# Strata Cloud Manager

## The Industry's First AI-Powered Unified Management and Operations Solution

Today's network security environment is more complex than ever. Massive volumes of data and devices are outpacing traditional defenses, allowing sophisticated threats to slip through. Attackers are moving faster, leveraging AI to craft ever more elusive threats. Meanwhile, organizations are juggling an array of security tools across headquarters, branch offices, remote users, virtualized data centers, and cloud environments. Over time, this patchwork of point products has created a web of complexity—multiple dashboards, siloed data, and inconsistent policies that are increasingly difficult to manage. The result? A security posture that struggles to keep up with evolving risks, hampered by poor visibility across the IT landscape, making it tough for teams to see where the next threat may arise.

## A Whole New Era of Complexity

To thrive in this landscape, the key isn't adding more tools. Instead, organizations must transform their existing IT environment into a unified, intelligent, and secure ecosystem that's ready for whatever comes next.

## Typical Solutions Can't Secure Modern Organizations

Organizations today are drowning in a proverbial flood of security tools, each designed to handle a specific threat vector but rarely speaking the same language. A fragmented approach like this leads to critical blind spots, ballooning costs, and operational burdens that stall innovation. We've identified four ways today's tools fall short—leaving your organization at risk.

### 1. Siloed Tools Limit Visibility

Siloed products and multiple consoles make it almost impossible to see the complete security picture. Nearly four out of five organizations admit they lack full visibility into their assets, resulting in a threefold spike in security incidents.[1] A unified view is vital to anticipate threats and respond faster.

### 2. Complex Network Security Management

Managing on-premises, cloud, and hybrid deployments creates a maze of manual processes and repeated efforts. Teams juggle an average of 45 security tools,[2] pushing complexity and operational costs through the roof. Standardizing tool sets and automating workflows are key to reigning in the chaos.

### 3. Misconfigurations and Human Error Cause Breaches

Even the best defenses fail when underutilized or improperly configured, resulting in poor security hygiene. Gartner predicts 99% of firewall breaches in 2025 will result from misconfigurations.[3] Intelligent automation to detect and resolve these policy gaps is essential to reduce these risks.

### 4. Delayed Issue Detection Drives Up Outage Costs

Reactive monitoring typically alerts you after an outage has wreaked havoc. The average organization takes 3.6 days to fully recover,[4] at a cost of up to $1.3 million per major disruption.[5] Proactive analytics and integrated AI can spot impending failures before they escalate, saving both money and reputation.

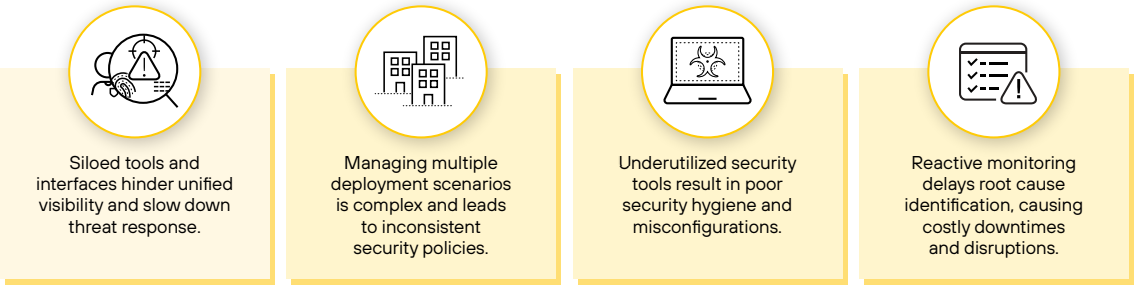


**Figure 1:** Significant management and operations challenges

1. *The Current State of the IT Asset Visibility Gap and Post-Pandemic Preparedness*, ESG and Axonius, April 27, 2021.
2. *Cyber Resilient Organization Report 2020*, IBM Security, June 30, 2020.
3. Charlie Winckless and Jay Heiser, *Risk-Based Evaluations of Cloud Provider Security*, Gartner, August 31, 2021.
4. "The many costs of downtime" survey, Opengear, September 26, 2022.
5. *Cost of a Data Breach Report 2023*, IBM Security, July 2023.

Securing the modern connected organization requires a holistic, unified approach. To do this, security needs to be deployed and managed holistically through a single pane of glass with each component working together seamlessly and leveraging the power of AI to stay ahead of rapidly evolving threats. Strata Cloud Manager by Palo Alto Networks provides exactly that—enabling customers to consolidate defenses, standardize policies, and respond faster across all environments.

## What Is Strata Cloud Manager?

Strata® Cloud Manager is the industry's first AI-powered unified solution for managing and operating the entire network security infrastructure. It transforms how organizations oversee their next-generation firewalls (NGFWs) and SASE deployments, aggregating telemetry from every enforcement point to deliver actionable insights. By combining AI-driven intelligence, automated operations, and integrated threat intelligence, it helps security teams stay ahead of emerging risks, maintain optimal performance, and reduce operational costs.

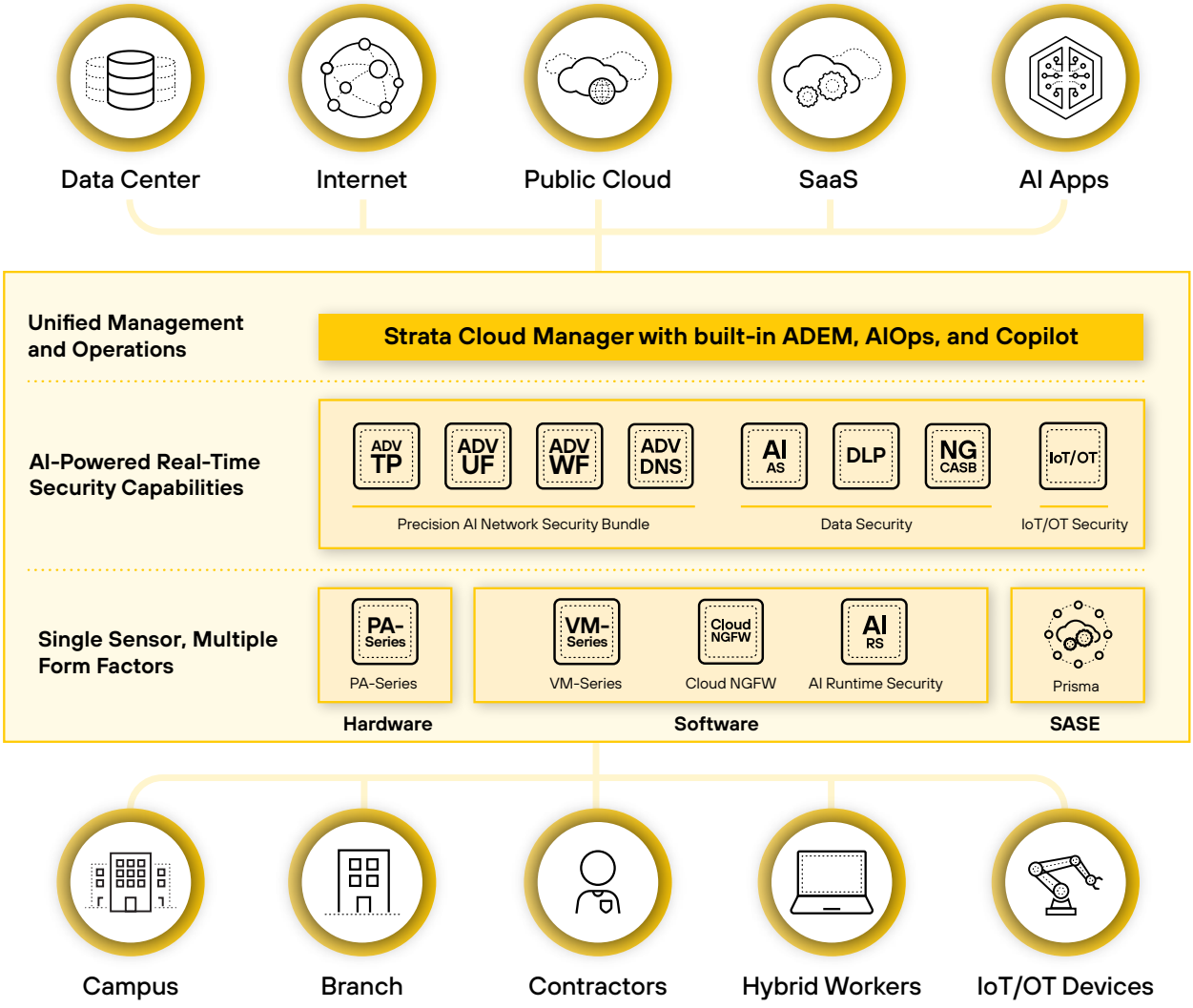


**Figure 2:** Strata Cloud Manager: A unified, cloud-based single pane of glass for network security management and operations

## Gain Complete Visibility Across Your Network Security Estate

Achieve real-time, comprehensive visibility of your entire network security landscape including all users, applications, devices, and the most critical threats that need attention through a unified interface.

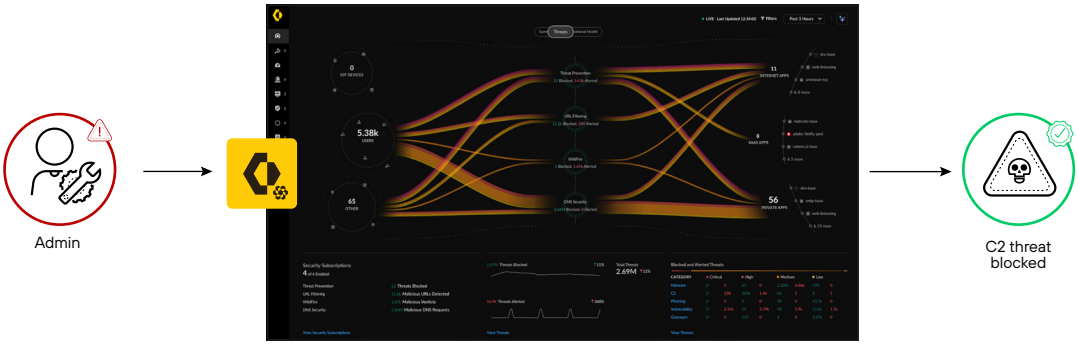


**Figure 3:** Strata Cloud Manager provides real-time insights into threats

## Enable Simple and Consistent Network Security Lifecycle Management

Streamline configuration and policy management across all enforcement points from a single interface. Apply consistent security policies across NGFWs and Prisma® Access with hierarchical folders and reusable snippets to simplify configurations. Improve operational efficiency with automated onboarding, policy deployment, and device refresh for seamless network security management.

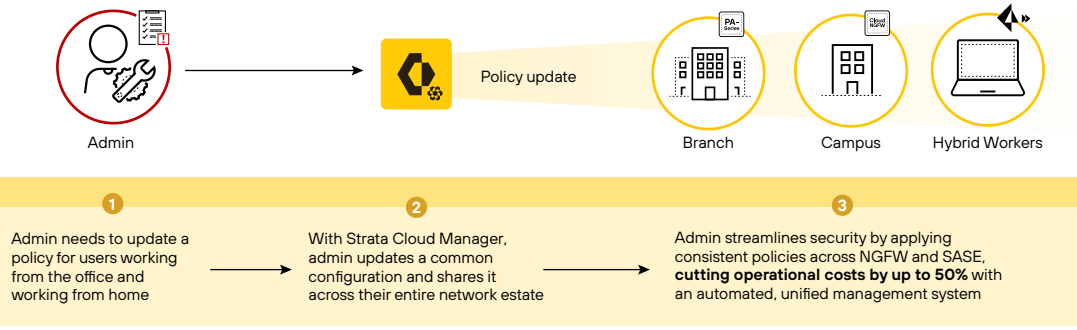


**Figure 4:** Share configuration across your entire network estate

## Strengthen Security Posture in Real Time

Leverage AI-powered analysis to detect, resolve, and optimize policy anomalies like shadow and redundant policies and overly permissive or unused rules. Improve your security posture with integrated best practice recommendations and maintain compliance with industry and InfoSec standards.

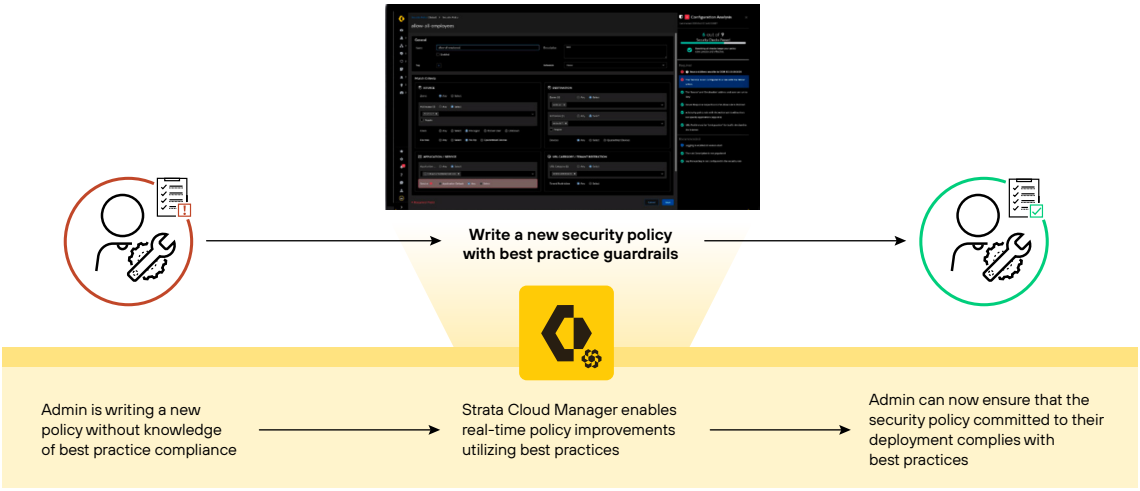


**Figure 5:** Write security policies with automated best practices

## Proactively Resolve Network Disruptions and Enhance User Experience

Predict, diagnose, and resolve network health issues—such as user experience problems, capacity bottlenecks, CVE vulnerabilities, service connection issues, and 130 other categories of issues—up to 90 days in advance to ensure smooth operations.

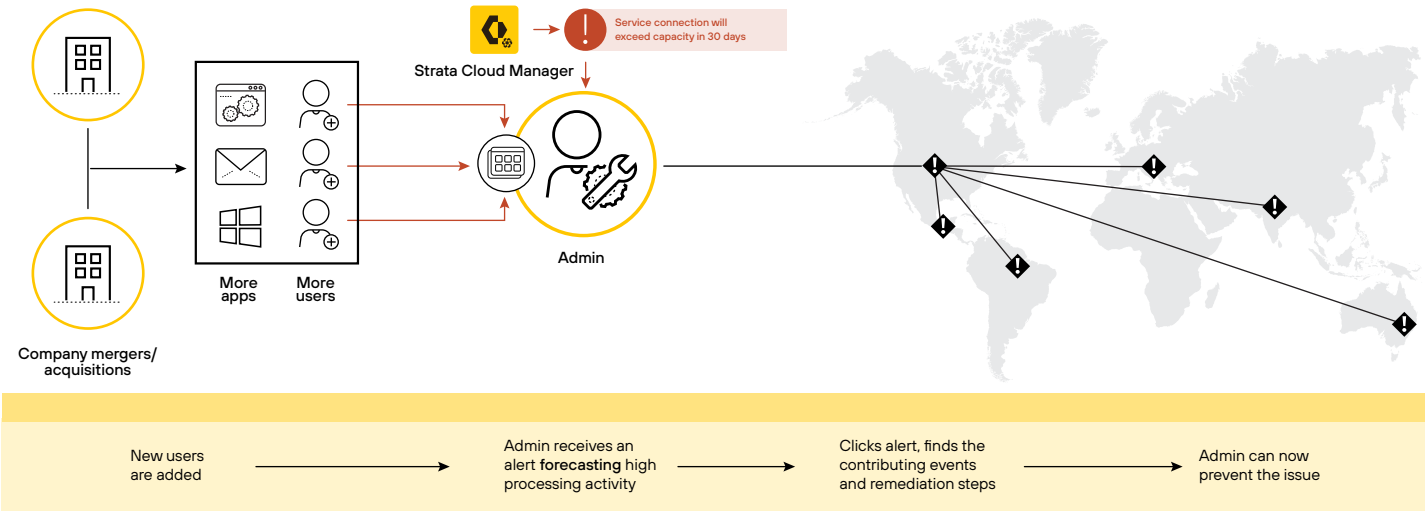


**Figure 6:** Predictive insights help admins identify and resolve issues before they escalate

## Instant Knowledge at Your Fingertips to Resolve Issues Fast

With Strata Copilot, our AI-powered assistant featuring a natural language interface, you can quickly find, understand, and address security and operational challenges before they escalate. Plus, its streamlined case creation capabilities ensure rapid support when you need it most.

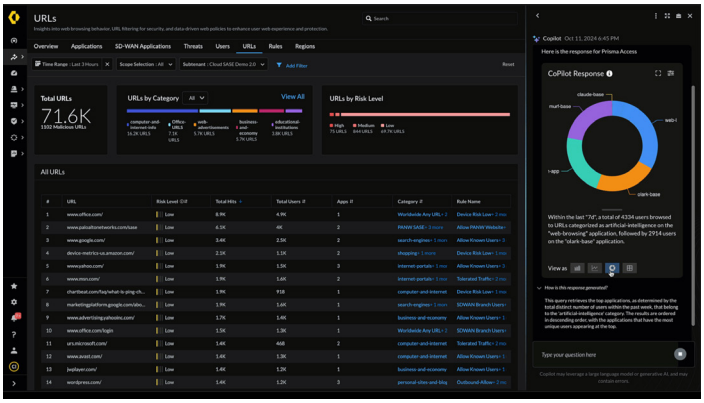


**Figure 7:** Contextually relevant questions and actionable suggestions for securing and optimizing your network

# Business Benefits

Key business benefits of Strata Cloud Manager:

- **Maximize ROI on security investments**: Save tens of thousands of dollars by automatically detecting and addressing security gaps.
- **Remediate misconfigurations**: Identify and resolve risky misconfigurations. Every month Strata Cloud Manager identifies and shares 2 million misconfigurations for resolution.
- **Proactively improve security posture**: Daily configuration assessments help identify gaps, maintain best practices, and ensure optimal security posture.
- **Ensure compliance**: Align configurations with industry standards (CIS, NIST) and custom checks for continuous compliance, reducing risk.
- **Achieve consistent security across deployments**: Update policies once for consistent security across NGFW and SASE.
- **Keep work going**: Predict and address critical network issues across 130+ categories to keep operations running smoothly.

## How Strata Cloud Manager Works

Strata Cloud Manager gathers telemetry data from all enforcement points and processes it in the cloud. Using predictive analytics and best practice analysis, it transforms this data into actionable insights. You can then use a single interface to create and enforce policies across your entire deployment.

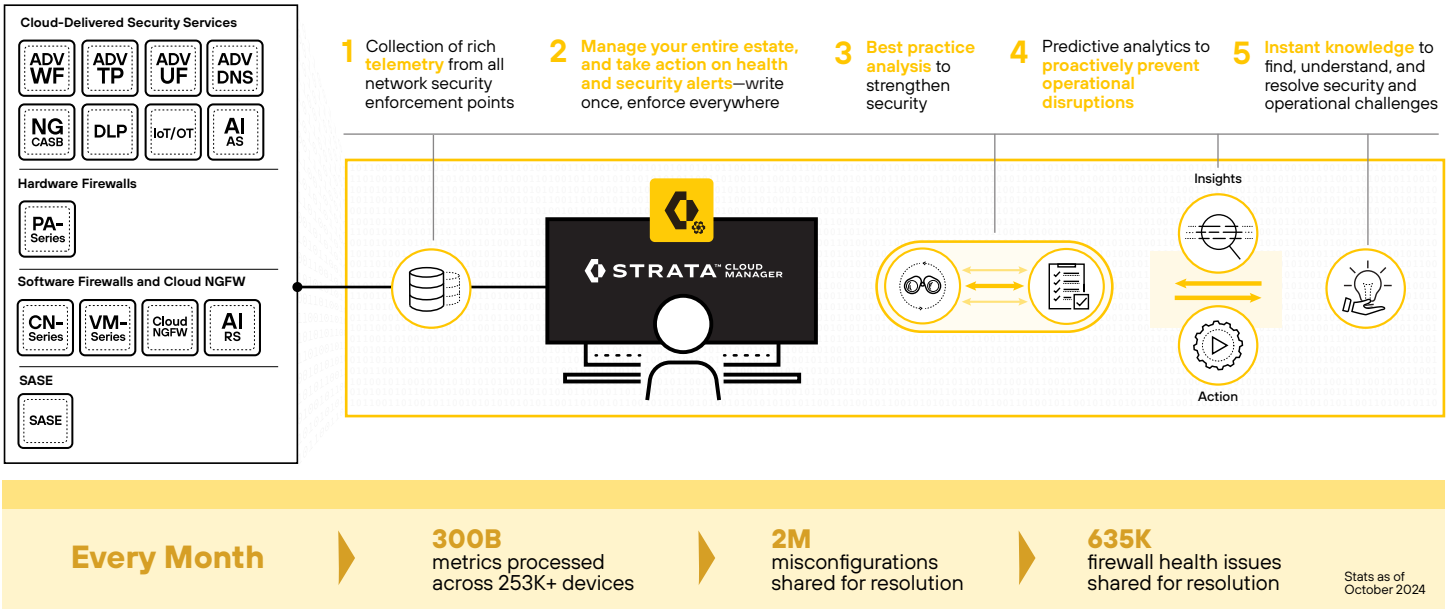


**Figure 8:** How Strata Cloud Manager works

## Features and Requirements

Strata Cloud Manager is available in Essentials and Pro (paid) tiers. Refer to TechDocs for a full list of features and descriptions.

| Table 1: Strata Cloud Manager Features and Capabilities | |
|---|---|
| **Visibility and Insights** | |
| Command Center: Centralized visibility across network security estate* | Activity Insights: Real-time, in-depth insights into network activities across applications, users, threats, URLs, and usage* |
| Interactive dashboards and reporting* | Log Viewer* |
| IoC Search | Seamless log forwarding* |
| **Configuration and Lifecycle Management** | |
| Consistent policy across all enforcement points | Configuration management for all form factors—NGFW, SASE, SD-WAN, and security services |
| Shareable, predefined, and custom snippets ensure consistency and simplify configurations | Auto provisioning of Large Scale VPN deployments |
| Automated bulk onboarding of devices | Software upgrade orchestration |
| Software upgrade recommendations based on enabled features and known CVE vulnerabilities for NGFW† | |
| **Security Posture** | |
| Predefined best practice checks | Custom best practice checks† |
| Inline best practice recommendations and enforcement to close existing security gaps† | Enforce security best practices in real time during configuration† |
| Configuration cleanup of unused rules and objects† | Regulatory compliance (CIS, NIST)† |
| Detect and remediate policy anomalies (shadow and redundant policies, generalizations, and correlations)† | Identify and optimize overly permissive, unused, and unhit rules† |
| **Operational Health and User Experience** | |
| Detect NGFW, software vulnerabilities, and SASE infrastructure issues | Proactively detect and remediate deployment-specific issues (failure prediction, root cause analysis, anomaly detection)† |
| ADEM for user to application experience† | Predict capacity needs for NGFW and SASE† |
| Centralized troubleshooting | Multidomain analysis for SASE with Access Analyzer† |
| In-app support ticket creation† | Root cause analysis for performance issues† |

* Requires Strata Logging Service (included in Strata Cloud Manager Pro).
† Requires Strata Cloud Manager Pro.

| Table 2: Strata Cloud Manager Privacy, Versions, and Requirements | |
|---|---|
| **Privacy** | |
| **Trust and Privacy** | Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our Privacy datasheet. |
| **Versions and Requirements** | |
| **Licensing** | Strata Cloud Manager is offered in two versions: **Essentials** (free) and **Pro** (paid). Pro adds advanced features, such as enhanced analytics, predictive AI insights, automated workflows, and ADEM capabilities to help teams optimize security outcomes. |
| **Supported Apps** | Strata Cloud Manager is a unified cloud-delivered management and operations solution for all Palo Alto Networks network security products, including hardware and software NGFWs, Prisma Access, Prisma SD-WAN, and Cloud-Delivered Security Services. |
| **Requirements** | • To use Strata Cloud Manager for your NGFW subscription, you'll need Palo Alto Networks NGFWs running PAN-OS® 10.1 or later with telemetry enabled.<br>• For Strata Cloud Manager for SASE, you'll need to enable cloud management for your Prisma Access deployment.<br>• Some Strata Cloud Manager features require an active Strata Logging Service license with firewall log forwarding. |
| **Supported NGFWs** | All firewall models and form factors can be managed with Strata Cloud Manager. |
| **Hosting Location** | For information on Palo Alto Networks cloud infrastructure, visit our regional cloud locations page. |

## To learn more, check out the following resources:

- Strata Cloud Manager TechDocs and Getting Started guide
- Strata Cloud Manager LIVEcommunity

For an exclusive demo, free trial, or answers to your questions, use our Contact us form.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com



strata_ds_strata-cloud-manager_022125