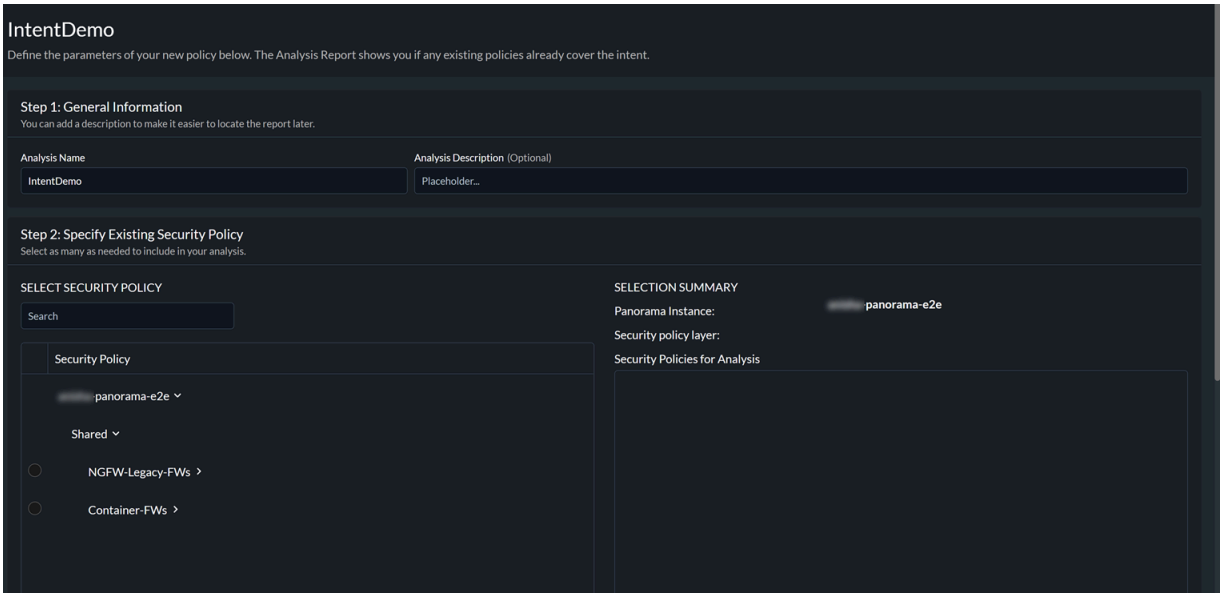
1. Gehen Sie zu **Verwalten** > **Sicherheitsstatus** > **Richtlinienanalyse** > **Richtlinienanalyse vor Änderung**.
2. Wählen Sie oben auf der Seite „Richtlinienanalyse“ die Panorama-Instanz aus, die die Richtlinienregeln enthält, die Sie analysieren müssen.



3. **Starten Sie eine Analyse der Sicherheitsrichtlinien**.

Führen Sie die folgenden Schritte aus, um eine neue Analyse zu starten:

STEP 1 | Geben Sie den **Namen der Analyse** und die **Beschreibung der Analyse** ein.



Auf einer Panorama-Appliance sind Gerätegruppen hierarchisch angeordnet. Sie können vier Ebenen von Gerätegruppen erstellen und Sie weisen NGFWs der Gerätegruppe auf der untersten Hierarchieebene zu. Die Richtlinie, die Sie auf einer höheren Ebene erstellen, wird dann von allen untergeordneten Gerätegruppen übernommen.

Sie können die Analyse für bis zu zehn Gerätegruppen ausführen, denen NGFWs direkt zugewiesen sind. Auf diese Weise können Sie alle Richtlinienregeln analysieren, die per Push an diesen Satz direkt zugewiesener NGFWs übertragen werden.

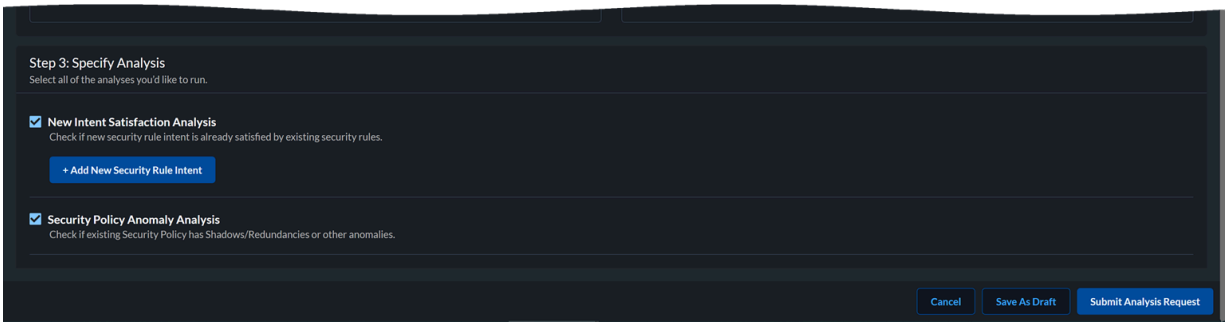
STEP 2 | Wählen Sie einen vorhandenen Sicherheitsrichtliniensatz zur Analyse aus.

Sie können maximal zehn Gerätegruppen pro Analyse auswählen.

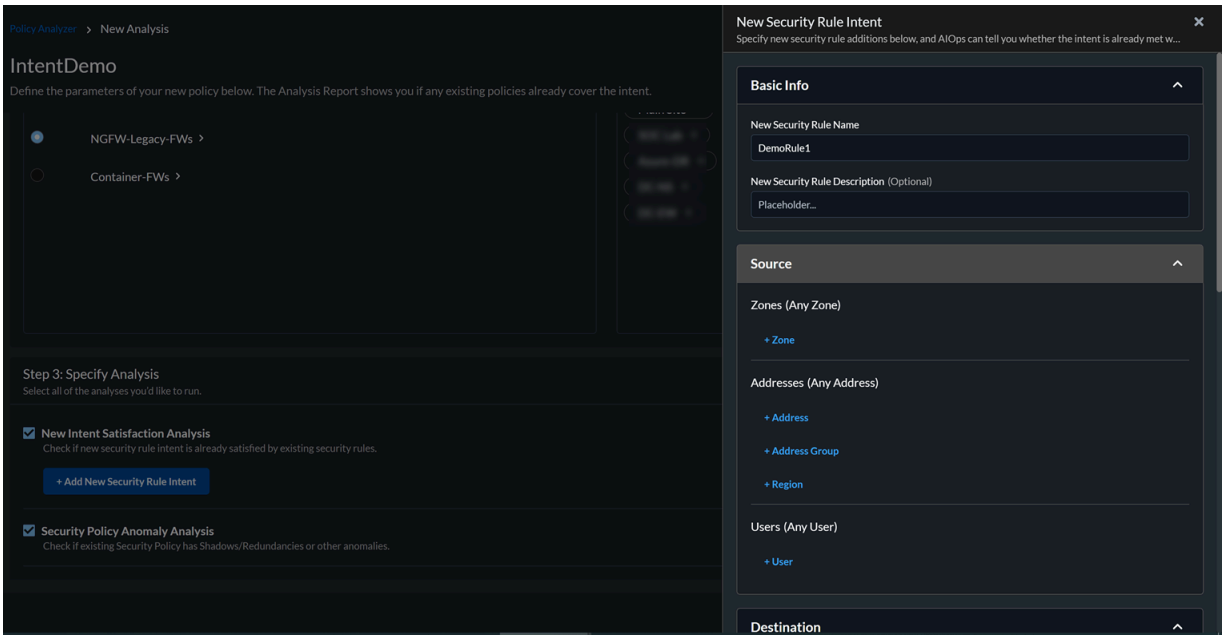
STEP 3 | Geben Sie den Analysetyp an, indem Sie einen oder mehrere Analysetypen auswählen:

- **Neue Analyse der Absichtszufriedenheit**

Fügen Sie eine neue Sicherheitsregelabsicht zur Analyse hinzu.



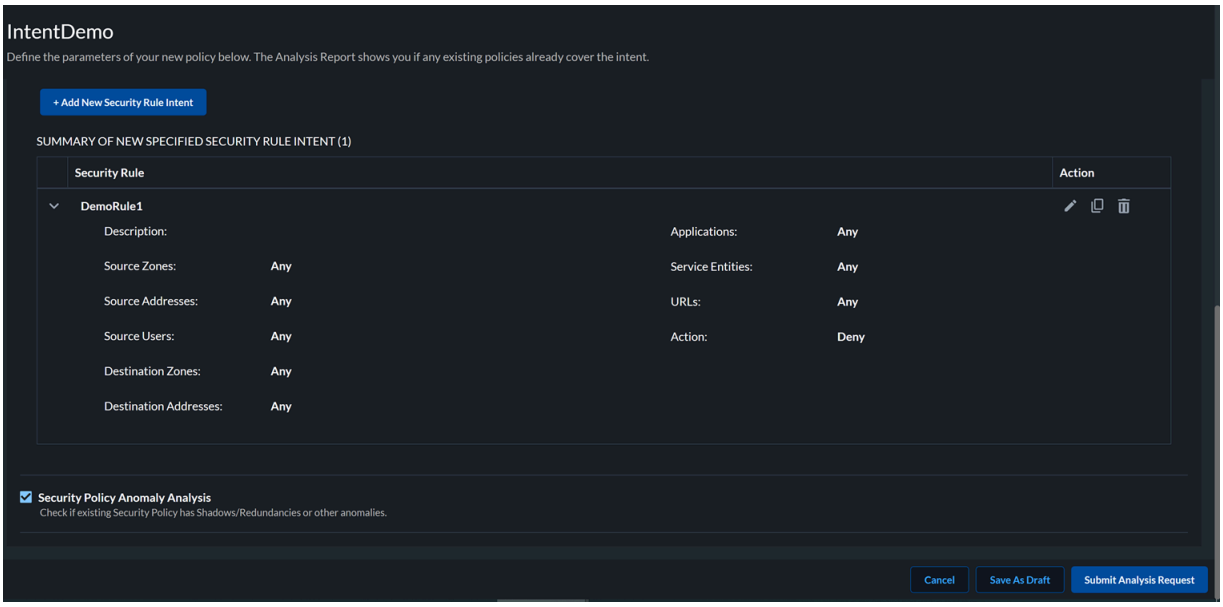
Geben Sie Informationen über die neue Sicherheitsregel an, damit AIOps for NGFW überprüfen kann, ob die bestehenden Regeln die Absicht abdecken.



Geben Sie die Werte für die Komponenten einer Sicherheitsrichtlinienregel ein. Der Standardwert für die Felder, die sich auf eine Sicherheitsregel beziehen, ist „Beliebige“.

Speichern Sie die Einstellungen.

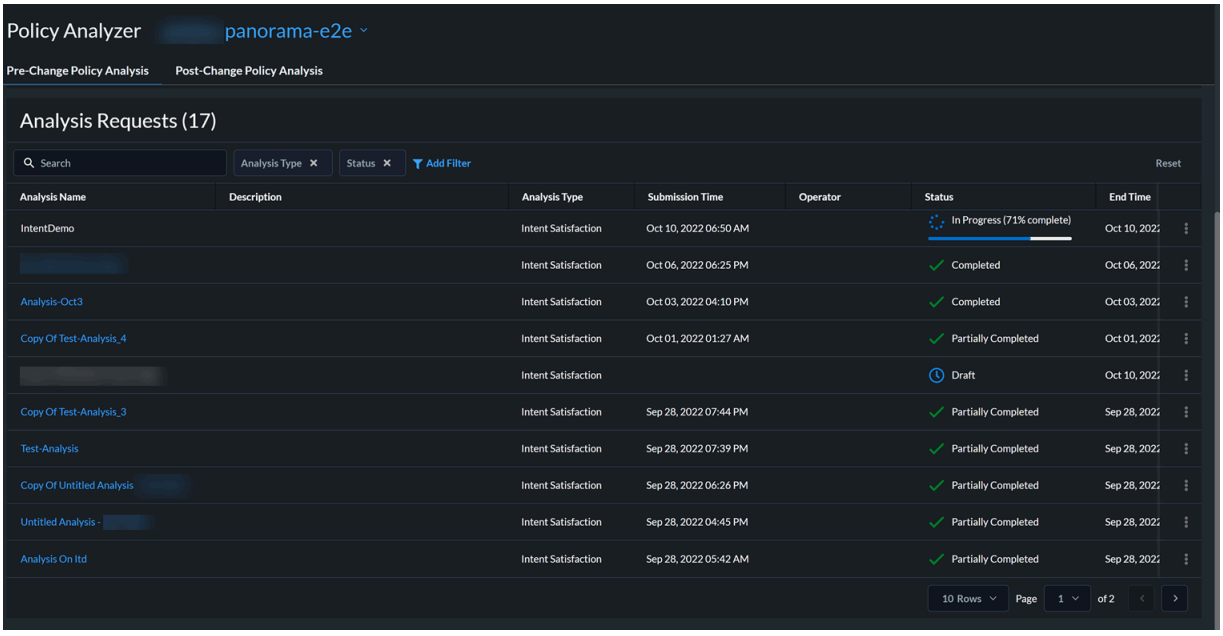
Überprüfen Sie die Zusammenfassung zur Absicht der neuen Sicherheitsregel.



Sie können bis zu zehn neue Sicherheitsregeln erstellen oder eine Regel kopieren und bearbeiten.

STEP 4 | **Übermitteln Sie die Analyseanfrage oder speichern Sie sie als Entwurf**, um die Regel später zu bearbeiten.

Sehen Sie sich den Status einer Analyse auf der Seite „Richtlinienanalyse“ unter „Analyseanforderungen“ an.



Sie können eine Regel, deren Status „In Bearbeitung“ lautet, stornieren. Daraufhin wird sie mit dem Status „Storniert“ angezeigt.

Sehen Sie sich nach Abschluss der Analyse den Analysebericht an.

Berichte zur Richtlinienanalyse vor Änderung

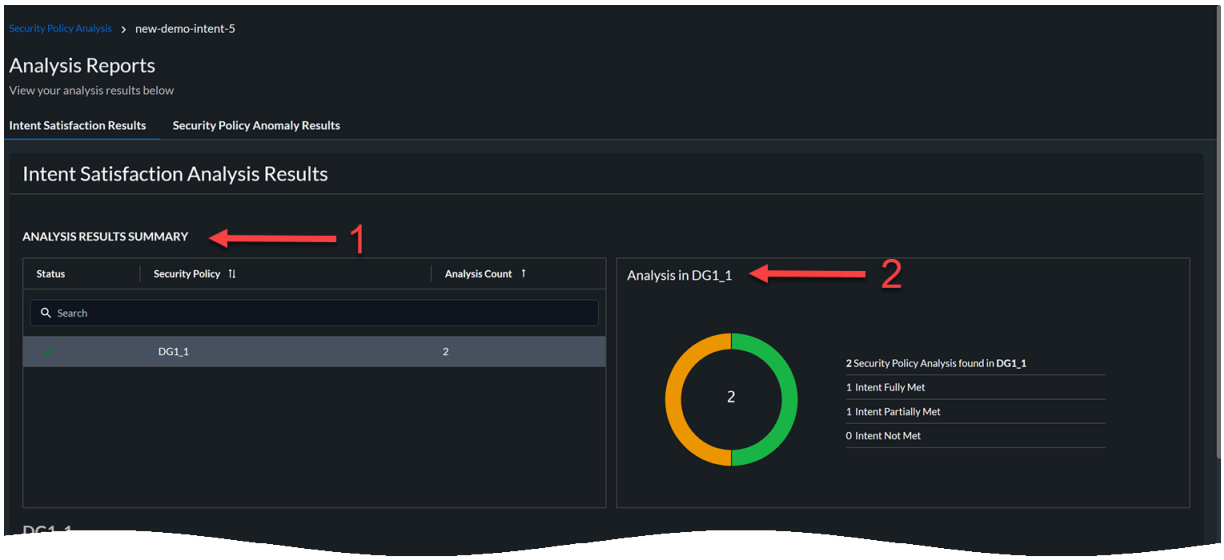
Wo kann ich das verwenden?	Was brauche ich?
• NGFW (von Panorama verwaltet) • (von Panorama verwaltet) •	❑ oder ❑ Panorama CloudConnector-Plug-in für von Panorama verwaltete Bereitstellungen

Wählen Sie einen Analysebericht mit dem Status „Abgeschlossen“ aus, um die Ergebnisse der Richtlinienanalyse anzuzeigen. Sie können sich die Ergebnisse der Analyse ansehen.

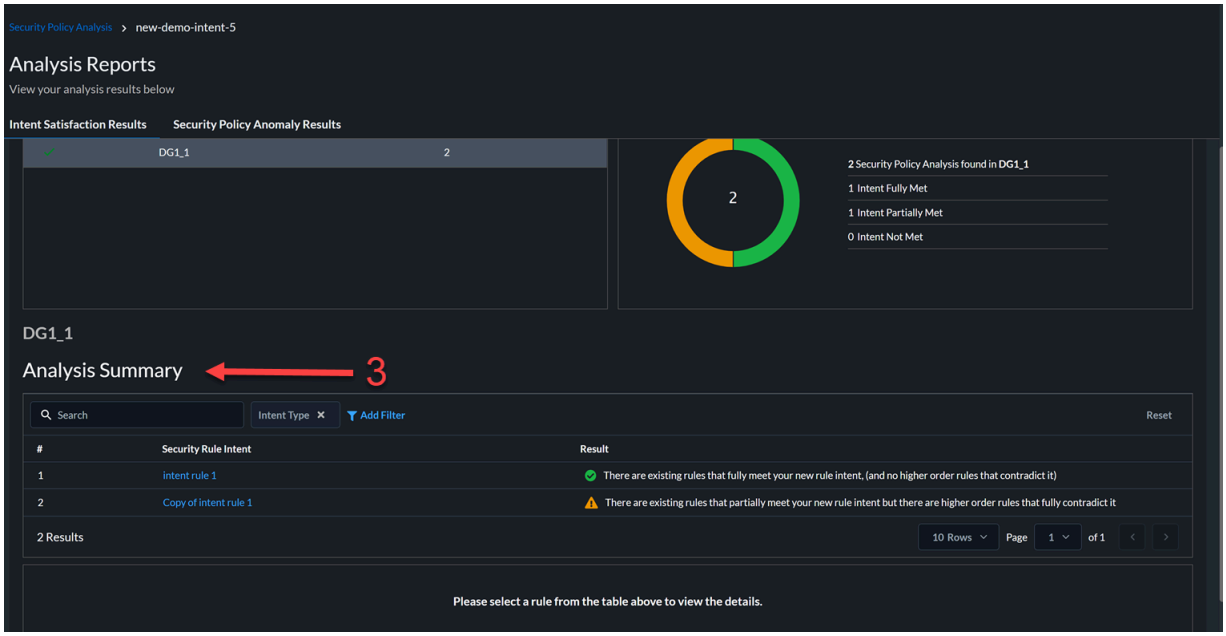
Ergebnisse zur Absichtszufriedenheit

Klicken Sie in der Liste der Analysen unter „Analyseanforderungen“ auf eine Analyse, um deren Analyseergebnisse anzuzeigen. Zu diesen Ergebnissen gehören:

1. Zusammenfassung der Analyse mit Details zu Gerätegruppen und Anomalieanzahl.
2. Klicken Sie auf den Namen einer Gerätegruppe, um das Ergebnis der Absichtszufriedenheitsanalyse anzuzeigen:
   - Absicht vollständig erfüllt – Ihre Sicherheitsregel ist ein Duplikat einer der vorhandenen Regeln in der Gerätegruppe.
   - Absicht teilweise erfüllt – Ihre Sicherheitsregel erfüllt die Absicht einer der vorhandenen Regeln in der Gerätegruppe teilweise.
   - Absicht nicht erfüllt – Ihre Sicherheitsregel ist eine eindeutige Regel, die in der Gerätegruppe nicht vorhanden ist. Sie können diese Regel der Gerätegruppe hinzufügen.

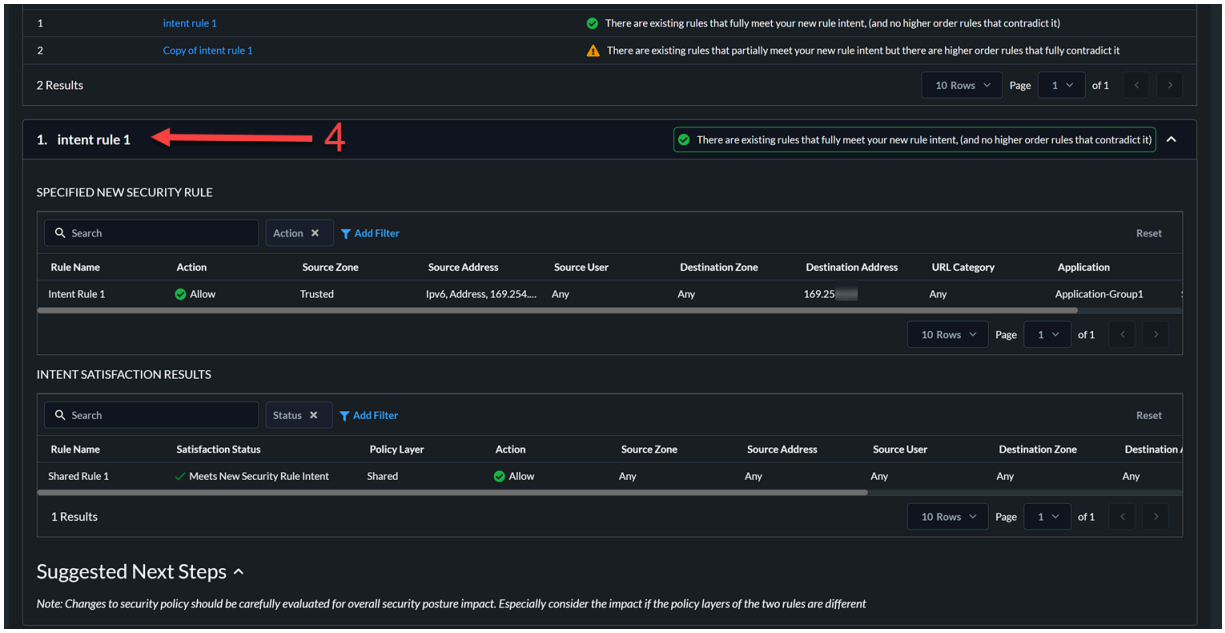


3. Zeigen Sie die Ergebnisse der Analyse für die neue Sicherheitsregelabsicht an.



In diesem Beispiel gibt es zwei Regeln. Die Absicht der ersten Regel stimmt vollständig mit den bestehenden Regeln überein und die Absicht der zweiten Regel stimmt teilweise mit den bestehenden Regeln überein.

4. Zeigen Sie die Details der neuen Sicherheitsregel an und überprüfen Sie die Ergebnisse zur Absichtszufriedenheit.



In diesem Beispiel stimmen alle Attribute der neuen Regel „Intent Rule 1“ mit den Attributen der vorhandenen Regel „Shared Rule 1“ überein. Die Absicht der neuen Regel entspricht vollständig der Absicht der bestehenden Regel. Daher müssen Sie diese neue Regel nicht zur Konfiguration hinzufügen.

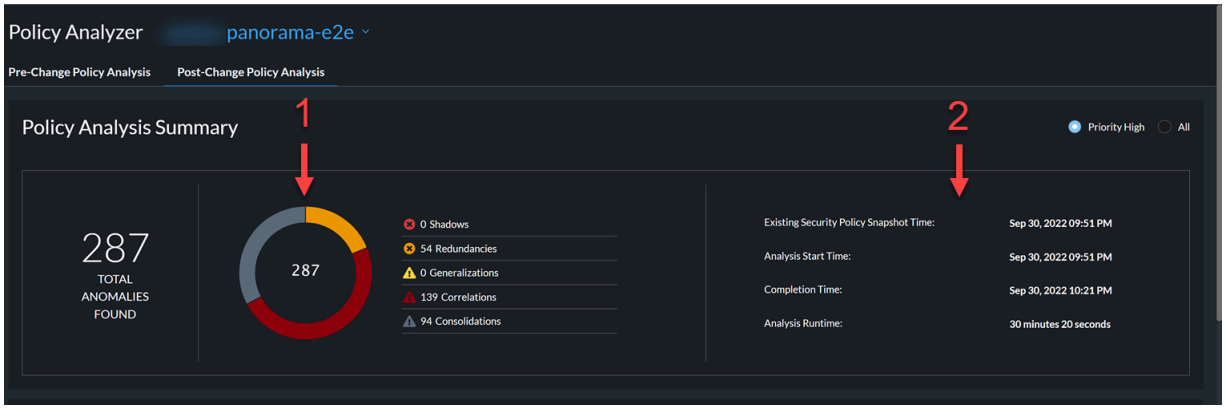
Richtlinienanalyse nach Änderung

Wo kann ich das verwenden?	Was brauche ich?
• NGFW (von Panorama verwaltet) • (von Panorama verwaltet) •	❑ oder ❑ Panorama CloudConnector-Plug-in für von Panorama verwaltete Bereitstellungen

Wenn Sie für eine Konfiguration einen Commit auf Panorama durchführen, steht sie über das Plug-in für Strata Cloud Manager zur Analyse zur Verfügung. Die Richtlinienanalyse analysiert diese Konfiguration auf Schatten, Redundanzen und andere Anomalien und die Ergebnisse stehen zur Überprüfung unter **Verwalten** > **Sicherheitsstatus** > **Richtlinienanalyse** > **Richtlinienanalyse nach Änderung** zur Verfügung.

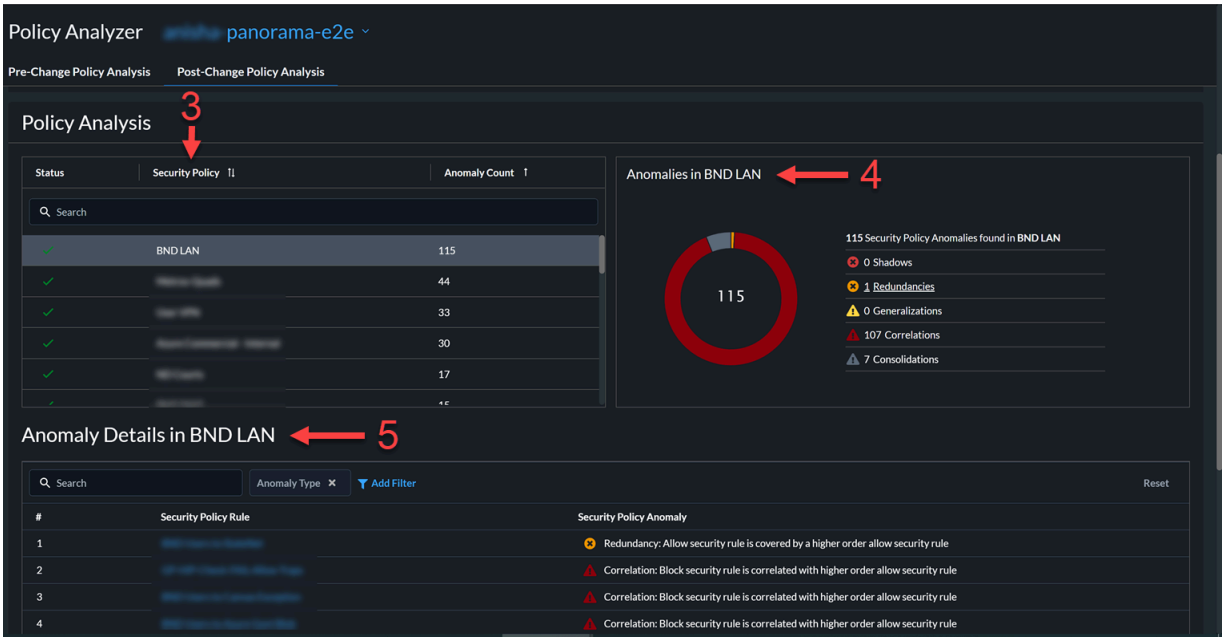
Sie können die folgenden Informationen anzeigen:

1. Es wird eine Zusammenfassung der Analyse aller Richtliniensätze angezeigt, d. h. aller Gerätegruppen, denen NGFWs direkt zugewiesen sind. Sie können alle Anomalien oder die Anomalien basierend auf hoher Priorität anzeigen. Die Werte in diesem Bericht geben die eindeutige Anzahl der in allen Gerätegruppen gefundenen Anomalien an. Die Farben im Diagramm zeigen die verschiedenen Anomalietypen an.

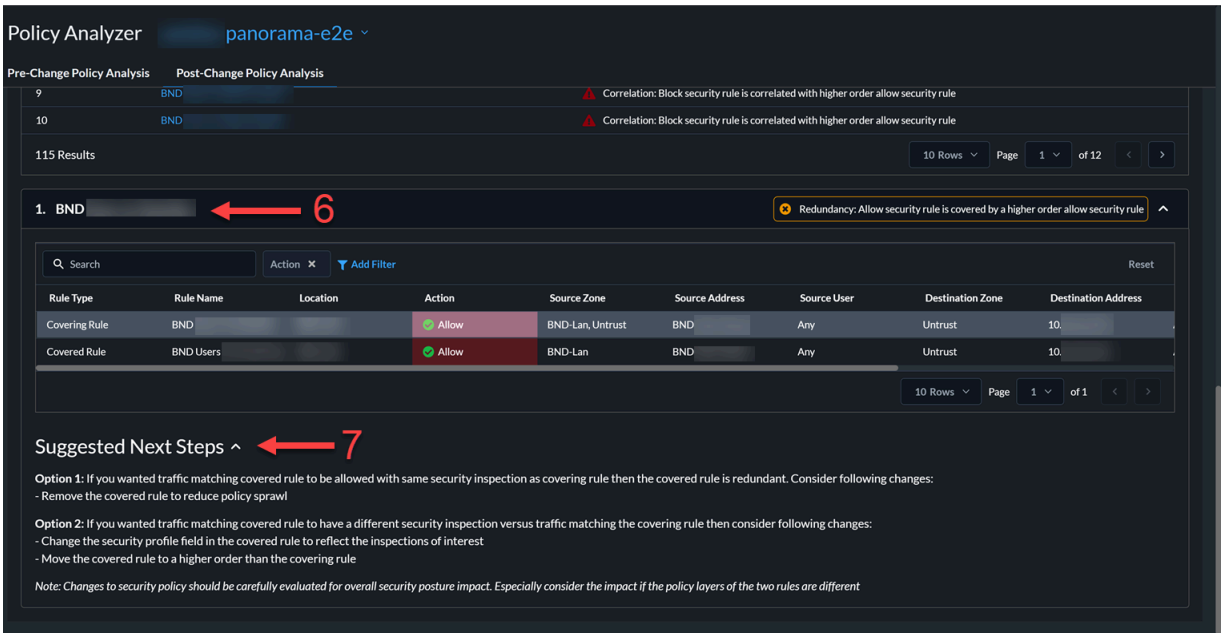


2. Zeitstempel für die Analyse, die Folgendes umfassen:
   - Vorhandener Snapshot der Sicherheitsrichtlinie – Zeitstempel des Zeitpunkts, an dem die Konfiguration nach einem Commit in Panorama als ausgeführt gekennzeichnet wurde.
   - Zeitpunkt des Analysebeginns
   - Zeitpunkt des Analyseabschlusses
   - Zeitaufwand für die Durchführung der Analyse
3. Anzeigen des Status der Sicherheitsrichtlinie und der Anzahl der Anomalien für jede Richtlinie.
4. Anzeigen einer Aufschlüsselung der Anomalien für eine ausgewählte Sicherheitsrichtlinie.

5. Anzeigen der Anomaliedetails für jede Regel in einer Sicherheitsrichtlinie.



6. Anzeigen der Attribute einer ausgewählten Regel und der Details zur Anomalie.



In dieser Abbildung ist ein Beispiel der Redundanzanomalie dargestellt. In diesem Beispiel wird die BND-Regel bereits durch eine andere BND-Benutzerregel abgedeckt. Daher können Sie die BND-Regel entfernen.

7. Anzeigen der vorgeschlagenen nächsten Schritte zur Behebung einer Anomalie.

Zustands- und Softwaremanagement für NGFWs

In diesem Kapitel wird beschrieben, wie Sie den Zustand und Software-Upgrades von NGFW verwalten.

- Gerätezustand anzeigen – Zeigen Sie den kumulativen Integritätsstatus und die Leistung Ihrer Bereitstellung basierend auf den Zustandsbewertungen der integrierten NGFWs an.
- Empfehlungen für Upgrade – Erstellen Sie Empfehlungen, um die beste Softwareversion für Ihre Geräte zu ermitteln, die aktualisiert werden kann.
- Analysieren der Metrikkapazität – Überwachen Sie die Ressourcenkapazität Ihrer Geräte, indem Sie die Nutzung von Metriken basierend auf ihren Modelltypen verfolgen.

Gerätezustand anzeigen

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Das Dashboard **Gerätezustand** zeigt Ihnen den kumulativen Integritätsstatus und die Leistung Ihrer Bereitstellung basierend auf den Zustandsbewertungen der integrierten NGFWs an. Der Gerätezustand wird durch den Schweregrad der Zustandsbewertung (0–100) und die entsprechende Zustandsnote (gut, angemessen, schlecht, kritisch) bestimmt. Die Zustandsbewertung wird anhand von Priorität, Anzahl, Art und Status der offenen Benachrichtigungen berechnet.

Dieses Dashboard unterstützt Sie dabei,

- die Verbesserungen bei der Bereitstellung, die Sie über einen bestimmten Zeitraum hinweg vorgenommen haben, anhand der historischen Daten zur Zustandsbewertung zu verstehen.
- die Geräte in Ihrer Bereitstellung, die Aufmerksamkeit erfordern, einzugrenzen und Prioritäten für die Fehlerbehebung festzulegen.

Weitere Informationen finden Sie unter Dashboard: Gerätezustand.

Erhalten von Upgrade-Empfehlungen

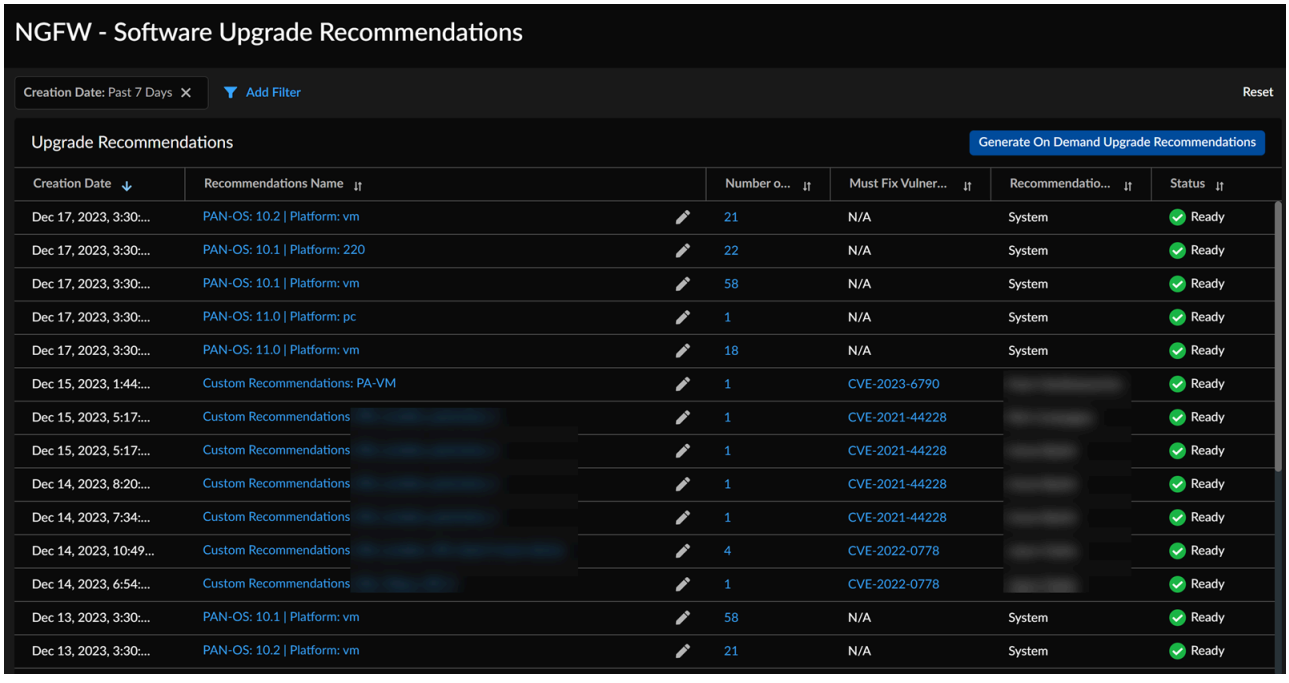
Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	❑ oder

Wählen Sie **Workflows** > **Software-Upgrades** > **Empfehlungen für Upgrade** aus, um mit Strata Cloud Manager die auf Ihren Firewalls aktivierten Funktionen zu analysieren und eine benutzerdefinierte Empfehlung zu erstellen, die spezifische Informationen für Ihr Netzwerk bereitstellt:

- Die beste Softwareversion für die Ausführung auf Ihren Geräten.
- Informationen zu neuen Funktionen, Verhaltensänderungen, Sicherheitslücken und Softwareproblemen in jeder empfohlenen Softwareversion.

Arten der Upgrade-Empfehlungen:

- Systemgenerierte Empfehlungen, die zweimal wöchentlich aus den Telemetriedaten des Geräts erstellt werden.
- Vom Benutzer erstellte, benutzerdefinierte Empfehlungen, die generiert werden, wenn Sie Geräte für bestimmte PAN-OS-CVEs auswählen.
- Benutzergenerierte Empfehlungen, die Sie durch Hochladen einer Datei für den technischen Support (Tech-Support-Datei, TSF) einer Firewall erstellen.



Sie können für jede Empfehlung folgende Aufgaben ausführen.

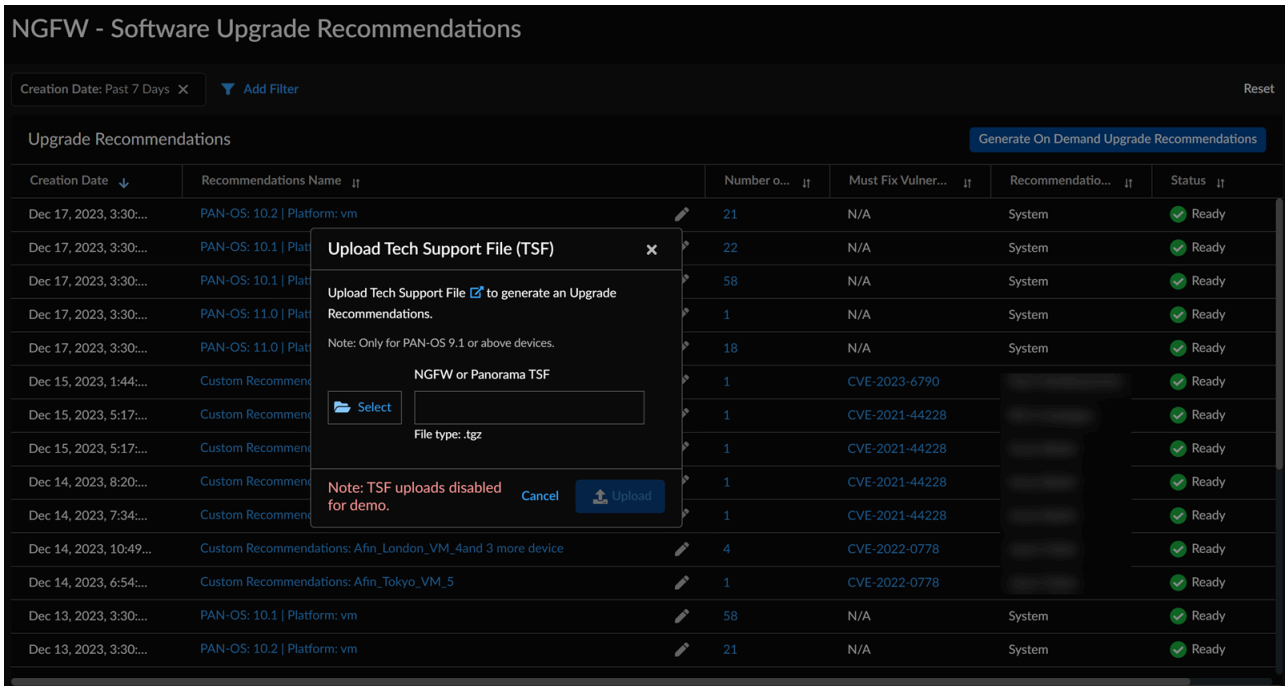
- Zeigen Sie die Anzahl der Geräte an, die ein Upgrade erfordern, und alle Schwachstellen, die Sie beheben müssen.

- Bearbeiten Sie den Namen einer Empfehlung, um zwischen benutzerdefinierten Empfehlungen zu unterscheiden.
- Filtern Sie die Empfehlungen nach „Erstellungsdatum“, „Empfehlungsname“ und „Empfehlungen generiert von“.
- Löschen Sie Empfehlungen, die fehlgeschlagen oder nicht mehr geeignet sind.

Generieren von Empfehlungen für On-Demand-Upgrades

1. **Generieren Sie Empfehlungen für On-Demand-Upgrades**.
2. **Wählen** Sie eine Datei für den technischen Support (Tech Support File, TSF) aus und **laden Sie sie hoch**.

   - *Sie können jeweils nur eine TSF-Datei von einem Gerät hochladen und die TSF-Datei muss im .tgz-Format vorliegen.*
   - *Sie können Empfehlungen für Software-Upgrades nur aus einer TSF-Datei generieren, die Sie für eine Firewall mit PAN-OS 9.1 oder einer späteren PAN-OS-Version generieren und von dieser hochladen.*



3. Sehen Sie sich die Empfehlungen zum Software-Upgrade an, sobald als Status „Bereit“ angezeigt wird.

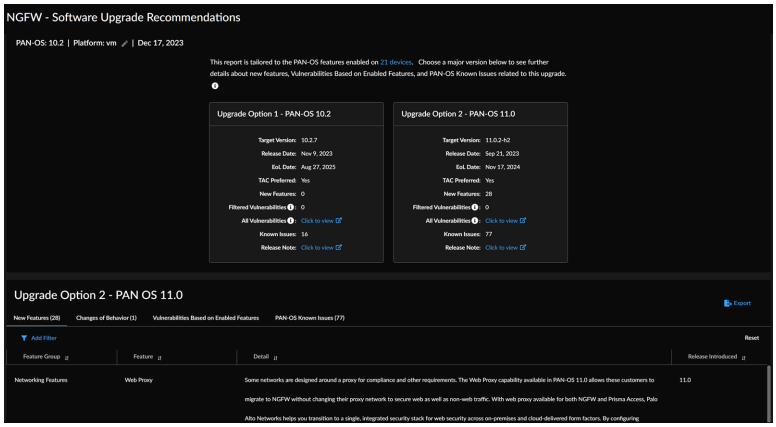
   Sie können den Status auch überprüfen, um festzustellen, ob Fehler im Zusammenhang mit dem Upload, dem Dateiformat oder der Verarbeitung der TSF-Datei vorliegen.

Anzeigen des Berichts mit Empfehlungen zum Software-Upgrade

Klicken Sie auf eine Empfehlung, um den ausführlichen Bericht mit den Upgrade-Optionen für Ihre Geräte anzuzeigen. Wählen Sie eine Upgrade-Option aus, um Details zu **neuen Funktionen**,

Verhaltensänderungen, **Sicherheitslücken aufgrund aktivierter Funktionen** und **bekannten Problemen in PAN-OS** anzuzeigen. Sie können diesen Bericht auch im CSV-Format **exportieren**.

- *Der Empfehlungsbericht enthält spezifische Informationen zu den aktivierten Funktionen auf Ihren Geräten.*
- *Bei **bekannten PAN-OS-Problemen** stellt die zugehörige Fallanzahl die Anzahl der Kunden dar, die das Problem gemeldet haben.*



Analysieren der Metrikkapazität

Wo kann ich das verwenden?	Was brauche ich?
•	❑ oder

Navigieren Sie vom Strata Cloud Manager zu **Überwachen** > **Kapazitätsanalyse**, um die Ressourcenkapazität Ihrer Geräte zu analysieren und zu überwachen, indem Sie deren Metriknutzung basierend auf ihren Modelltypen verfolgen. Sie können Metriken mit den folgenden Methoden analysieren:

- Analysieren der Metrikkapazität basierend auf Metrik, Modell und Gerät
- Analysieren der Metrikkapazität basierend auf Gerätemodellen
- Analysieren der Metrikkapazität basierend auf Metriken

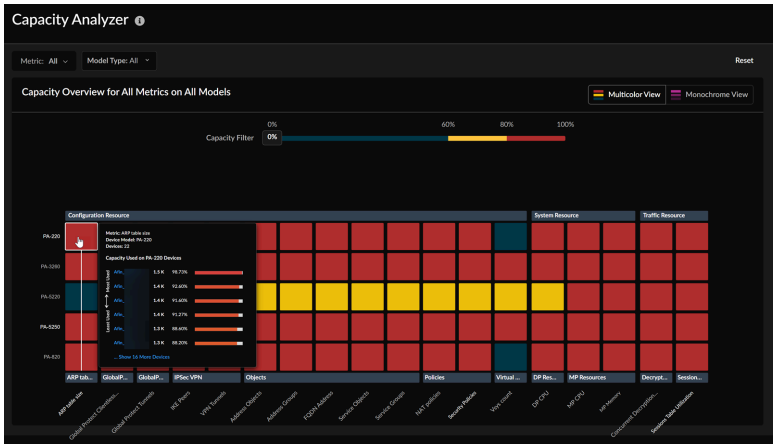
Die Kapazitätsanalyse wurde erweitert und unterstützt nun Benachrichtigungen, die Ihnen dabei helfen, die Annäherung des Ressourcenverbrauchs an seine maximale Kapazität vorherzusehen und Benachrichtigungen auszulösen. Siehe Verwalten von Kapazitätsanalysebenachrichtigungen.

*Die Funktion **Kapazitätsanalyse** wird für die Firewalls der VM-Series nicht unterstützt.*

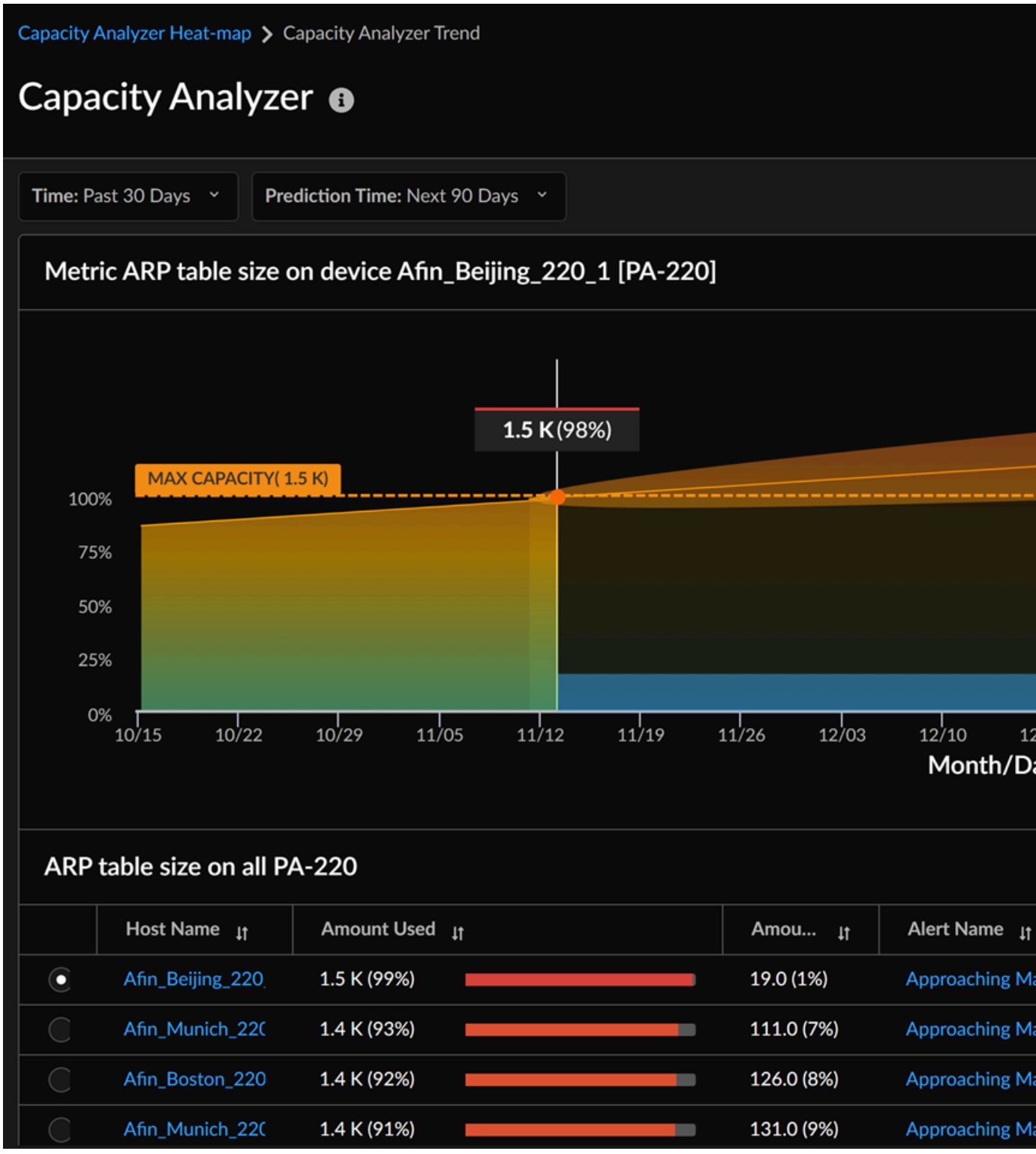
Analysieren der Metrikkapazität basierend auf Metrik, Modell und Gerät

1. Bewegen Sie den Cursor in der Heatmap der Kapazitätsanalyse über eine Zelle, um die Nutzung der Metrikkapazität für alle Geräte anzuzeigen, die zum entsprechenden Gerätemodell gehören.

   In diesem Beispiel zeigt das Pop-up-Fenster die Metrikkapazität **ARP-Tabellengröße** für alle Geräte an, die zum Modell **PA-220** gehören.



2. Klicken Sie auf eine Zelle, die dem Gerätemodell und der Metrik entspricht, um die Kapazitätsnutzung zu überprüfen. In diesem Beispiel wird auf die ARP-Tabellengröße für das Gerätemodell **PA-220** geklickt.



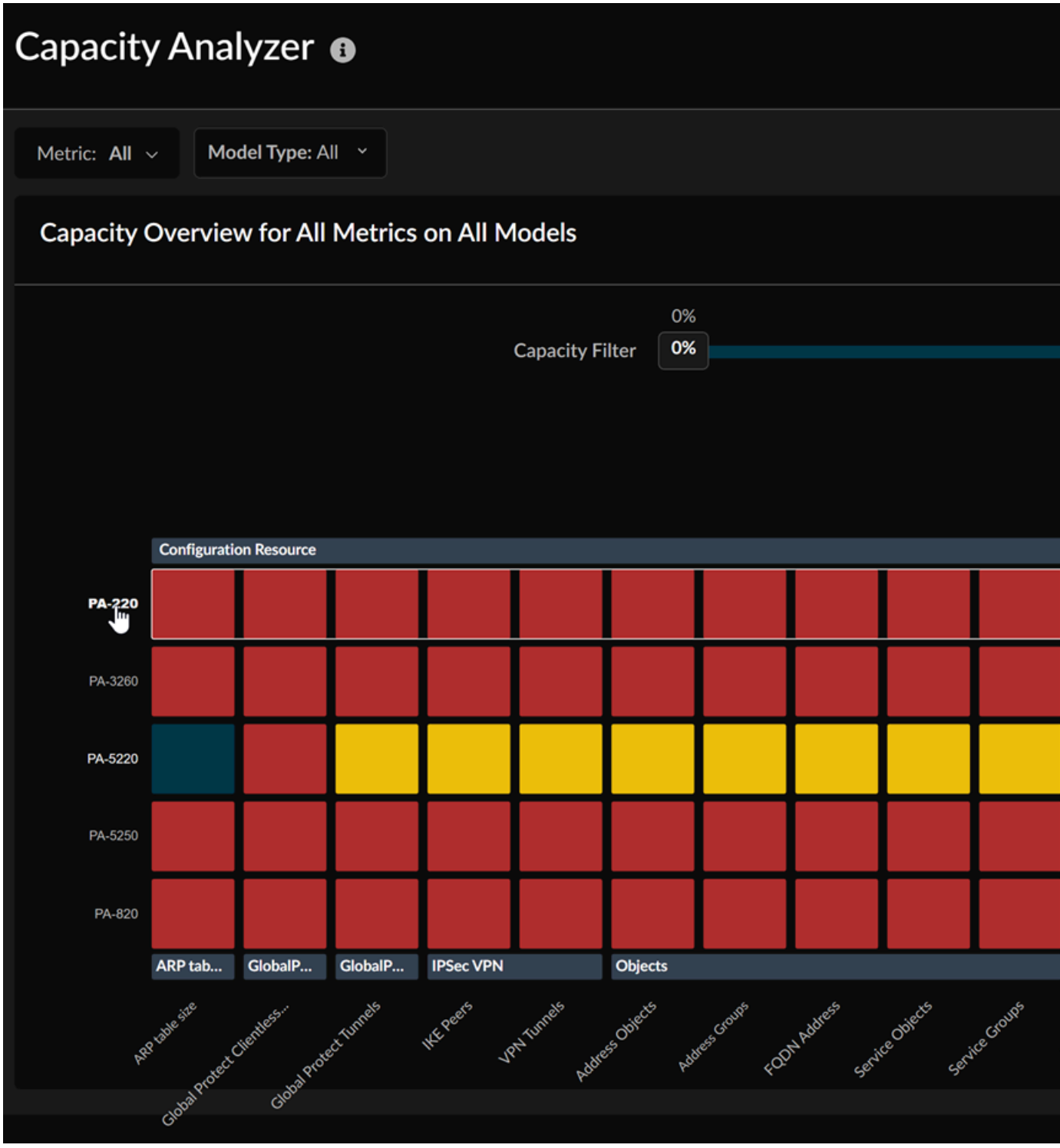
Es wird Folgendes angezeigt:

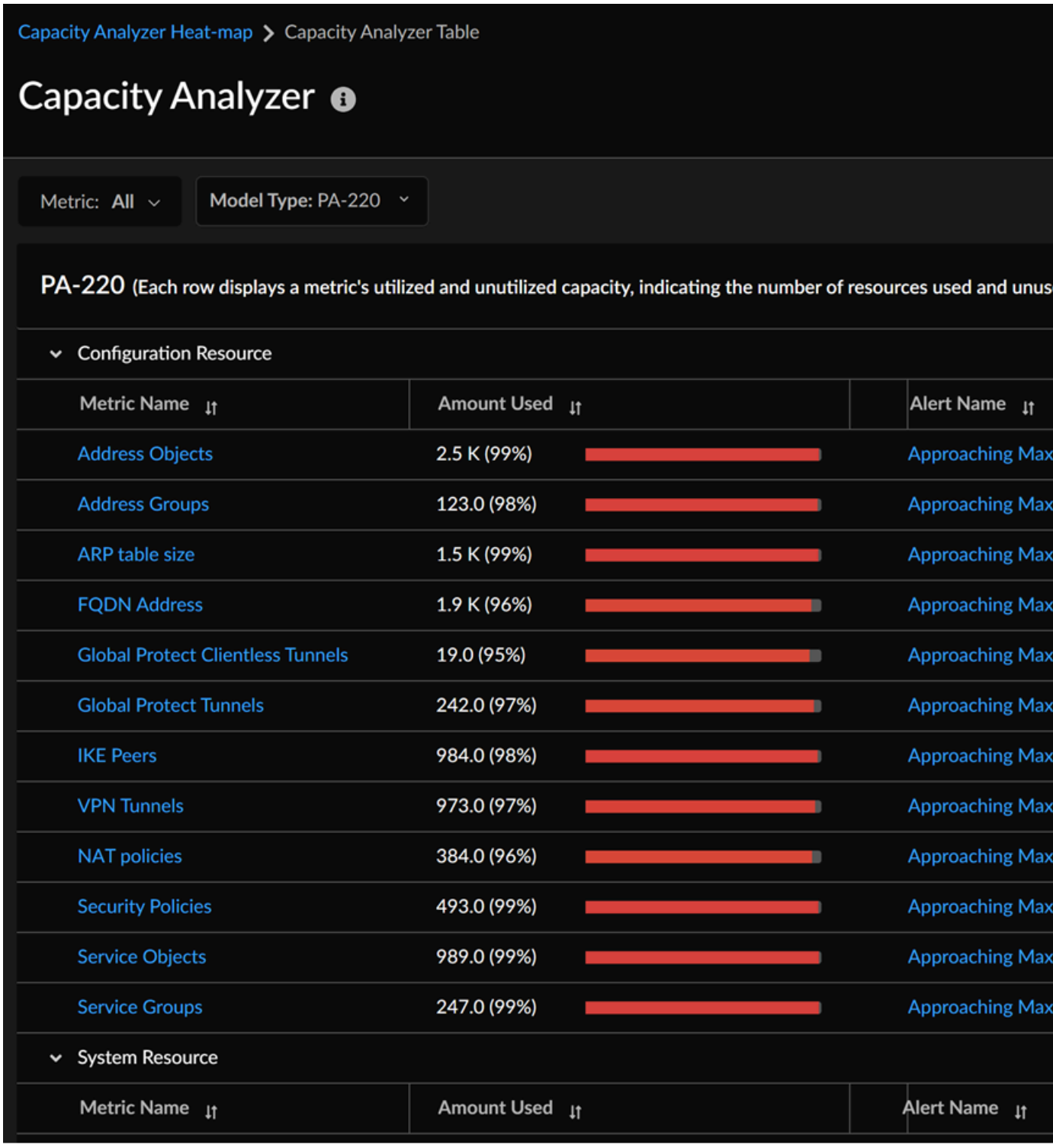
- Metrikkapazität der ARP-Tabellengröße für alle Geräte des Modells **PA-220**.

- Wählen Sie einen der Hostnamen aus, um den Trend für die Metrikkapazität anzuzeigen.
- Ausgelöste Benachrichtigungen für die Metrik und das Datum, an dem die Metrik ihre maximale Kapazität erreichen wird.
- Vorhergesagter Trend für die Metrik. Strata Cloud Manager prognostiziert das Datum, an dem die Metrik die maximale Kapazität erreichen wird. Sie können den Cursor über das Diagramm bewegen, um die Kapazität einer Metrik zu einem beliebigen Zeitpunkt zu überprüfen.

Analysieren der Metrikkapazität basierend auf Gerätemodellen

1. Wählen Sie aus der Heatmap der Kapazitätsanalyse ein Gerätemodell aus, um alle zugehörigen Metriken anzuzeigen.





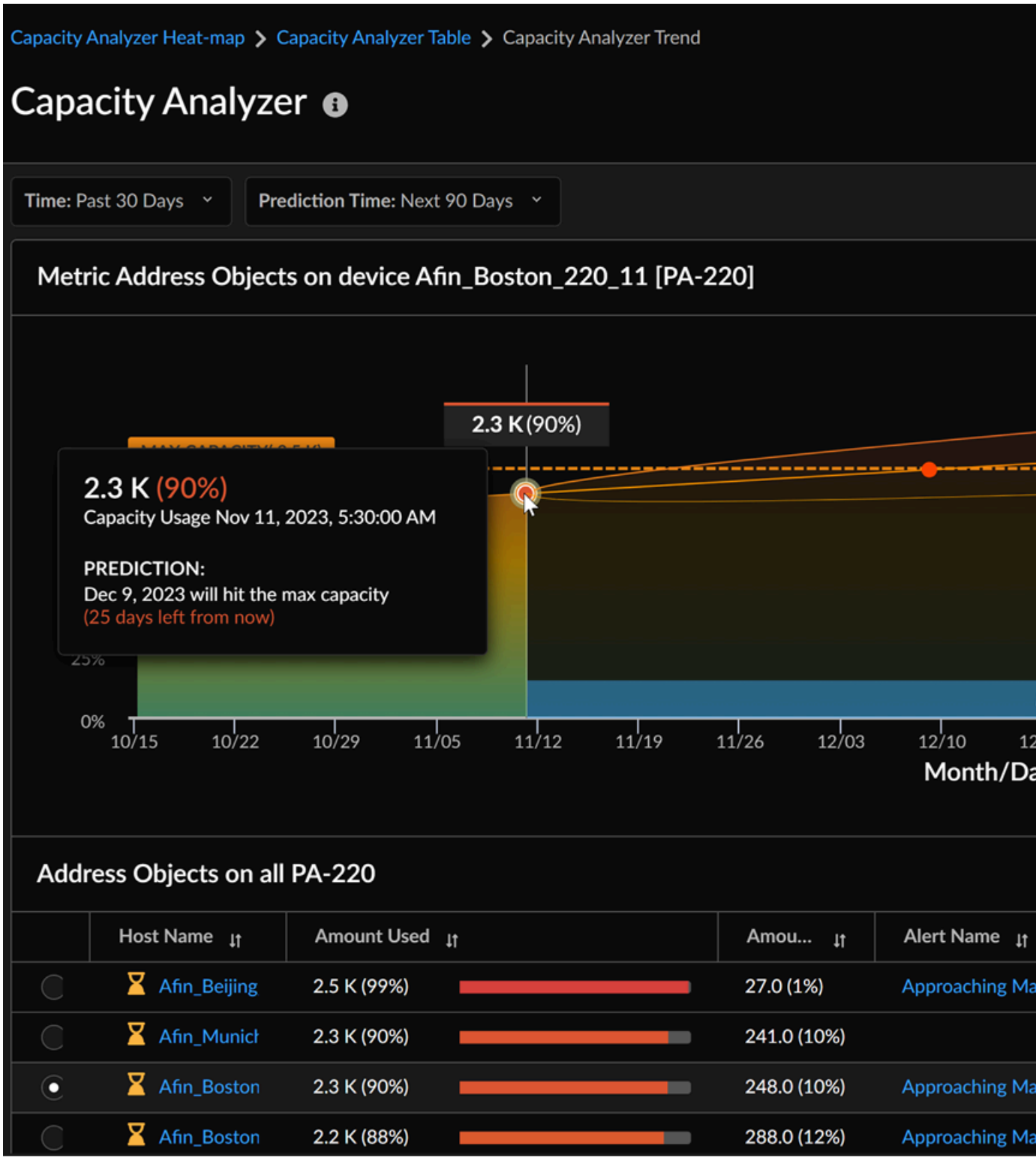
Jede Zeile zeigt die genutzte Kapazität einer Metrik an und gibt die Anzahl der Ressourcen an, die für diese Metrik in einem Gerät verwendet wurden. Darüber hinaus können Sie ausgelöste Benachrichtigungen für die Metrik und das Datum, an dem die Metrik ihre maximale Kapazität erreichen wird, anzeigen.

2. Wählen Sie in der Tabelle „Kapazitätsanalyse“ eine Metrik aus, um deren Trend auf einem Gerät anzuzeigen.

3. Wählen Sie ein Gerät aus, um seinen Metriktrend anzuzeigen.

   Sie können die **Prognosezeit** auswählen, um den vorhergesagten Trend für die Metrik zu überprüfen. Strata Cloud Manager prognostiziert das Datum, an dem die Metrik die maximale Kapazität erreichen wird.

   Sie können den Cursor über das Diagramm bewegen, um die Kapazität einer Metrik zu einem beliebigen Zeitpunkt zu überprüfen.

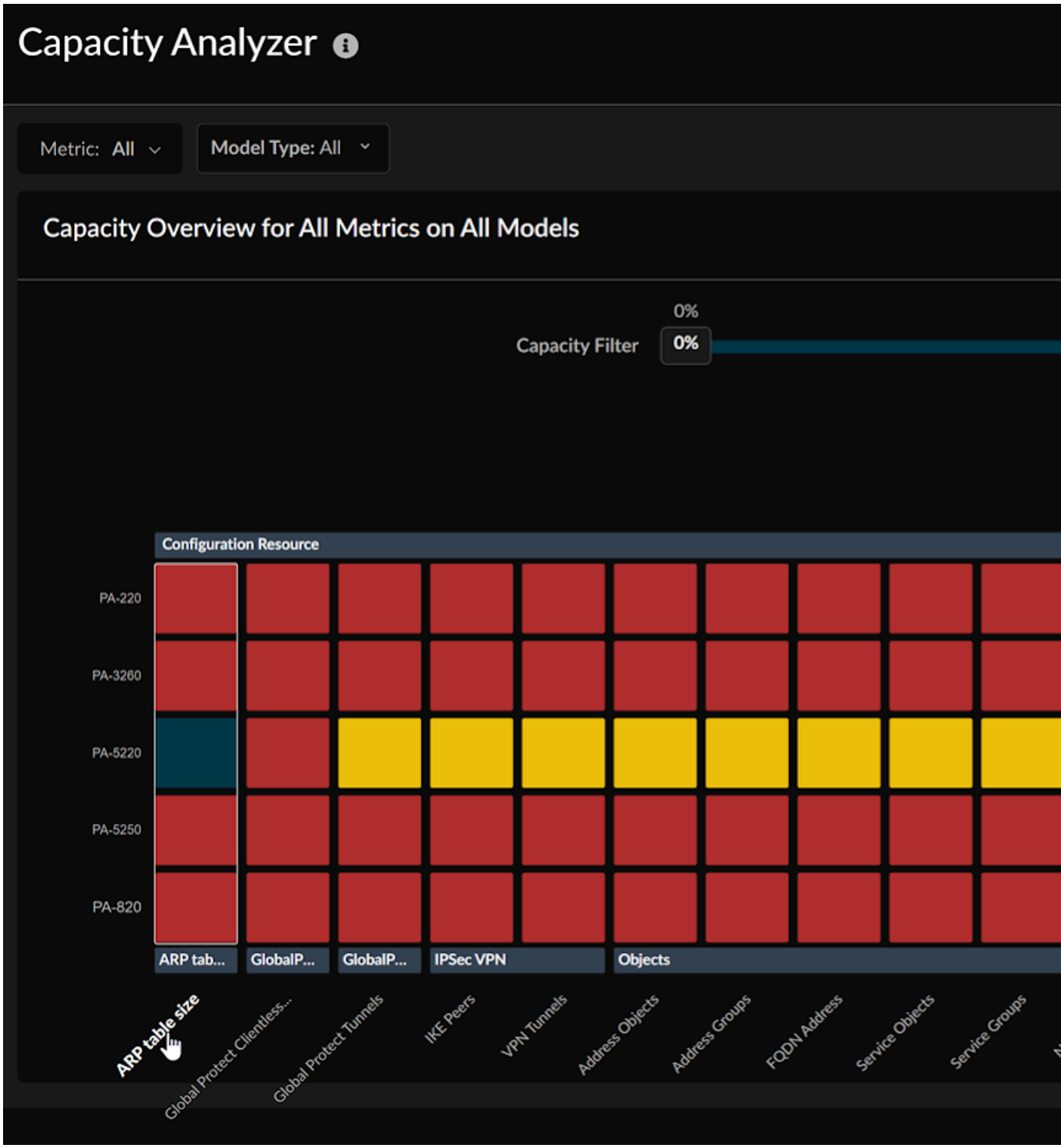


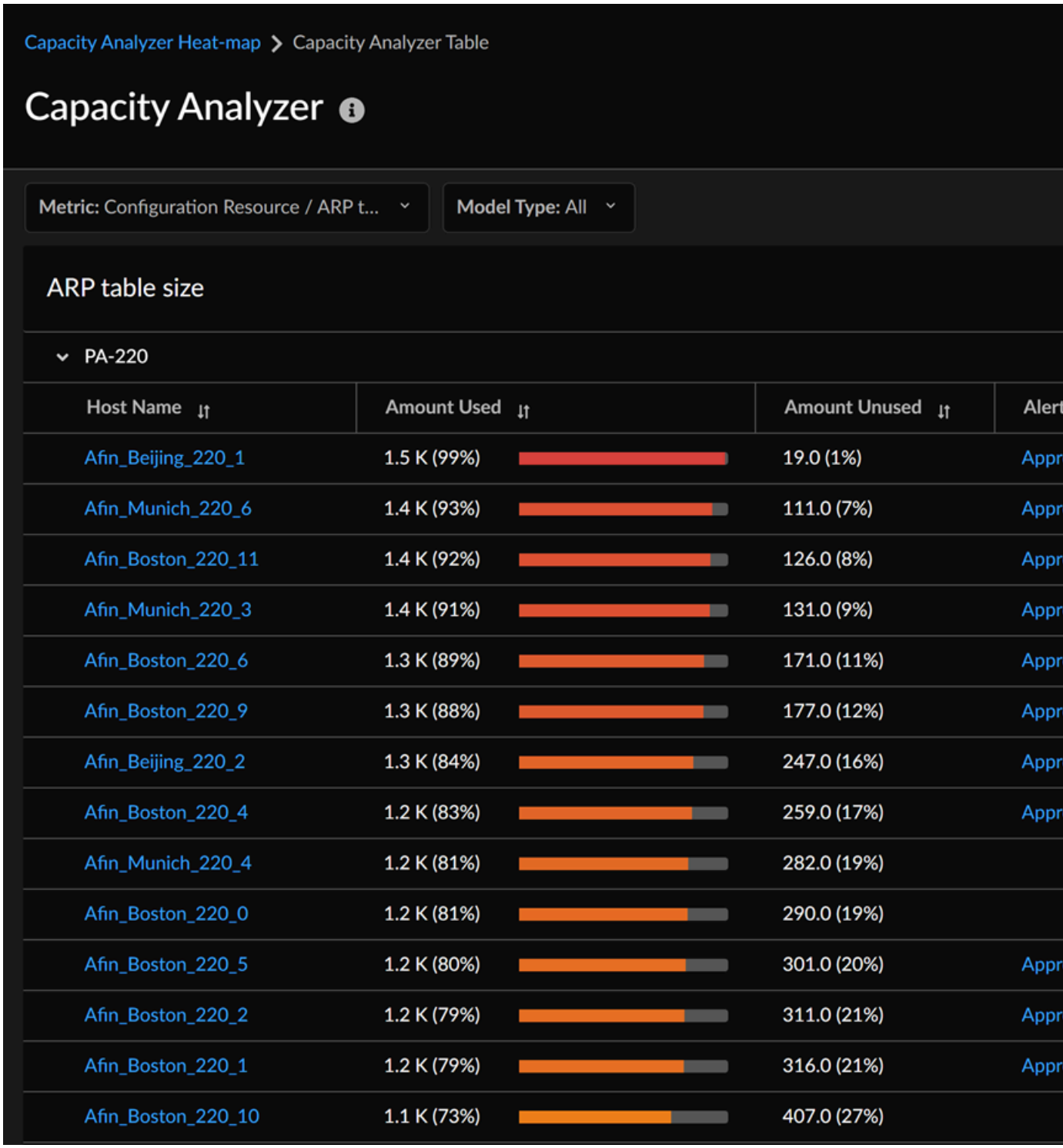
Unter **Benachrichtigungsname** können Sie die für die Adressobjektmetrik ausgelösten Benachrichtigungen anzeigen, die einem Hostnamen entsprechen.

Analysieren der Metrikkapazität basierend auf Metriken

1. Wählen Sie aus der Heatmap der Kapazitätsanalyse eine Metrik aus, um ihre Kapazität auf allen Geräten in einem tabellarischen Format anzuzeigen. In diesem Beispiel wird die Metrik **ARP-Tabellengröße** ausgewählt.

   *Sie können auch einen Metriktyp auswählen und zu einer Metrik navigieren, um ihre Kapazität auf allen Geräten in einem tabellarischen Format anzuzeigen. Beispiel: Metriktyp **Konfigurationsressource** > **Objekte** > **Adressobjekte**.*

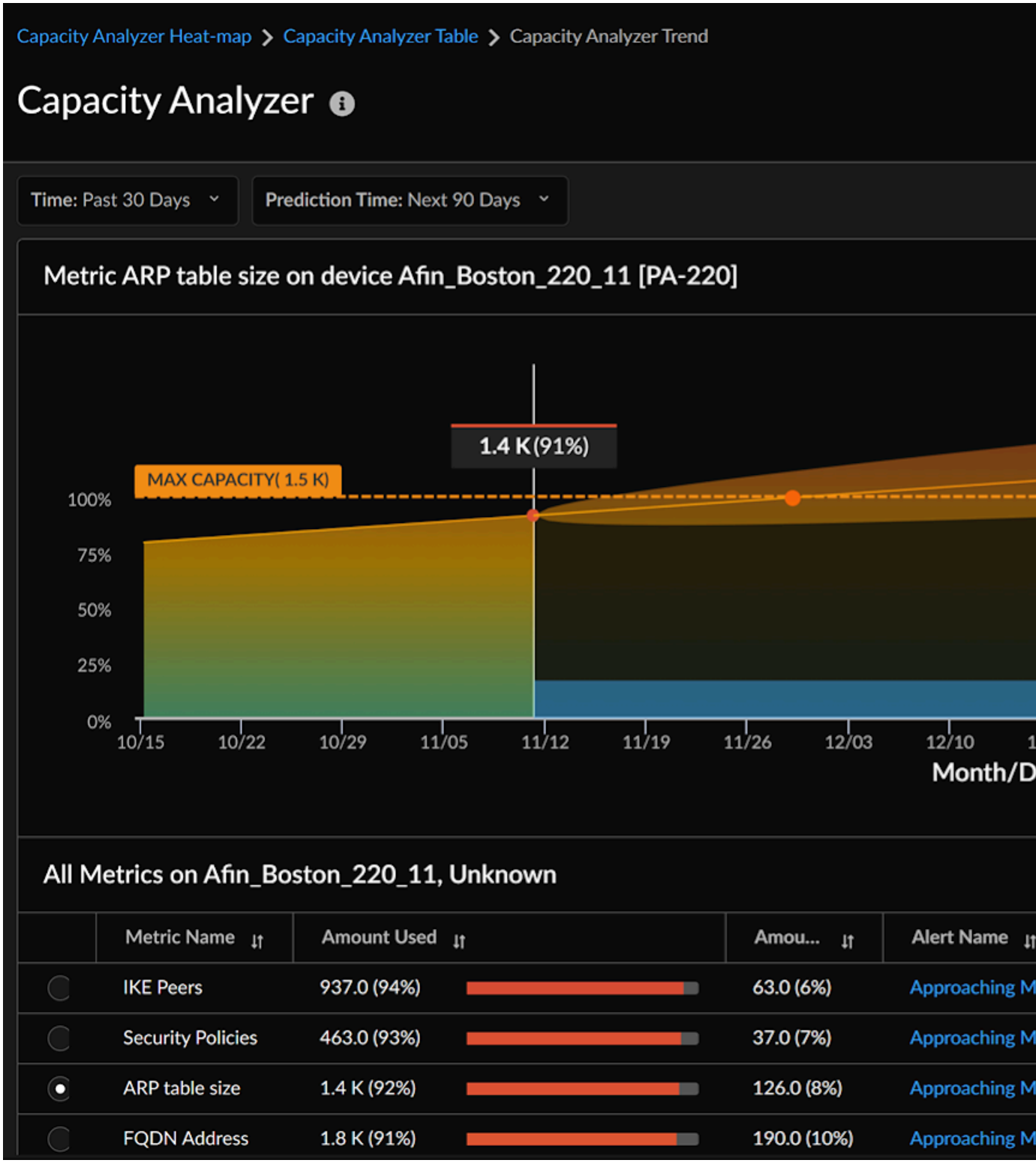




In jeder Zeile wird die genutzte und ungenutzte Kapazität der Metrik **ARP-Tabellengröße** für jeden Host unter den Gerätemodellen angezeigt. Darüber hinaus können Sie für diese Metrik ausgelöste Benachrichtigungen für jeden Host und das Datum, an dem die Metrik ihre maximale Kapazität erreichen wird, anzeigen.

2. Wählen Sie einen Hostnamen aus, um den grafischen Trend der ausgewählten Metrik anzuzeigen.

   Sie können die **Prognosezeit** auswählen, um den vorhergesagten Trend für die Metrik zu überprüfen. Strata Cloud Manager prognostiziert das Datum, an dem die Metrik die maximale Kapazität erreichen wird.



Sie können den Cursor über das Diagramm bewegen, um die Kapazität einer Metrik zu einem beliebigen Zeitpunkt zu überprüfen.

Best Practices in NGFWs

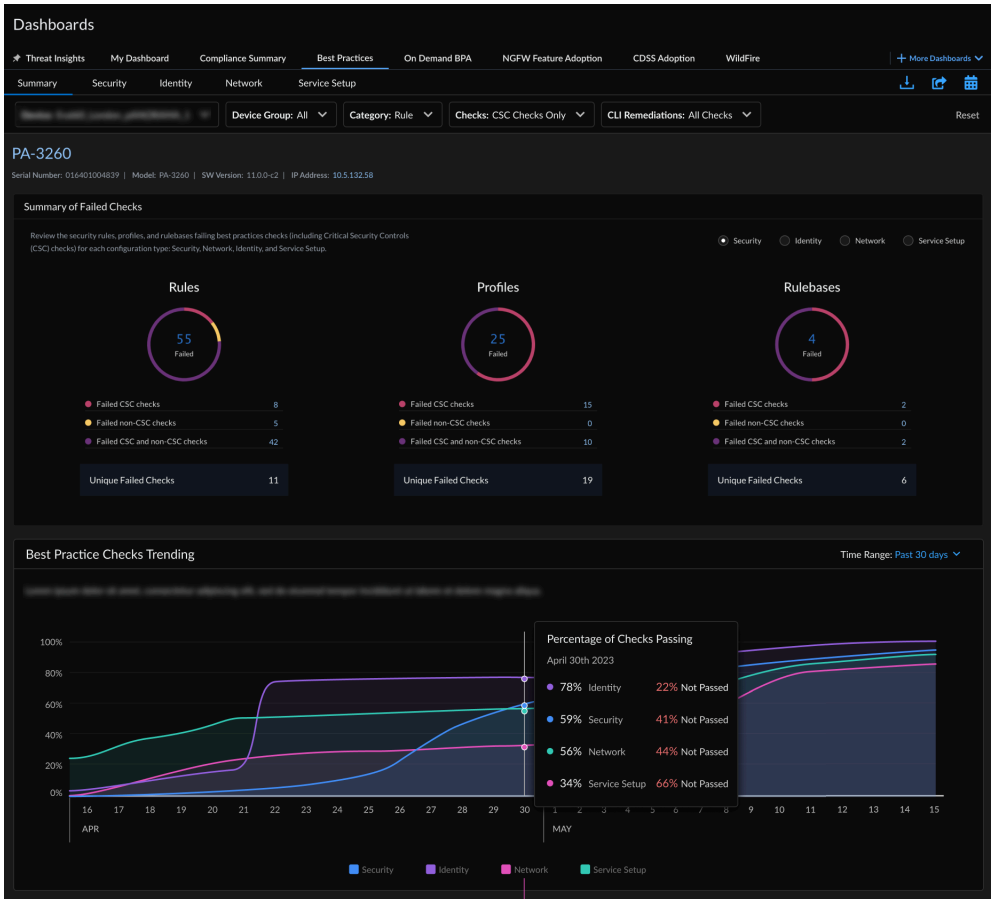
Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

AIOps für NGFW hilft Ihnen, Ihren Sicherheitsstatus durch die Ausrichtung an Best Practices zu verbessern. Sie können AIOps für NGFW nutzen, um Ihre Sicherheitskonfigurationen von Panorama, NGFW und von Panorama verwaltetem Prisma Access anhand von Best Practices zu bewerten und fehlgeschlagene Best Practice-Überprüfungen zu korrigieren. AIOps für NGFW optimiert den Prozess zur Überprüfung der InfoSec-Konformität Ihrer Netzwerkinfrastruktur.

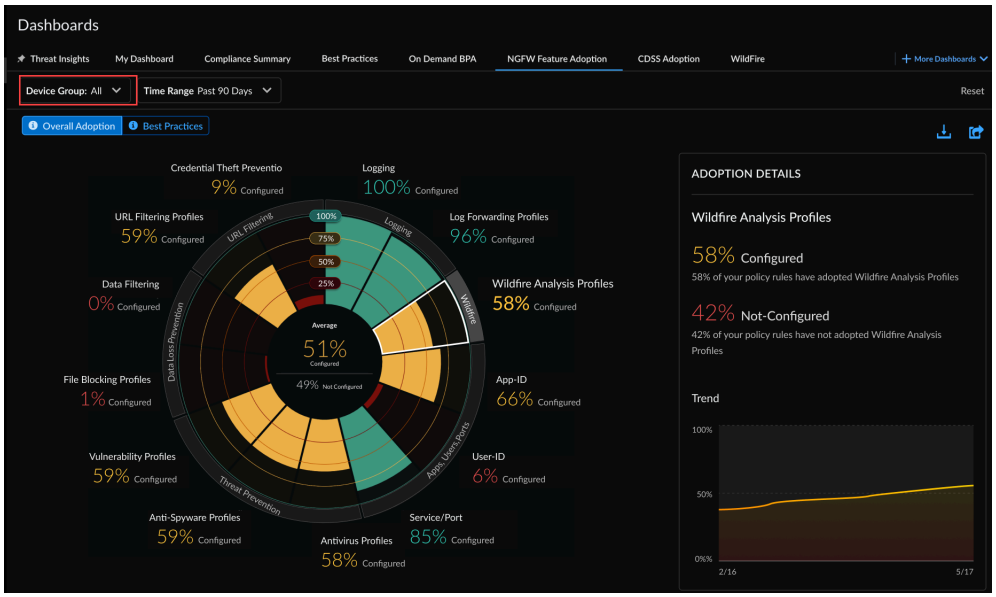
AIOps für NGFW ist kostenlos und die folgenden Best Practice Assessment-(BPA-)Funktionen von AIOps sind ohne AIOps-Premium-Lizenz verfügbar. Die vollständige Liste der verfügbaren Best Practice-Funktionen finden Sie unter Integrierte Best Practices:

- Auf dem Dashboard „Best Practices“ finden Sie tägliche Best Practice-Berichte und deren Zuordnung zu den Critical Security Controls (CSC) des Center for Internet Security. So können Sie Bereiche identifizieren, in denen Sie Änderungen vornehmen können, um die Einhaltung

Ihrer Best Practices zu verbessern. Geben Sie den Best Practice-Bericht als PDF frei und planen Sie die regelmäßige Zustellung in Ihren Posteingang.

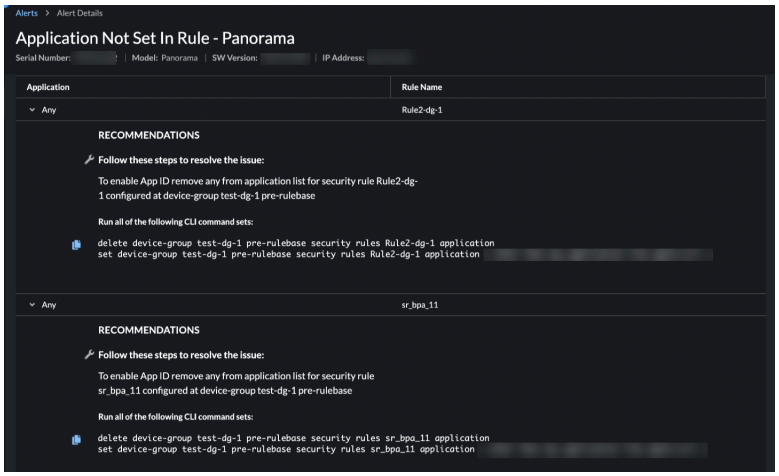


- Überwachen Sie die Funktionsannahme und bleiben Sie auf dem Laufenden, welche Sicherheitsfunktionen Sie in Ihrer Bereitstellung verwenden und welche potenziellen Abdeckungslücken bestehen.



- Erhalten Sie von AIOps für NGFW Benachrichtigungen zu Ihrem Sicherheitsstatus, um zu erfahren, wann Ihre Sicherheitseinstellungen möglicherweise einer genaueren Überprüfung bedürfen.

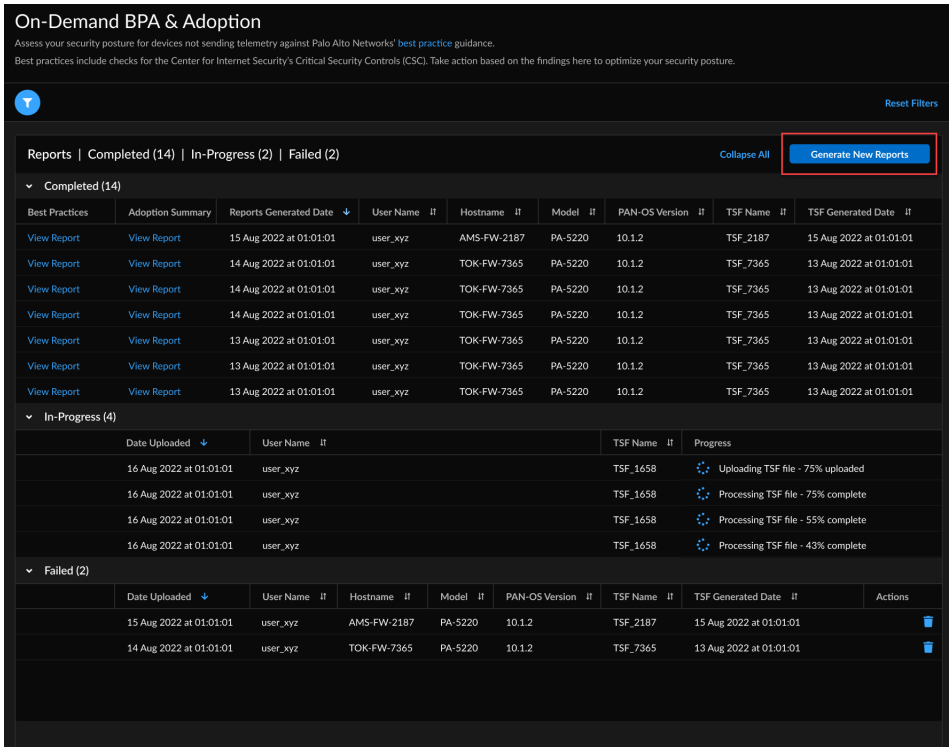
  Korrekturen über die Befehlszeilenschnittstelle (CLI) sind auch in AIOps für NGFW unter **Benachrichtigungen** > **Sicherheit** > **Benachrichtigungsdetails** verfügbar. Sehen Sie sich Empfehlungen an, die Ihnen dabei helfen sollen, Probleme zu beheben, die zum Auslösen einer Benachrichtigung führen.



  Sicherheitsbenachrichtigungen und CLI-Korrekturen sind nur für Geräte verfügbar, die Telemetrie gemeinsam nutzen. Diese Funktion unterstützt nicht das manuelle Hochladen von Dateien für den technischen Support (Tech Support Files, TSF) für PAN-OS-Geräte mit Version 9.1 und höher.

- Erstellen Sie BPA-Berichte für (nicht-telemetrische) PAN-OS-Geräte mit Version 9.1 und höher, jetzt einschließlich Metriken zur Funktionsannahme. Wenn Sie das eigenständige BPA-Tool zum Generieren von BPA-Berichten verwendet haben, fragen Sie sich möglicherweise:

„Kann ich weiterhin BPA-Berichte über das Customer Support Portal erstellen?“. Auch dafür haben wir eine Lösung.



Mit einer Premium-Lizenz bietet AIOps für NGFW auch erweiterte Funktionen für den Sicherheitsstatus. Die Premium-Funktionen konzentrieren sich darauf, die optimale Nutzung und Sicherheit für ihre Firewalls zu gewährleisten. Sehen Sie sich an, was kostenlose (Free) und Premium-Lizenzen zu bieten haben.

On-Demand-BPA-Bericht

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Sie können nun die Best Practice-Bewertung (Best Practice Assessment, BPA) und die Funktionsannahmeübersicht direkt von Strata Cloud Manager aus ausführen. Laden Sie einfach eine Datei für den technischen Support (Tech Support File, TSF) hoch. Sie können den BPA-Bericht auf Abruf für Geräte generieren, die keine Telemetriedaten senden oder nicht in AIOps für NGFW integriert sind.

Bei der BPA wird Ihr Sicherheitsstatus anhand der Best Practices von Palo Alto Networks bewertet und es werden Prioritäten für Verbesserungen der Geräte festgelegt. Sicherheitsrelevante Best Practices verhindern bekannte und unbekannte Bedrohungen, verringern die Angriffsfläche und bieten Einblick in den Datenverkehr, sodass Sie wissen und kontrollieren können, welche Anwendungen, Benutzer und Inhalte sich in Ihrem Netzwerk befinden. Außerdem gehören zu den Best Practices Prüfungen für die Critical Security Controls (CSC) des Center for Internet Security. Sehen Sie sich die Best Practice-Anleitung an, um den Sicherheitsstatus zu stärken und Verbesserungen umzusetzen.

Kann ich weiterhin BPA-Berichte über das Customer Support Portal erstellen?

Bevor es AIOps gab, mussten Sie zum Customer Support Portal gehen, um auf BPA zuzugreifen und es auszuführen. Heutzutage wird der Bericht zur Best Practice-Bewertung für NGFW/von Panorama verwaltetes Prisma Access vorzugsweise über AIOps generiert und heruntergeladen.

Ab dem 17. Juli 2023 können Sie nicht mehr über das Customer Support Portal auf das BPA zugreifen und es ausführen.

STEP 1 | Gehen Sie zum Hub und aktivieren Sie AIOps für NGFW. Es ist kostenlos. Die Aktivierung kann ohne Strata Logging Service erfolgen, wenn Sie derzeit keine Geräte mit aktivierter Telemetrie einbinden möchten.

> *Das Dashboard „Best Practices“, die Sicherheitsbenachrichtigungen und die Annahmeübersicht sind für Geräte, die ohne Strata Logging Service oder Telemetrie aktiviert wurden, nicht verfügbar.*

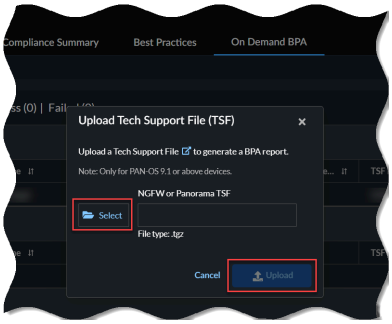
STEP 2 | Melden Sie sich bei Ihrer aktivierten AIOps für NGFW-Instanz an. Es werden die folgenden Registerkarten angezeigt (auch ohne Strata Logging Service):

- Status
- Aktivität
- Einstellungen

STEP 3 | Gehen Sie zu **Dashboards** > **On-Demand-BPA**.

STEP 4 | **Generieren Sie einen neuen BPA-Bericht**.

STEP 5 | **Wählen Sie die TSF-Datei aus** und **laden Sie die TSF-Datei hoch**.



Die Dauer des Uploads hängt von der Größe Ihrer .tgz-Datei und von Ihrer Internetgeschwindigkeit ab. Bei größeren Dateien kann das Hochladen der Datei einige Minuten dauern. Erweitern Sie **In Bearbeitung**, um den Status der TSF-Dateien anzuzeigen.

- *On-Demand-BPA unterstützt nur die Dateien für den technischen Support (Tech Support Files, TSF) im .tgz-Dateiformat.*
- *On-Demand-BPA unterstützt zur Berichterstellung nur TSF-Dateien von Geräten mit PAN-OS-Version 9.1 oder höher.*

STEP 6 | Wählen Sie nach dem Verarbeiten der TSF-Datei unter **Abgeschlossen** die Option **Bericht ansehen** aus, um den generierten BPA-Bericht von Ihrem Gerät anzuzeigen.

Best Practices

Wo kann ich das verwenden?	Was brauche ich?
• •	❑ oder ❑ -Lizenz ❑ Aktivieren der Telemetriefreigabe auf Geräten

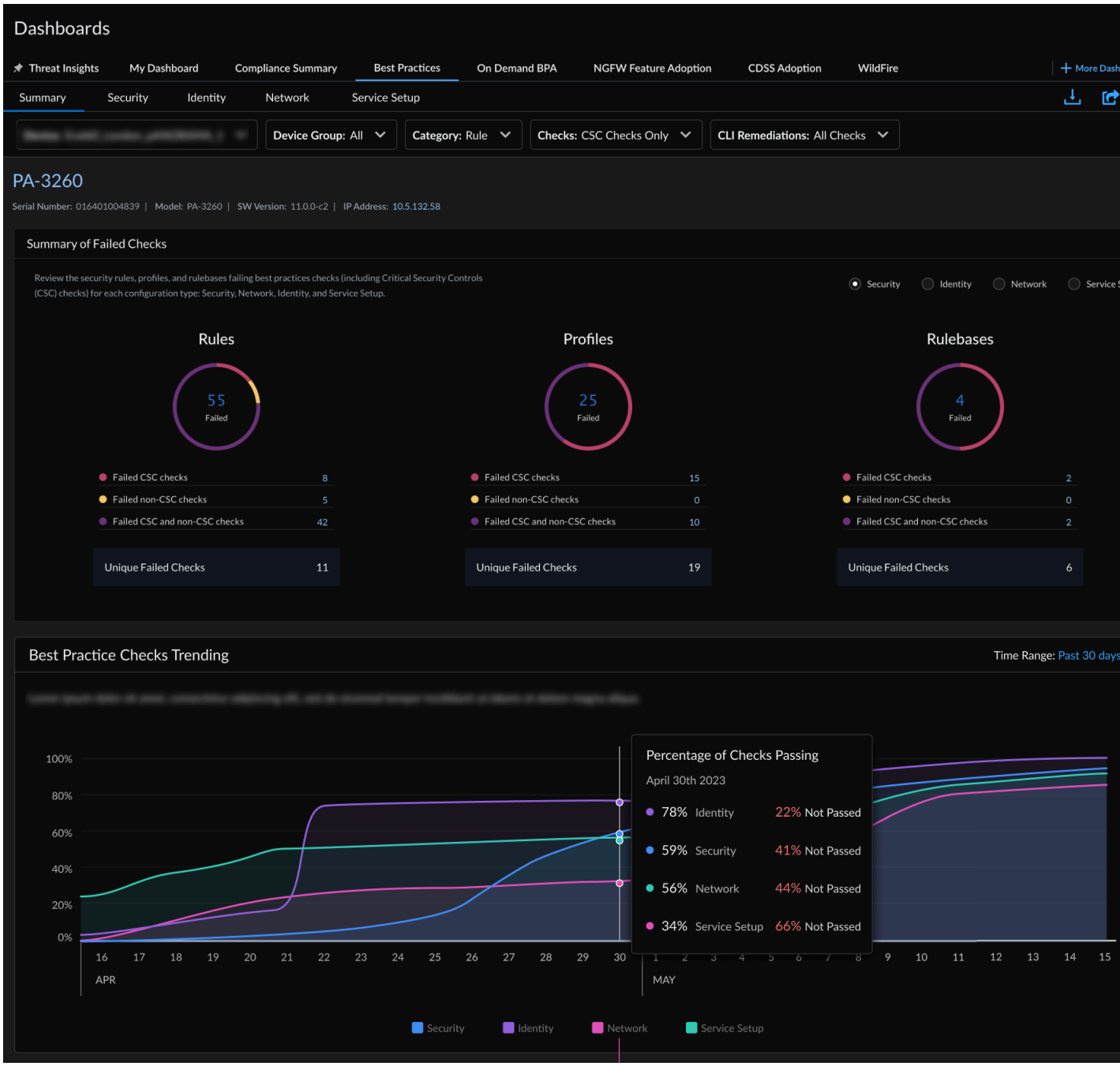
Was sehen Sie in diesem Dashboard?

Das Dashboard zeigt aggregierte Daten pro Prisma Access und NGFW/Panorama, die Ihrem Mandanten zugeordnet sind.

Navigieren Sie zum Dashboard **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Best Practices**, um Ihren Sicherheitsstatus anhand der Best Practice-Anleitung von Palo Alto Networks zu messen. Vor allem umfasst die Best Practice-Bewertung Prüfungen für die Critical Security Controls (CSC) des Center for Internet Security. CSC-Prüfungen werden getrennt von anderen Best Practice-Überprüfungen durchgeführt, sodass Sie Updates, die Sie an die CSC-Compliance heranführen, einfach auswählen und priorisieren können.

Wie können Sie die Daten aus dem Dashboard verwenden?

Während Best Practice-Leitfäden Ihnen helfen sollen, Ihren Sicherheitsstatus zu stärken, können Sie die Ergebnisse dieses Berichts auch dabei unterstützen, Bereiche zu bestimmen, in denen Sie Änderungen vornehmen können, um Ihre Umgebung effektiver zu verwalten.



Das Dashboard „Best Practices“ ist in fünf Abschnitte unterteilt:

- **Zusammenfassung**

  Bietet Ihnen einen umfassenden Überblick über alle fehlgeschlagenen Überprüfungen für ein Gerät über die Konfigurationstypen (Sicherheit, Netzwerk, Identität und Diensteinrichtung), historische Trenddiagramme für BPA-Überprüfungen und die Bewertung Ihrer Best Practice-Akzeptanzraten für wichtige Funktionsbereiche.

- **Sicherheit**

  Zeigt die Regeln, Regelsätze oder Profile an, bei denen Best Practice- und CSC-Prüfungen für das ausgewählte Gerät und den ausgewählten Standort fehlschlagen. Sofern verfügbar, können

Sie mit CLI-Korrekturen Probleme mit Ihren Richtlinienregeln beheben. CLI-Korrekturen werden mithilfe von TSF-Daten generiert, die Sie beim Erstellen eines On-Demand-BPA-Berichts hochladen.

- **Regelsätze**

  Betrachtet, wie Ihre Richtlinie organisiert ist und ob Konfigurationseinstellungen, die für viele Regeln gelten, mit Best Practices (einschließlich CSC-Prüfungen) übereinstimmen.

- **Regeln**

  Zeigt Ihnen die Regeln an, die Best Practice- und CSC-Überprüfungen nicht bestanden haben. Erfahren Sie, wo Sie schnell Maßnahmen ergreifen können, um fehlgeschlagene Prüfungen zu beheben. Regeln werden nach Anzahl der Sitzungen sortiert, sodass Sie damit beginnen können, die Regeln zu überprüfen und zu aktualisieren, die sich auf den größten Teil des Datenverkehrs auswirken.

- **Profile**

  Zeigt Ihnen, wie sich Ihre Profile mit Best Practices messen, einschließlich CSC-Überprüfungen. Profile führen eine erweiterte Überprüfung auf Datenverkehr durch, der einer Sicherheits- oder Entschlüsselungsregel entspricht.

- **Identität**

  Zeigt an, ob die Einstellungen für die Authentifizierungsdurchsetzung (Authentifizierungsregel, Authentifizierungsprofil und Authentifizierungsportal) für ein Gerät den Best Practices entsprechen und mit den CSC-Prüfungen konform sind.

- **Netzwerk**

  Überprüft, ob die Anwendungsüberschreibungsregeln und Netzwerkeinstellungen mit Best Practices und CSC-Prüfungen übereinstimmen.

- **Diensteinrichtung**

  Sehen Sie, wie die Abonnements, die Sie auf Ihren Geräten aktiviert haben, mit den Best Practices und CSC-Prüfungen übereinstimmen. Sie können hier die WildFire-Einrichtung sowie die Konfigurationen von GlobalProtect Portal und GlobalProtect Gateway überprüfen und die fehlgeschlagenen Prüfungen korrigieren.

Freigeben, Herunterladen und Planen von Berichten für ein Dashboard

Sie können neben Berichten, die die Daten abdecken, die das Dashboard im PDF- und CSV-Format anzeigt, auch CLI-Korrekturen im TXT-Format herunterladen, freigeben und planen. Diese Symbole finden Sie oben rechts im Dashboard: