Small and Medium Enterprises Solution Guide—Large

Multiple Sites 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 more than 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 in need of 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.

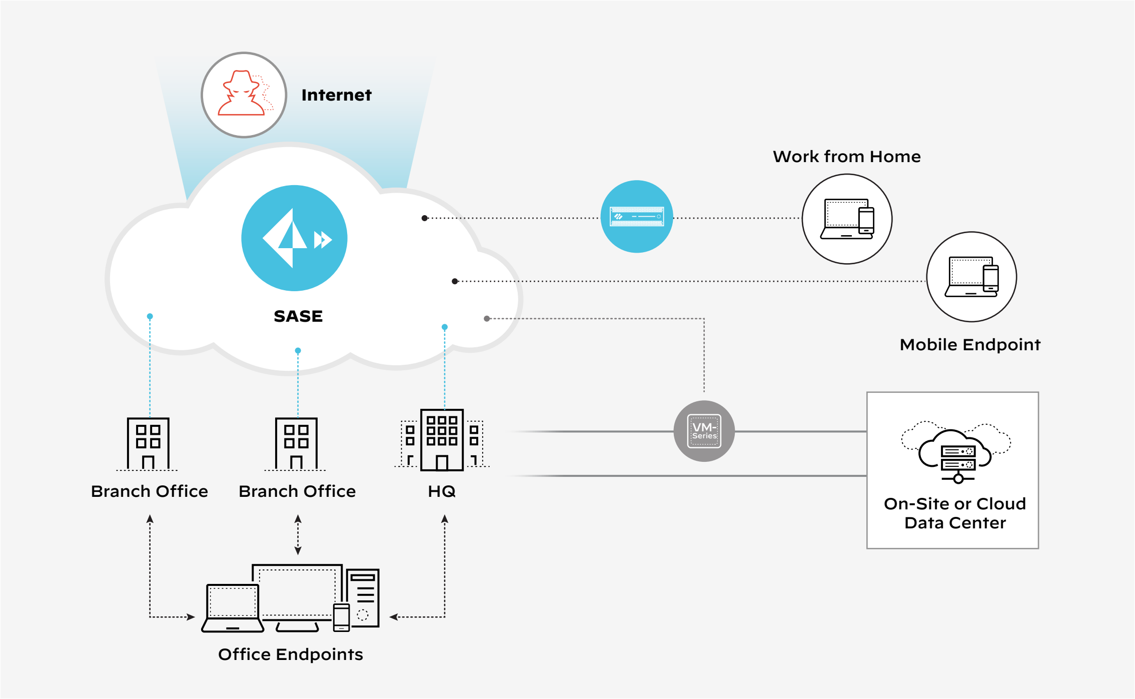

Figure1: A single, multisite, unified, and easy-to-manage solution

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 a security solution would need to address. Solution highlights are covered at the end of this document.

Use Cases

Table 1: Use Cases, Trends, and Problems

Use Cases and Description	Common Trends	Resulting Problems
Threat Landscape 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 1 serious issue every 12 hours; almost 30% of response cases today touch the cloud; cyberthreats are out-pacing 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 downloads 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 and protected from threats and unneeded access	Unknown protection of and access to data upload and download, its contents, and 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

Table 1: Use Cases, Trends, and Problems (continued)		
Internet of Things (IoT) Smart devices such as cameras, SCADA controllers, screens, etc. 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
Work from Home (WFH) Work is now anywhere along with access to systems and data	50% of US workers WFH and 18% WFH part-time; personal and work use same device; traffic is encrypted	Easy to attack, weak device protection, and unknown device posture; other devices easy to breach and move laterally into org
Secure Access Service Edge (SASE) Secure access service edge is cloud-delivered "secure" access for mobile/WFH user devices and connected branches/sites	WFH is the norm post-COVID; workloads are in physical and in many public clouds; SaaS apps are the norm; secure and high-performance access is a mandate	HQ-based VPN concentrators, URL filtering, and data centers are now dispersed in the cloud and/or SaaS based; access and security must now save money and provide better user experiences and performance

Easily deploy, manage, and operate a complete and single system of devices to collectively secure networks, hosts, endpoints, and remote sites regardless of location and mobility. A true security solution provides for common security policies, decryption, logs, the 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 a snapshot-in-time 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 at 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 zero-day WildFire, Advanced DNS, 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 (ML) and cloud intelligence to fully understand the SaaS apps used by the company's user population. It enables control over which SaaS apps can be used, tolerated, and blocked. It also can be tied into Palo Alto Networks cloud-hosted SaaS API 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 companies' networks average 30% of their devices as IoT devices. The IoT security service uses ML to discover, group, and recommend IoT security policies based on IoT device vendor, specific model, and even software release.

Prisma SASE/Work From Home

Palo Alto Networks SASE offers a cloud-delivered and highly available user mobility and branch network connectivity and security solution as a service. Built on leading public cloud providers' data centers across the globe, Prisma SASE offers the full complement of NGFW and CDSS spun up in the cloud for each client to uniquely connect and secure their mobile users and company buildings/sites.

Prisma SASE often solves VPN, content web filtering/secure web gateway, and branch interconnect issues and problems (or any combination) through a common cloud-delivered service based on Palo Alto Networks world-leading Strata NGFWs and CDSS. It saves customers the need to hire, staff, select, procure, and maintain up to eight different vendor products and services—all via cloud-delivered and dynamically scalable security processing units in the public cloud.

Cortex XDR Endpoint and System-Wide Extended Detection and Response

Palo Alto Networks XDR provides independently tested and market-leading endpoint protection for all endpoint operating systems, rich data logging and collection, as well as a cloud-hosted configuration manager.

XDR extends its visibility and collection of data to NGFWs, Prisma Access, and other products from Palo Alto Networks and third-party suppliers resulting in extended detection and response to incidents where 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