Strata Cloud Manager

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

Network Security Has Become Increasingly Complex

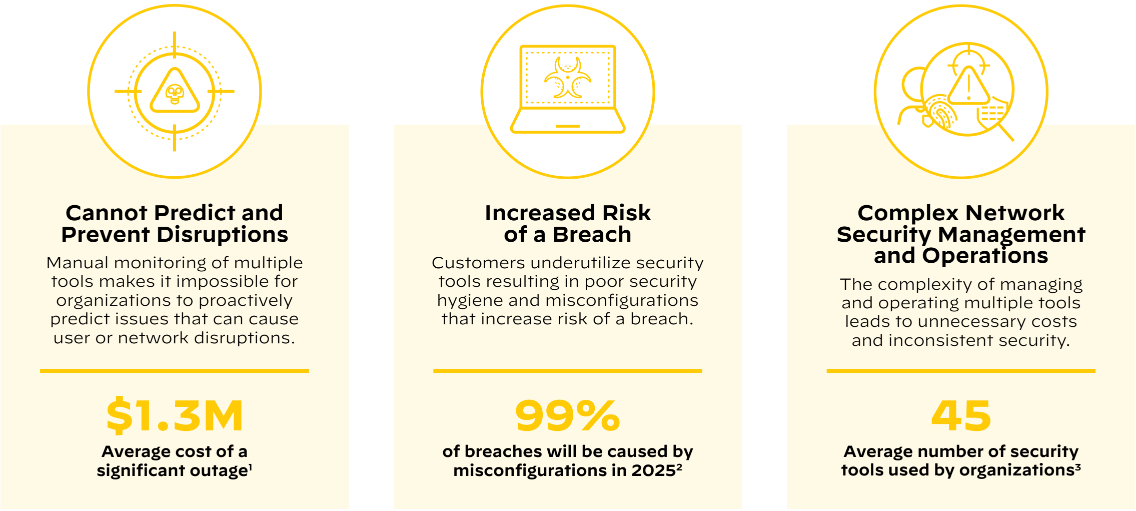
In today's digital landscape, the surge in data and devices is met with sophisticated cyberthreats that consistently outsmart traditional security measures. Adversaries are increasingly leveraging new techniques and technologies to launch more evasive and never-before-seen threats. Moreover, the expansion of the corporate network has complicated the network security stack, forcing organizations to manage and operate many point products and tools.

Sprawling corporate networks across multiple locations connect and support dispersed users working from diverse locations around the globe, and all of this is happening in the context of an evolving digital landscape where the rapid growth of network traffic and connectivity demands higher performance, flexibility, and protection.

Typical Solutions Can't Secure Modern Organizations

Typical network security management and operations solutions can't adequately secure modern organizations. Current approaches to network security management and operations lack predictive, actionable insights and integration across security tools, which leads to security gaps, inconsistent policies, and poor operational experiences. Specifically:

1. Predictive insights are often lacking, exposing vulnerabilities. When security tools face capacity issues, network disruptions can result in significant financial losses, averaging $1.3M per outage.[1]
2. Security teams struggle to optimize tool functionalities, leading to gaps in their security posture. Misconfigurations pose a significant risk, with Gartner predicting that 99% of firewall breaches through 2025 will be due to misconfigurations.[2]
3. Managing numerous security tools leads to gaps, inefficiencies, and higher costs. On average, organizations use 45 security tools,[3] contributing to unnecessary costs and inconsistent security practices.



Cannot Predict and Prevent Disruptions

Manual monitoring of multiple tools makes it impossible for organizations to proactively predict issues that can cause user or network disruptions.

$1.3M

Average cost of a significant outage[1]

Increased Risk of a Breach

Customers underutilize security tools resulting in poor security hygiene and misconfigurations that increase risk of a breach.

99%

of breaches will be caused by misconfigurations in 2025[2]

Complex Network Security Management and Operations

The complexity of managing and operating multiple tools leads to unnecessary costs and inconsistent security.

45

Average number of security tools used by organizations[3]

Figure 1: Significant management and operations challenges

Securing the modern connected organization requires an integrated, unified approach. To do this, security needs to be deployed and managed holistically through a platform with each component working together seamlessly and leveraging the power of AI to stay ahead of rapidly evolving threats. We intend to provide this with Strata Cloud Manager by Palo Alto Networks.

[1] *Cost of a Data Breach Report 2023*, IBM Security, July 2023.

[2] Charlie Winckless and Jay Heiser, *Risk-Based Evaluations of Cloud Provider Security*, Gartner, August 31, 2021.

[3] *Cyber Resilient Organization Report 2020*, IBM Security, June 30, 2020.

What Is Strata Cloud Manager?

Strata™ Cloud Manager is the industry's first AI-powered Zero Trust management and operations solution. Strata Cloud Manager revolutionizes network security management and operations, proactively preventing network disruptions and strengthening security in real time and across all enforcement points. Strata Cloud Manager enables security teams to:

- **Predict and prevent operational disruptions**: Security teams can forecast deployment health and proactively identify capacity bottlenecks up to seven days in advance with predictive analytics to prevent operational disruptions.
- **Reduce misconfigurations and increase best practices and security compliance**: Security teams can benefit from AI-powered analysis of policies and real-time compliance checks against industry and Palo Alto Networks best practices.
- **Centrally manage the entire network security estate**: For the first time, security teams can manage configuration and security policies across all form factors, including SASE, hardware and software firewalls, as well as all security services to ensure consistency and reduce operational overhead.

Business Benefits

- **Eliminate blind spots and identify problems**: Get unified visibility into all users, apps, infrastructure, and network connectivity.
- **Prevent potential disruptions**: Avoid preventable disruptions and reduce downtime. Strata Cloud Manager uses machine learning to predict up to 51% of disruptions to your NGFWs (based on support case analysis of a focused customer) before they impact you.
- **Reduce resolution time**: Reduce resolution time with remediation playbooks and automatic support tickets.
- **Maximize ROI on security investments**: Save tens of thousands of dollars by automatically detecting security gaps in your network.
- **Remediate misconfigurations**: Every month Strata Cloud Manager shares 715.5K misconfigurations for resolution.
- **Proactively improve security posture**: Strata Cloud Manager processes 77B metrics across 133K+ devices.
- **Achieve consistent security posture across NGFW and SASE**: Update a policy once for all deployments.
- **Increase productivity**: Increase productivity with automated configuration workflows.
- **Reduce operational burden**: Get an easy-to-use single interface with unified data from the entire deployment.

Key Capabilities

Proactive Health

Gain insights across your deployment and reduce NGFW and SASE downtime with proactive insights to maintain optimal firewall health, performance, and user experience. Strata Cloud Manager can intelligently predict firewall health, performance, capacity problems, flood detection, and many other problems up to seven days in advance based on machine learning powered by telemetry data and provide actionable insights to resolve the predicted disruptions.

For example, a sudden addition of hundreds of new users as part of company expansion combined with the introduction of new applications results in significantly high network processing activity, resulting in firewalls dropping traffic and slowing down the network. In these situations, security teams often struggle to cite the reason for failure. Strata Cloud Manager saves time in problem discovery and helps address the issue ahead of time. How?

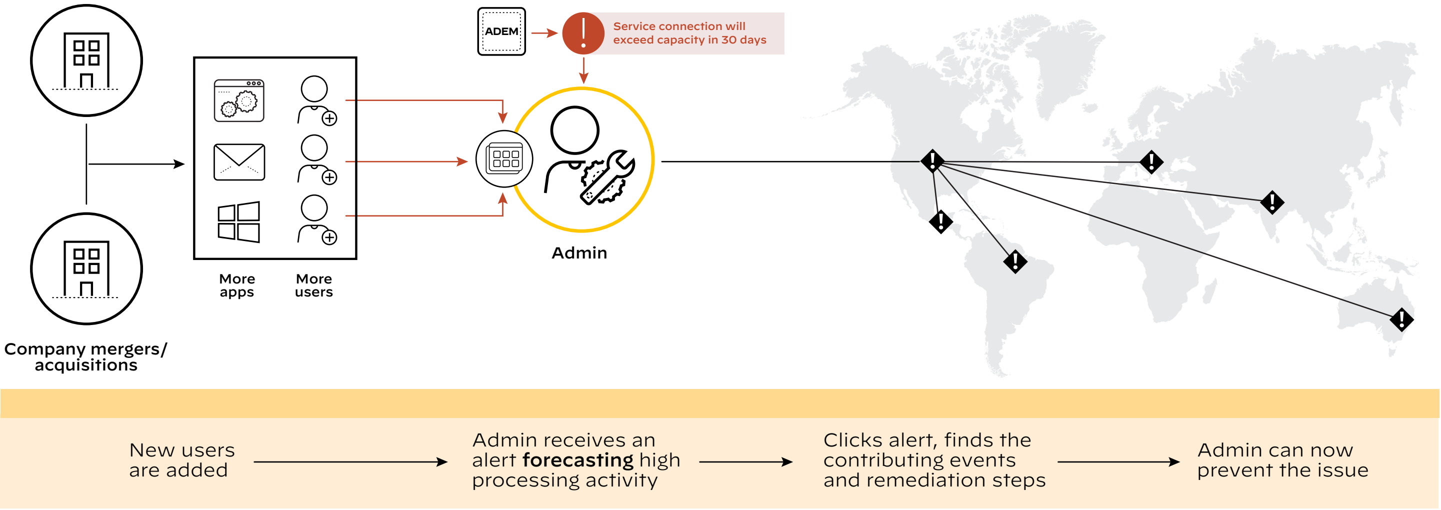
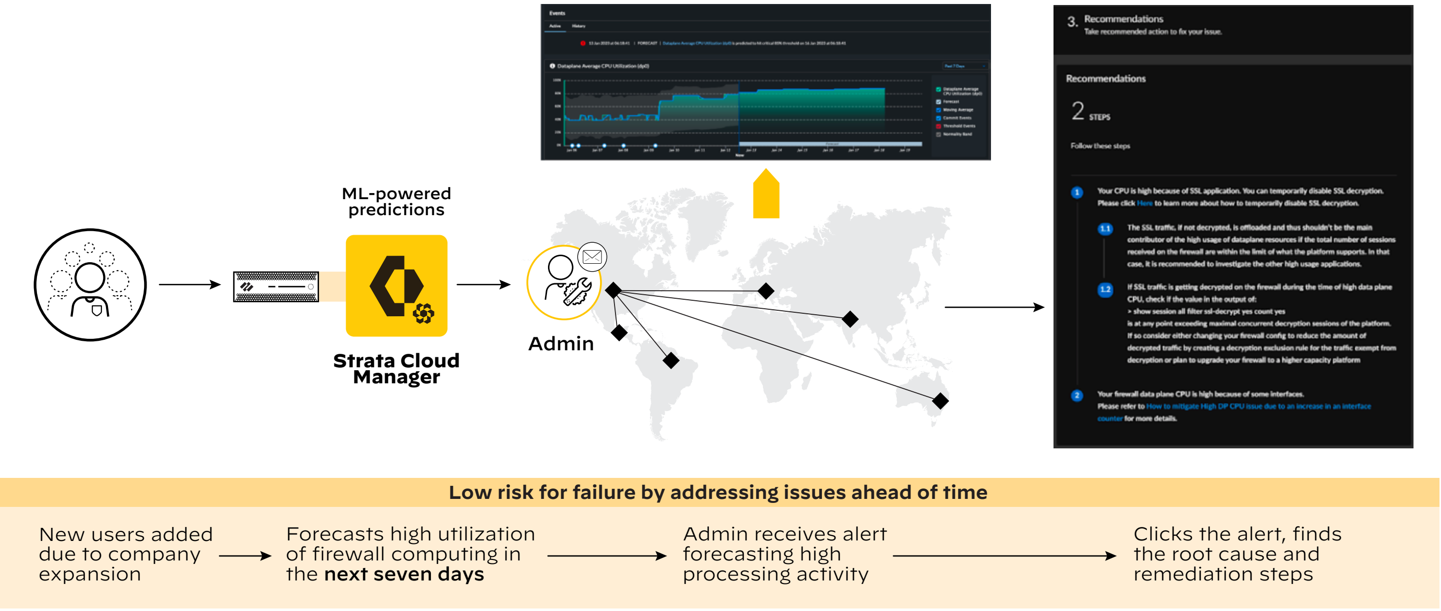

ADEM
Service connection will exceed capacity in 30 days
Company mergers/ acquisitions
More apps
More users
Admin
New users are added
Admin receives an alert **forecasting** high processing activity
Clicks alert, finds the contributing events and remediation steps
Admin can now prevent the issue

Figure 2: Forecast capacity requirements for growth

Strata Cloud Manager forecasts high utilization of firewall computing in the next seven days and sends an email alerting the concerned team. The alert cites the reasons for the potential issue with step-by-step recommendations either in the form of CLI commands or technical documentation links to remediate the issue. The predictive analytics capability gives the team a runway to prevent firewall disruptions before they become a problem and develops an effective strategy to optimize their usage. If the security teams cannot resolve the issue independently, a support ticket is automatically created in the context of the alert.


Events
Active
History
Dataplane Average CPU Utilization (dp0)
Past 7 Days
100%
80%
60%
40%
20%
0%
Jan 06
Jan 07
Jan 08
Jan 09
Jan 10
Jan 11
Jan 12
Now
Jan 13
Jan 14
Jan 15
Jan 16
Jan 17
Jan 18
Jan 19
Forecast
🟩 Dataplane Average CPU Utilization (dp0)
☑ Forecast
☑ Moving Average
☑ Commit Events
🟥 Threshold Events
☑ Normality Band
ML-powered predictions
Strata Cloud Manager
Admin
Low risk for failure by addressing issues ahead of time
New users added due to company expansion
Forecasts high utilization of firewall computing in the **next seven days**
Admin receives alert forecasting high processing activity
Clicks the alert, finds the root cause and remediation steps

13 Jan 2023 at 06:18:41 | FORECAST | Dataplane Average CPU Utilization (dp0) is predicted to hit critical 85% threshold on 16 Jan 2023 at 06:18:41

3. Recommendations
Take recommended action to fix your issue.

Recommendations

2 STEPS

Follow these steps

1. Your CPU is high because of SSL application. You can temporarily disable SSL decryption. Please click Here to learn more about how to temporarily disable SSL decryption.

   1.1 The SSL traffic, if not decrypted, is offloaded and thus shouldn't be the main contributor of the high usage of dataplane resources if the total number of sessions received on the firewall are within the limit of what the platform supports. In that case, it is recommended to investigate the other high usage applications.

   1.2 If SSL traffic is getting decrypted on the firewall during the time of high data plane CPU, check if the value in the output of:
   > show session all filter ssl-decrypt yes count yes
   is at any point exceeding maximal concurrent decryption sessions of the platform. If so consider either changing your firewall config to reduce the amount of decrypted traffic by creating a decryption exclusion rule for the traffic exempt from decryption or plan to upgrade your firewall to a higher capacity platform

2. Your firewall data plane CPU is high because of some interfaces.
Please refer to How to mitigate High DP CPU issue due to an increase in an interface counter for more details.

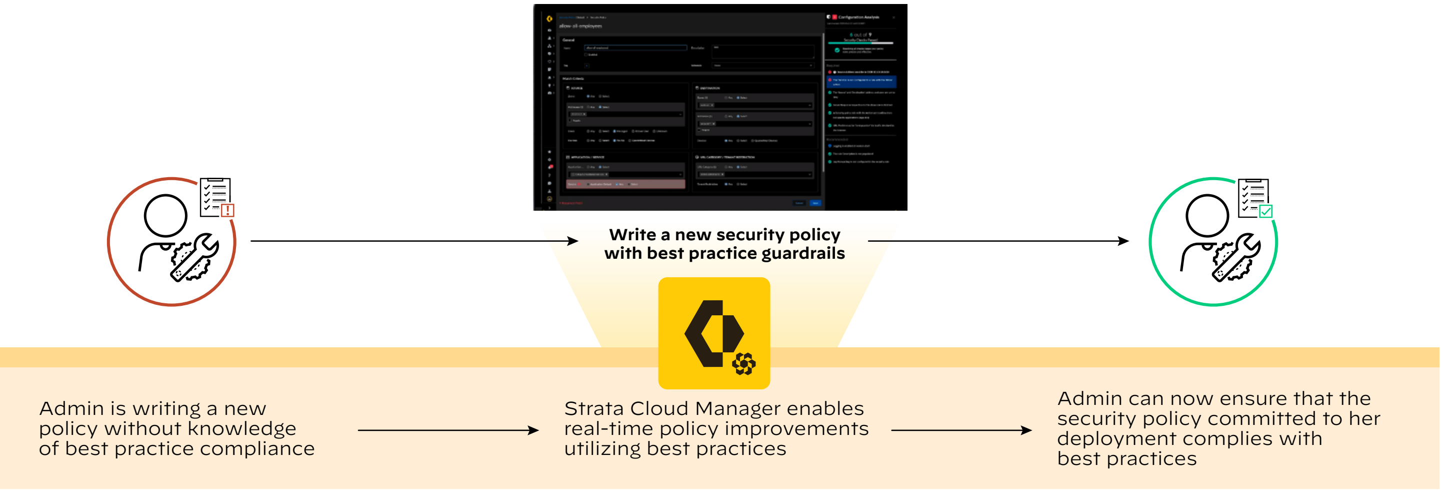
Figure 3: Forecast disruptions up to seven days in advance

Write Secure Configuration in Real Time

Strata Cloud Manager provides real-time best practice guardrails at the time of creating a new security policy. You have the confidence that the policy committed to the firewall automatically complies with best practices. By having secure policies right from the start, the need to react and review is eliminated and security risks are avoided. The result? A more streamlined and secure policy creation process, significantly reducing the risk exposure for your organization.

For example, Emily is writing a new policy and wishes there was a quick way to ensure that every policy she wrote got double-checked against best practices before she saved and committed the policy. Strata Cloud Manager enables real-time policy improvements utilizing best practices. Emily can now ensure that the security policy committed to her deployment complies with best practices. With Strata Cloud Manager:

- Configuration is analyzed in real time against a comprehensive set of best practices and customized guidelines.
- Misconfigurations can be prevented by alerting if a configuration drifts from best practices and information security guidelines.



Admin is writing a new policy without knowledge of best practice compliance

Strata Cloud Manager enables real-time policy improvements utilizing best practices

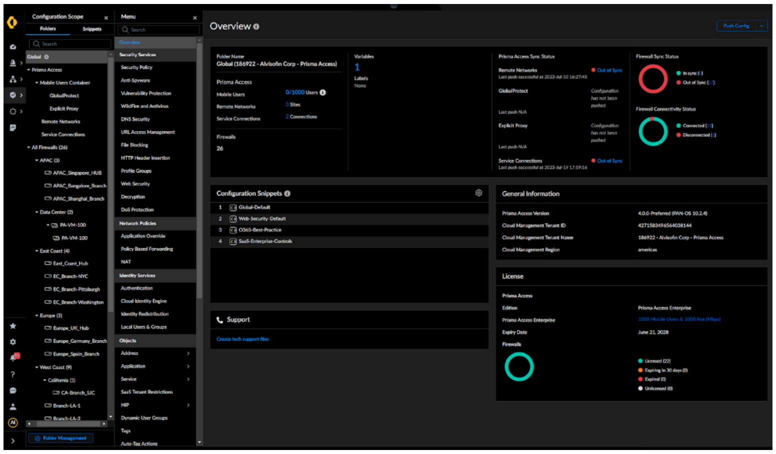
Admin can now ensure that the security policy committed to her deployment complies with best practices

Figure 4: Implement best practices at the time of security policy configuration

Consistent Configuration

Achieve consistent security posture across all deployments with flexible configuration organization. Here's how:

- Write common configurations using hierarchical folders and snippets.
- Update a policy once for all deployments.
- Achieve consistent security posture across NGFW and SASE.



Folder Name
Global (186922 - Alvisofin Corp - Prisma Access)

Prisma Access
Mobile Users 0/1000 Users
Remote Networks 3 Sites
Service Connections 2 Connections

Firewalls
26

Variables
1
Labels
None

Prisma Access Sync Status
Remote Networks ● Out of Sync
Last push successful at 2023-Jul-10 16:27:45
GlobalProtect Configuration has not been pushed
Last push N/A
Explicit Proxy Configuration has not been pushed
Last push N/A
Service Connections ● Out of Sync
Last push successful at 2023-Jul-19 17:19:16

Firewall Sync Status
● In sync ( )
● Out of Sync ( )

Firewall Connectivity Status
● Connected ( )
● Disconnected ( )

Configuration Snippets
1 Global-Default
2 Web-Security-Default
3 O365-Best-Practice
4 SaaS-Enterprise-Controls

General Information

Prisma Access Version	4.0.0-Preferred (PAN-OS 10.2.4)
Cloud Management Tenant ID	4271583496564038144
Cloud Management Tenant Name	186922 - Alvisofin Corp - Prisma Access
Cloud Management Region	americas

License

Prisma Access	
Edition	Prisma Access Enterprise
Prisma Access Enterprise	1000 Mobile Users & 1000 Net (Mbps)
Expiry Date	June 21, 2028
Firewalls	

● Licensed (22)
● Expiring in 30 days (0)
● Expired (0)
● Unlicensed (0)

Support
Create tech support files

Benefits

Write common configuration using hierarchical folders and snippets

Update a policy once for all deployments

Achieve consistent security posture across NGFW and SASE

Figure 5: Share configuration across NGFW and SASE

How Strata Cloud Manager Works

Strata Cloud Manager gathers extensive 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.

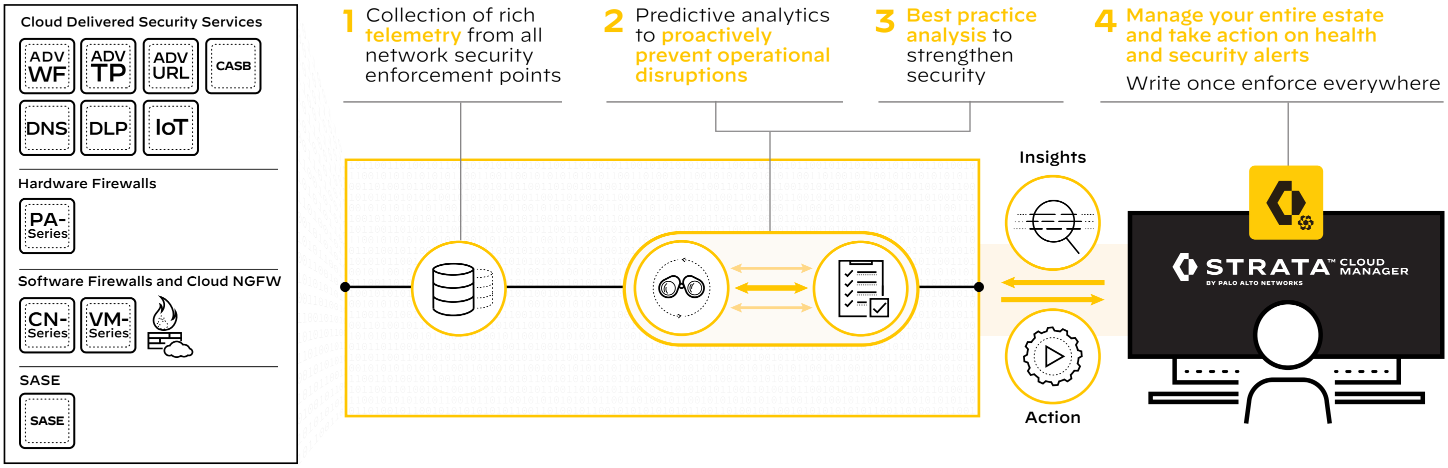

Cloud Delivered Security Services
ADV WF
ADV TP
ADV URL
CASB
DNS
DLP
IoT
Hardware Firewalls
PA-Series
Software Firewalls and Cloud NGFW
CN-Series
VM-Series
SASE
SASE
1 Collection of rich telemetry from all network security enforcement points
2 Predictive analytics to proactively prevent operational disruptions
3 Best practice analysis to strengthen security
4 Manage your entire estate and take action on health and security alerts
Write once enforce everywhere
Insights
Action
STRATA™ CLOUD MANAGER
BY PALO ALTO NETWORKS

Figure 6: How Strata Cloud Manager works

Strata Cloud Manager

Forecast Resource Bottlenecks
Forecast deployment health and proactively identify capacity bottlenecks to prevent operational disruption.

Continual Health Monitoring and Analysis
Real-time monitoring of metrics and telemetry to optimize operational health and user experience.

Best Practices and InfoSec Compliance
AI-powered analysis of policies and compliance checks against industry and Palo Alto Networks best practices.

Unified Config Management Aligned with Best Practices
Manage your SASE, NGFW, and all security services from a single UI and enforce best practices inline with scalable configuration sharing for consistent security.

Comprehensive Security Visibility
In-depth security analytics and reporting across applications, users, threats, and device posture for your network security deployment

Figure 7: Key Strata Cloud Manager features

To learn more, check out the following resources:

- Strata Cloud Manager TechDocs and getting started guide
- Strata Cloud Manager product demo
- Strata Cloud Manager LIVEcommunity to ask questions

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