Small and Medium Enterprises Solution Guide—Small

One Site and Fewer 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 fewer 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 presents 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.

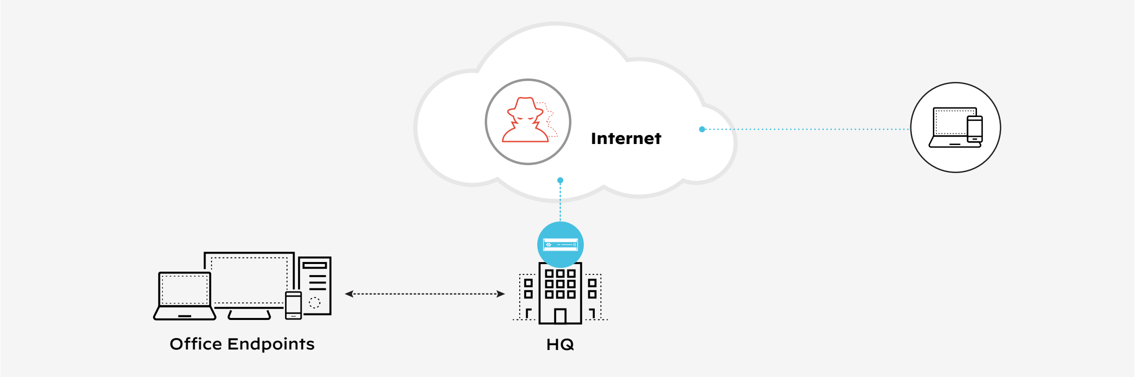

Figure 1: A single, unified, and easy-to-manage solution

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 the 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, Common Trends, and Resulting Problems

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 1 serious issue every 12 hours; almost 30% of response cases today touch the cloud; cyberthreats 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 downloads and uploads, access to malicious sites, command and control, and files
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 (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 the same device; traffic is encrypted	Easy to attack, full of known issues and have weak device protection; device posture unknown; difficult for company to control personal devices

Easily deploy, manage, and operate a complete and single system of devices to collectively secure networks, hosts, endpoints, and WFH networks regardless of location and mobility. A true security solution provides for common security policies, decryption, logs, operational management of events (not a bunch of 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 the company system's vulnerabilities. Xpanse is a service that provides a quarterly or 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, resolve any weaknesses in their security posture, and plan for as well as react to breaches and ransomware. Taking advantage of these offerings is often helpful in preventing breaches and ransomware. They are also 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 NGFWs is 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 public cloud virtual machines.

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 and cloud intelligence to maintain a full understanding of the SaaS apps in use by the company's user population. It enables control over 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.

Work from Home

In this design, WFH commonly consists of a few laptops that work from home while mobile or in the office. In this scenario, the GlobalProtect CDSS is often used to create VPN tunnels from the computer to the NGFW, so all traffic is inspected and secured, similar to any computer behind the NGFW. Additionally, this allows for unified security policies, logging, and system management. If and when WFH becomes more important (such as for executives), small, affordable NGFWs can be employed and inherit perimeter security policies from the HQ NGFW.

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.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
www.paloaltonetworks.com