Small and Medium Enterprises Solution Guide—Medium

One Site and More Than 125 Employees

This solution guide aims to help you understand the cybersecurity use cases, market trends, and problems that Palo Alto Networks customers with one site and more than 125 employees face today while offering potential solutions to help meet their network security needs. For these clients, there are several use cases we typically see when evaluating and addressing their security needs, such as their threat landscape, internet perimeter, SaaS, and work from home.

Figure 1 depicts how these organizations are commonly structured and how different components of the solution are dispersed and need a single, unified, and easy-to-manage solution. Figure 1 also depicts an associated suite of preintegrated products needing to be set up, accessed, logged, and monitored as a whole, as opposed to many disparate suites of devices, logs, admin consoles, and alerts.

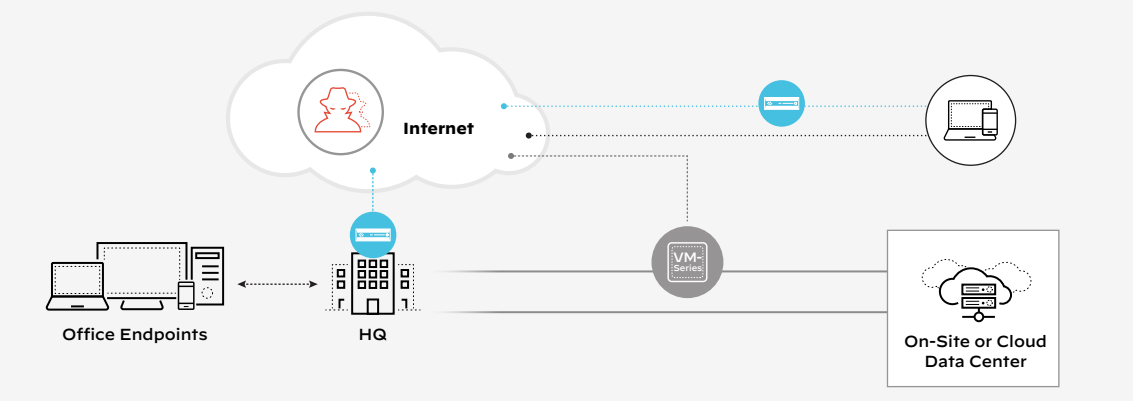

Figure 1: A single, unified, and easy-to-manage solution

What's not needed or very helpful are disparate devices, logs, systems, management and operational tools, or unstitched and difficult-to-correlate information, especially during a crisis.

Table 1 lists trends and problems for each use case that a security solution would need to address. A solution overview is covered at the end of this guide.

Use Cases

Table 1: Trends and Problems per Use Case

Use Cases and Description	Common Trends	Resulting Problems
Threat Landscape A company's external threat landscape; assessment of internal security system and processes; breach detection; and response	Adversary automation, 358% malware and 438% ransomware growth; significant cyber incidents continue to increase rapidly	Most dynamic threat landscapes we've ever seen; companies today average one serious issue every 12 hours; almost 30% of response cases today touch the cloud; cyberthreats are outpacing most enterprise security systems
Internet Perimeter Protecting internal networks and DMZ from internet threats	Growth of internet bandwidth, encryption, malicious malware, phishing, command and control, and ransomware	Increased threats, avenues, hidden download and uploads; access to malicious sites, command and control, and files
Private-Public Data Center Data needs to be located, stored, and accessed in-house and in the public cloud	Hosts in physical and virtual locations need to be isolated/protected from threats and unneeded access	Unknown protection of and access to the uploading and downloading of data, its contents, and its unauthorized transmission
SaaS/CASB Use of cloud SaaS apps, storage, and access	Unbridled number of business and personal SaaS apps are used, store critical data, and broadly share data internally and externally	Data can be bulk uploaded, downloaded, and contain sensitive, confidential and personal material as well as malware
Work from Home Work is now anywhere, and so is access to company systems and data	50% of US workers work from home, and 18% work from home part-time; the same device is used for personal and work tasks; traffic is encrypted	Easy to attack and weak device protection; unknown device posture; other devices are easy to breach and move laterally into the organization
Internet of Things Smart devices such as cameras, SCADA controllers, and screens, expand the threat landscape and increase breaches	Home and corporate IoT devices expand company risks and broaden avenues to breach organizations	Easy to find and employ IoT device vulnerabilities; easy to laterally move onto corporate devices, especially when devices share a network

Easily deploy, manage, and operate a complete and single system of devices to collectively secure networks, hosts, endpoints, and remote site/users regardless of location and mobility. A true security solution provides for common security policies, decryption, logs, operational management of events (not alarms), and deployment flexibility without compromising the aforementioned items.

Highlights of a Palo Alto Networks Solution

Unit 42-Backed and Built Threat Landscape Technologies and Services

Unit 42 offers three primary value-added services to discover, assess, and respond to threat adversaries and their exploitation of company system vulnerabilities. Xpanse is a service that provides an ongoing and constant mapping of a company's threat landscape from an external threat adversary's viewpoint (externally from the internet). Various assessment tools and services are also provided by Unit 42 to expose and tangibly determine a company's security posture and vulnerabilities so they can be known and addressed. Finally, Unit 42's expertise garnered from years of helping enterprises detect and respond to cyber breaches and ransomware is brought to bear as a Unit 42 breach detection and response retainer.

Unit 42's tools, services, and retainers offer businesses the opportunity to know their cybersecurity weaknesses and landscape to adversaries, resolve any weaknesses in their security posture, and plan for and react to breaches and ransomware. Taking advantage of these offerings is often helpful to prevent breaches and ransomware as well as costs a fraction of the cost associated with breach/ransomware impact on the business and its ability to recover from incidents.

Strata Network Security System

Palo Alto Networks Strata suite of physical and virtual NGFWs are the world's leading NGFW with Cloud-Delivered Security Services (CDSS) based on a patented single-pass architecture; App-, User- and Content-ID; predictable performance and a common OS deployed on hardware, virtual machine, and cloud-delivered NGFWaaS. They are deployed on-premises and on virtual devices/hosts on-premises and in public cloud environments such as GCP, Azure, and AWS to protect traffic flows to and from the internet, internal DMZ and server networks, as well as various public cloud networks and virtual machine environments.

Strata includes a suite of CDSS, such as Advanced Threat Protection, Advanced URL Filtering, Advanced WildFire, Advanced DNS Security, IoT, AIOps, SaaS, and other services. These advanced CDSS are shown to reduce breaches, malware, ransomware, command and control, etc.

SaaS Cloud-Delivered Security Service

This is a Palo Alto Networks NGFW cloud-delivered security service specifically built to help see, control, protect, and prevent access to and from SaaS applications. With the proliferation of SaaS apps, the SaaS CDSS uses machine learning and cloud intelligence to maintain a full understanding of the SaaS apps in use by the company's user population. It controls which SaaS apps can be used, tolerated, and blocked. It can also be tied into Palo Alto Networks cloud-hosted API SaaS tool to identify, classify, isolate, and prevent access to these files internally and externally. Together, the SaaS, CDSS and API products combine to deliver our next-generation CASB solution.

IoT Cloud-Delivered Security Service

This is a Palo Alto Networks NGFW cloud-delivered security service specifically built to help see, control, protect, and prevent access to an endless array of IoT devices. Most company networks average 30% of their devices as IoT devices. The IoT Security service uses machine learning to discover, group, and recommend IoT security policies based on IoT device, vendor, specific model, and even software release.

Work from Home

With so many users and sensitive workers at home, the home and its many IoT devices need true NGFWs to protect the site's many devices along with advanced endpoint software to provide breach and ransomware protection while being managed from a single system that provides a unified expanded detection and response (XDR) console.

Cortex XDR Endpoint and System-Wide XDR

Palo Alto Networks XDR provides independently tested and market-leading campus, cloud, mobile, and work-from-home endpoint protection for all endpoint operating systems, rich data logging and collection, as well as a cloud-hosted configuration manager. Work-from-home devices need to be protected from attack and ransomware.

XDR also extends its visibility and collection of data to NGFWs and other products from Palo Alto Networks and third-party suppliers resulting in XDR to incidents where detailed alarm details are collected and visualized in a graphical and easy-to-understand causality chain.

Services

Should customers require experienced help, partners and distributors have a full line of services consisting of jump-start and deployment programs, ongoing support, training, and managed services offerings that utilize both automation and certified engineering teams to ensure customers achieve their desired outcomes on budget.

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