Bringing Zero Trust Security to the Public Cloud

Virtual Firewalls Play Essential Roles in Multitiered Defenses

paloalto NETWORKS | STRATA BY PALO ALTO NETWORKS

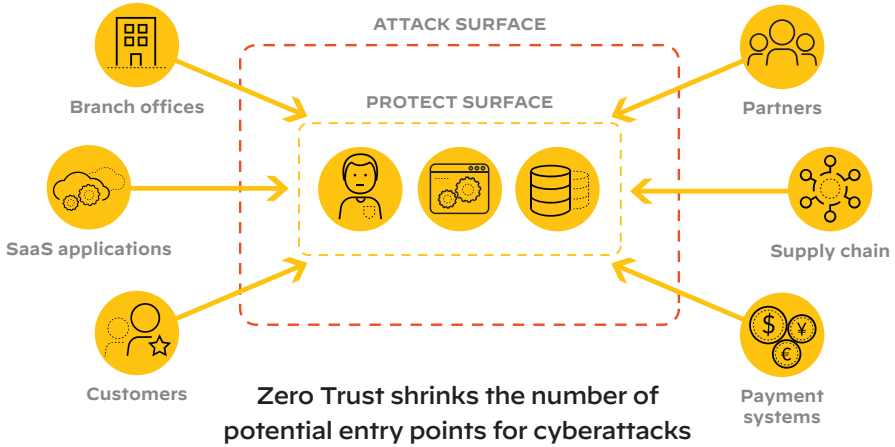
Table of Contents

Never Trust, Always Verify

The old proverb "trust but verify" was made famous by U.S. president Ronald Reagan in December 1987 after the signing of the Intermediate-Range Nuclear Forces (INF) Treaty with Mikhail Gorbachev. The phrase seems self-contradictory: if you trust someone, what is there to verify?

The actual principle of the treaty was "never trust, always verify," which is also the guiding principle behind Zero Trust in cybersecurity. In a Zero Trust architecture, your network location is not a primary criterion for trust. Instead, every device, user, application, and network flow is considered a potential threat and therefore must be authenticated and authorized.[1]

Zero Trust embodies a fundamental shift in security strategy. Legacy security revolves around the concept of the **attack surface**—the sum total of the devices and connections hackers could potentially use to penetrate network defenses. Zero Trust turns that notion on its head by shifting the emphasis from the attack surface to the **protect surface**, which consists of the data, applications, assets, services, and infrastructure that must be protected. The protect surface is orders of magnitude smaller than the attack surface and far easier to determine.



Now let's bring cloud into the conversation, starting with a breakdown of the three flavors of public cloud.

Flavors of Public Cloud

While people often talk about the public cloud as though it were one thing, that's not the case. Public cloud is an umbrella term that covers three distinct models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

Software as a Service (SaaS)

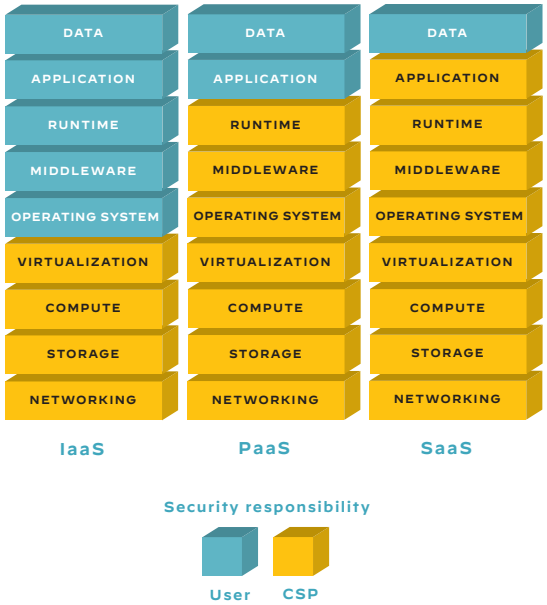
SaaS is familiar to most corporate users in the form of applications such as Salesforce CRM, Adobe Creative Cloud, Google Docs, and Microsoft Windows 365. In this public cloud model, the customer owns the data, while the cloud service provider (CSP) is responsible for everything else, from networking to the application itself.

Platform as a Service (PaaS)

Software developers are the primary users of PaaS. In contrast to SaaS, the customer owns both the data and the application in PaaS. Some popular PaaS services include AWS Elastic Beanstalk, Windows Azure, Google App Engine, and Red Hat OpenShift.

Infrastructure as a Service (IaaS)

IaaS is by far the most common model for public cloud usage today, offered by large providers such as AWS, Microsoft Azure, Google Cloud, and Alibaba. In IaaS deployments, the provider offers the networking, storage, and computing infrastructure resources, while you need to run and maintain your OS, middleware, runtime, applications, and data.



Security models for the three flavors of public cloud

Public cloud security is complicated because you and the cloud provider share ownership of the security within the stack, as the next section will explain.

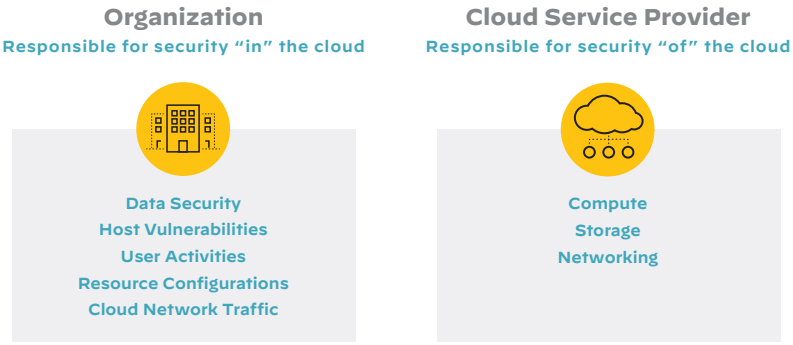
The Shared Responsibility Model

In an on-premises or private cloud model, you own the entire stack from the physical hardware to the applications and data—and everything in between. When it comes to security, there's never confusion about who is responsible—it's all yours, all the time.

Things are not so straightforward in the public cloud where security follows a shared responsibility model. The cloud service provider secures the platform foundation. This encompasses the hardware and software that provide the networking, storage, computing, and virtualization services—as well as standard operating systems, such as Red Hat Enterprise Linux (RHEL) and Windows Server.

For your part, you must secure the middleware, runtimes, applications, and data. If you use a non-supported operating system, that too falls into your area of responsibility. Essentially, the provider is responsible for security "**of the cloud**," while the customer is responsible for security "**in the cloud**."

To make shared responsibility work well, you and the CSP need to collaborate to avoid security gaps at the "seams" where the two areas of responsibility intersect.



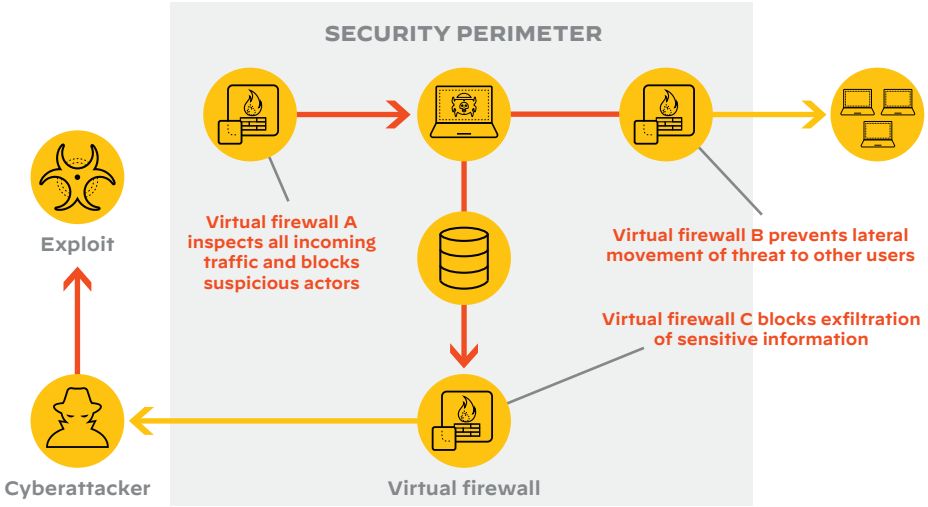
Division of security responsibilities in the public cloud

It's important to remember that Zero Trust is a set of principles, not a specific tool or architecture. The next section explains the important role virtual firewalls play in implementing a Zero Trust architecture.

Virtual Firewalls: Essential for Public Cloud

The next-generation firewall (NGFW) serves as the cornerstone of modern network security, guarding against network and transport level threats (layers 3 and 4 of the OSI model) and application level (layer 7) attacks such as distributed denial of service (DDoS), HTTP floods, and SQL injections. Until recently, NGFWs were deployed solely as physical appliances, an approach that works well in traditional physical client/server application data centers. However, you can't deploy hardware in today's dynamic multi-cloud environments—each CSP owns its own infrastructure.

Virtual firewalls—software NGFWs—are the response to public cloud security needs. Virtual firewalls have all the capabilities of physical devices with the added benefit of automatically following the dynamic nature of applications and workloads within the virtualized environment.



Virtual firewalls offer defense-in-depth protection against cyberthreats

The need for regulatory compliance is just as critical for public cloud as with on-premises deployments. However, the way that you get there is significantly different, as the next section explains.

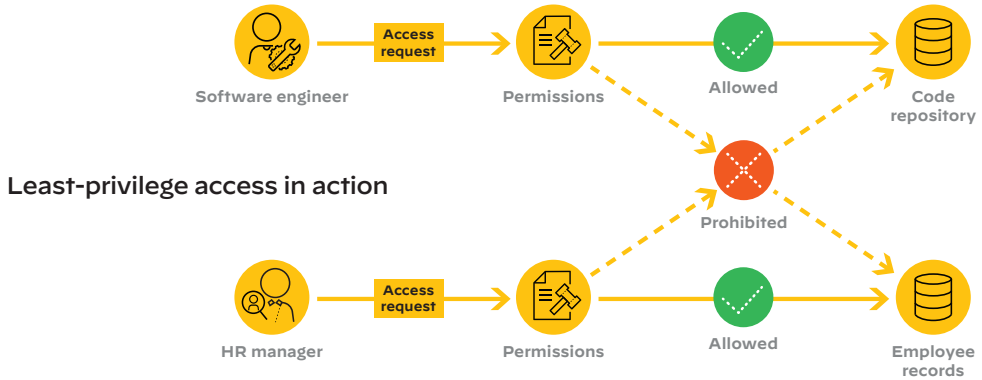
Cloud Environments Strain Existing Compliance Frameworks

Companies in highly regulated industries face considerable risk exposure if they fail to comply with stringent regulations and standards such as HIPAA in healthcare, PCI DSS2 in retail, and ACH3 in banking. Moving applications and data from an on-premises data center to the public cloud can significantly impact compliance strategies.

Fortunately, CSPs are ready and able to partner with your organization's compliance program. For one thing, you can "inherit" the security controls the CSP uses on its own infrastructure, which strengthens your own compliance and certification programs. Most CSPs allow you to use their activity monitoring services to detect configuration changes and security events across your system, even integrating their services with your existing solutions to simplify compliance reporting.

Developing an effective strategy for compliance in cloud environments requires changes to the security system. Security managers need centralized security management so they can harmonize policies across the entire cloud environment and even complex multiple cloud deployments. In order to meet regulatory compliance requirements, security teams need to be able to harmonize the management and security posture across all public cloud environments, something the CSPs are not set up to do.

In addition, access control should be tightened with policies such as least-privilege access and multifactor authentication. In least-privilege access, users are assigned only application permissions needed to fulfill the job duties of their organizational roles. For example, a software engineer needs access to the code repository but is prohibited from accessing employee records. Not surprisingly, those permissions are reversed for HR managers.

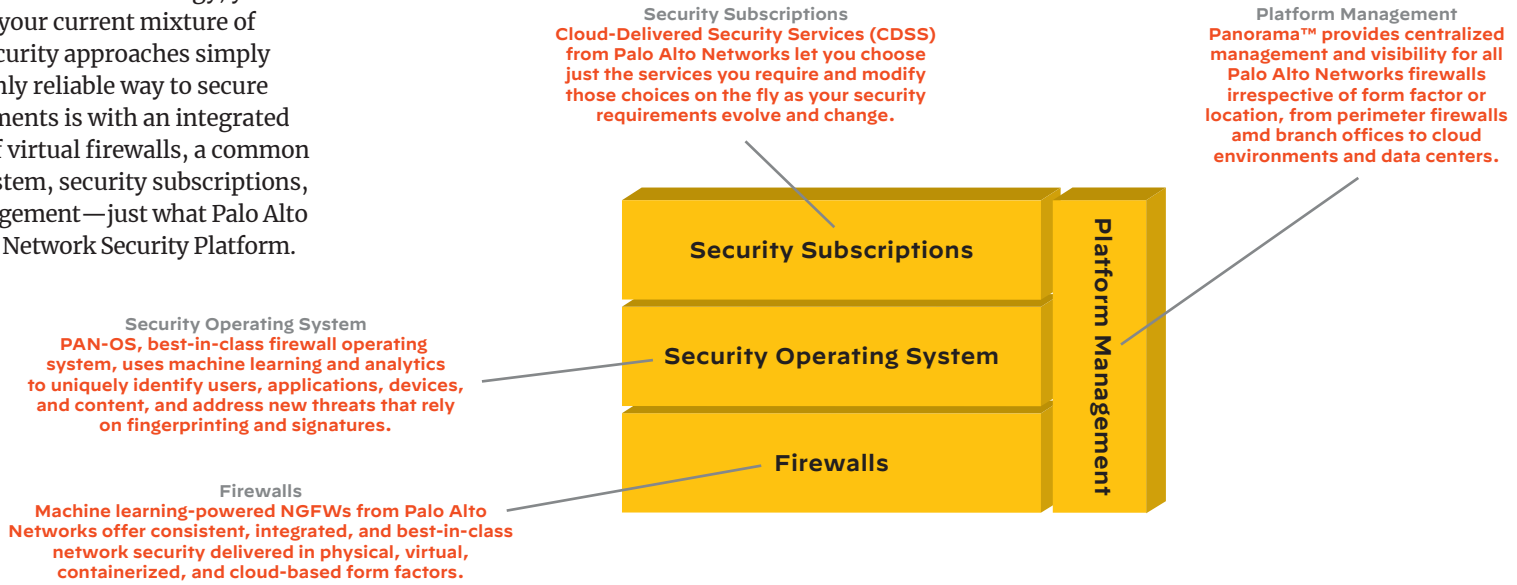


Least-privilege access in action

With so many challenges, you may be wondering just how you can ever implement effective public cloud security. If so, the next section will soon be your new best friend.

Architecture of the Network Security Platform

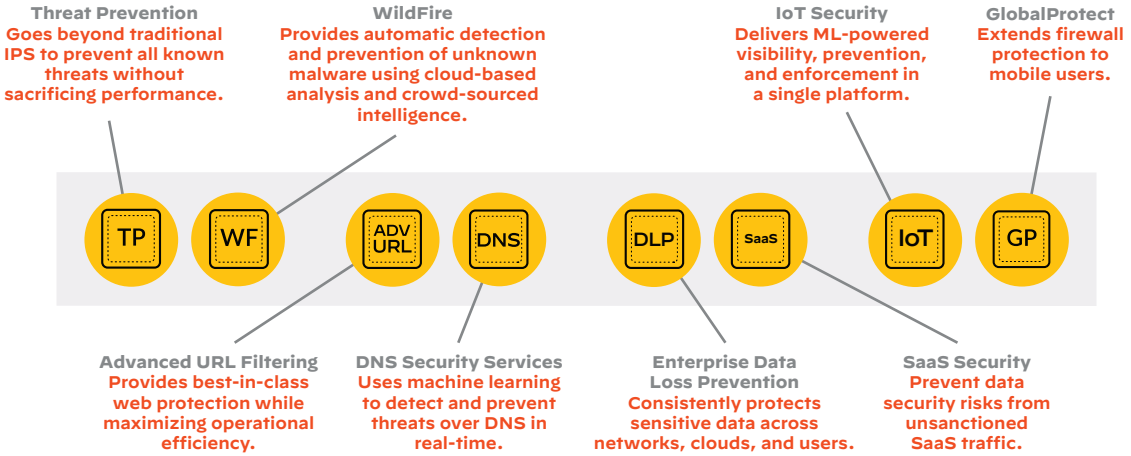
Once you commit to a Zero Trust strategy, you will quickly find that your current mixture of multiple tools and security approaches simply aren't enough. The only reliable way to secure public cloud environments is with an integrated offering consisting of virtual firewalls, a common firewall operating system, security subscriptions, and centralized management—just what Palo Alto Networks offers in its Network Security Platform.



In dynamic cloud environments, security requirements often change.
The Network Security Platform allows you to respond by adding security services easily, as discussed next.

Cloud-Delivered Security Services for the Network Security Platform

The Network Security Platform offers a full range of Cloud-Delivered Security Services specifically designed to complement and enhance each other so that you can confidently secure all traffic that transverses all your networks and clouds. While some competitive solutions bundle services—forcing you to buy services you don't really need—the Network Security Platform gives you complete flexibility. Select just the services you need today, then add and subtract services later as your security requirements evolve.

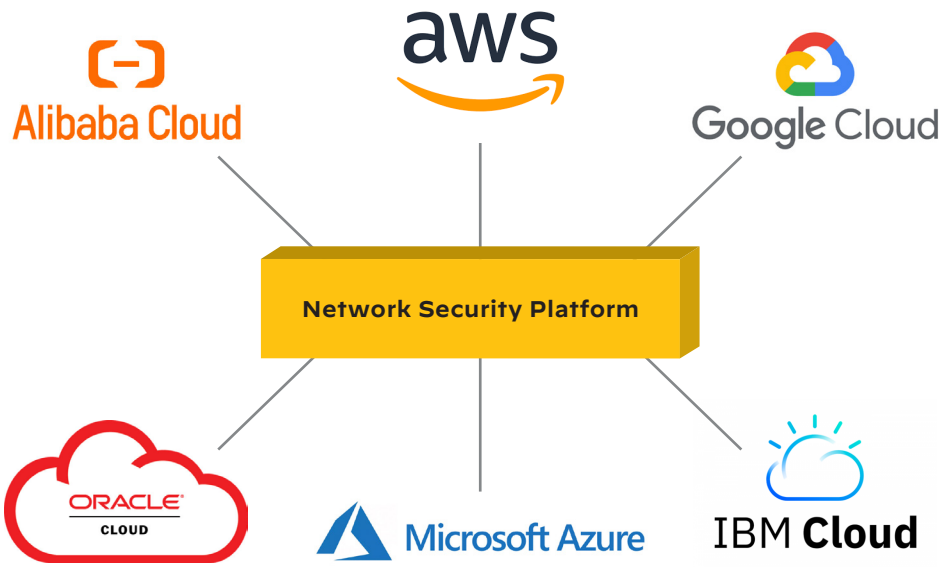


The trend toward multiple cloud environments requires the flexibility to mix and match offerings from different CSPs—no vendor lock-in. Learn more in the next section.

CSPs Supported by the Network Security Platform

The public cloud marketplace is highly competitive—some would say cutthroat. Savvy organizations can leverage this dynamic to negotiate more favorable contracts and move between CSPs to gain access to emerging technologies faster.

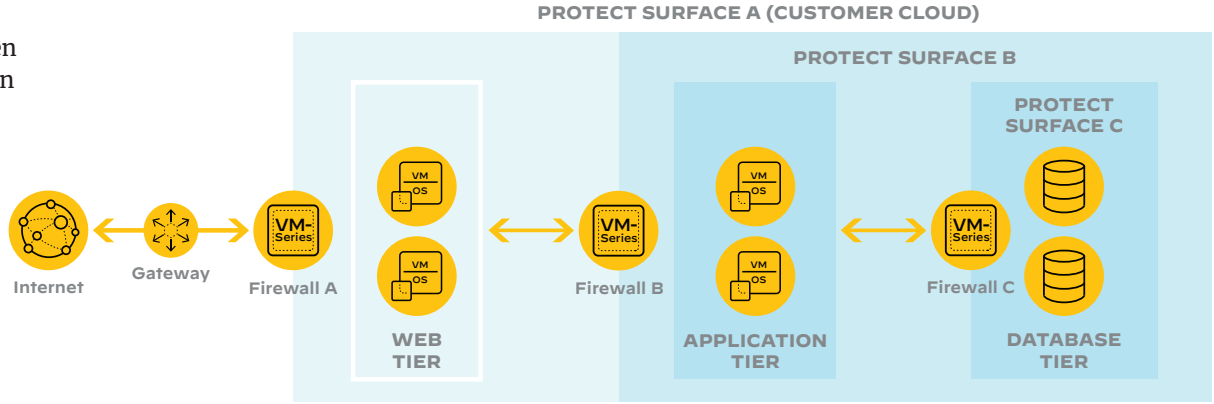
The Network Security Platform integrates smoothly with all major public cloud providers. This means you can choose the provider—or providers in the case of multi-cloud environments—that best meets your requirements with confidence, knowing Palo Alto Networks can help you secure your part of the shared responsibility model of any cloud, multi-cloud, and hybrid-cloud environment.



It's time to put it all together and see how Zero Trust works in the real world—our next topic.

Zero Trust Security for Defense in Depth

An earlier section of this e-book explained the shift from attack surface to protect surface when implementing Zero Trust. In the example shown at right, three VM-Series firewalls and Cloud Delivered Security Services (CDSS) are used to secure a multitiered application architecture consisting of web, application, and database tiers. Each VM-Series virtual firewall essentially creates a well-defined protect surface. The gateway firewall inspects and secures incoming and outgoing traffic, while the application tier firewall controls access to the private subnet containing the application and database tiers. The final piece of the in-depth security consists of a microsegmentation approach—implemented by a firewall—that puts an additional level of protection between the database and the rest of the infrastructure.



Multitiered protection of public cloud applications using VM-Series virtual firewalls

With that brief overview of the technology under your belt, let's get to the heart of the matter—how the Network Security Platform delivers tangible business value and impressive ROI.

Business Value—ROI, Staff Productivity

Organizations implement Zero Trust for security reasons and business impact. The benefits of the Network Security Platform include maximizing the return on security investments, mitigating the impact of skills shortages, speeding up threat responses, and improving the user experience. Let's take these benefits in order:

Rapid ROI

In the past, security professionals often focused on the protective aspects of security investments and considered financial considerations to be secondary matters. Now organizations are demanding more, pushing CISOs to protect data and other valuable "soft" assets in ways that make the most of tight security budgets. A recent Forrester Consulting study found that VM-Series Virtual Firewalls deliver 115% ROI over three years with a six-month payback period.[2] The same survey showed a 30% reduction in the time to achieve proper security posture.

115%

ROI
6-month playback

30%

Reduction
in time achieving a proper security posture

Moving to the cloud shifts capital expenses (CapEx) to operational expenses (OpEx). Instead of buying hardware and software, you effectively lease the assets from the CSP. The burden of procuring, installing, operating, and maintaining the infrastructure now falls on the CSP, freeing your people and capital for other assignments.

Cybersecurity Skills Gap

Network security management has traditionally been a labor-intensive activity, which is a problem given the current shortages in IT staff positions—especially security professionals—across the industry. A recent survey showed that more than 2.7 million positions are unfilled and that the workforce would need to grow by 65% annually to ensure adequate staffing.[3]

Not surprisingly, organizations are not counting on such phenomenal growth and instead are looking at other ways to address the human resource shortages. Technology is at the top of the list: 38% of organizations are using cloud service providers to shift workload out of the organization's owned data center infrastructure to reduce the amount of staff time needed to operate, maintain and refresh the computing infrastructure.[4]

Now that we've covered ROI and staff productivity, let's take a look at how the Network Security Platform provides value by boosting threat response and enhancing the user experience in the next section.

Business Value—Threat Response, User Experience

Effective Threat Response

One of the biggest challenges for public cloud security is the highly dynamic nature of the threat landscape. Not only are attackers launching new and more sophisticated threats, they also modify existing ones to bypass current security measures. As a result, the security team can never wash its hands and declare "mission accomplished."

The Network Security Platform delivers security services using a modular, cloud-based approach, which allows security professionals to respond rapidly and effectively to changes in the threat environment as well as the organization's architecture. For example, assume that you receive a tip that someone is exfiltrating proprietary information using a USB drive. If you consider the threat to be credible, your team can deploy Data Loss Prevention (DLP) literally in minutes to beef up defenses against this insider threat.

Improved User Experience

Organizations have high expectations for their CIOs and CISOs, and none higher than the mandate to keep their infrastructures operating at peak performance to support the employees, vendors, contractors, and others who depend on the network to do their jobs. Anything that interferes with access to business-critical applications and data—from network slowdowns and outages to data exfiltration exploits and ransomware attacks—can degrade productivity, morale, and innovation.

However, the outside world constitutes another user community whose experience matters. When customers come to your website, they expect to find the information and services that they need quickly and accurately. If the website is down or slow, they likely won't come back. And it gets worse. If your visitors are infected with malware or have their personal data stolen due to inadequate security on your end, you could be subject to severe financial and regulatory penalties—and there goes your brand.

Zero Trust is admirably positioned as the antidote to these potential problems. The integrated Network Security Platform manages security in a unified, holistic way, meaning that all parts of the security infrastructure work together to maximize protection and minimize disruptions. In most cases, users are unaware that the platform even exists—the best possible outcome.

Congratulations! You've walked through this e-book tour showing the essentials Zero Trust in public clouds. Now it's time to take action. Head to the next section to see how to get started.

Your Next Steps for Zero Trust Security

Moving your valuable information and applications to the public cloud creates new security challenges. Fortunately, there are solutions at hand from Palo Alto Networks. Our VM-Series virtual firewalls are the essential building blocks for creating a multitiered Zero Trust Architecture that defends against zero-day and other threats, improves the user experience, delivers impressive ROI, and significantly reduces user downtime by as much as 67%.[5]

Migrating applications to the public cloud involves risk. Implementing a Zero Trust Architecture aims to reduce risk and secure your critical business needs and requirements. Be sure to read the just-released total economic impact (TEI) report by Forrester Consulting to learn more about ROI and other economic benefits of our virtual firewalls. Or simply see your potential savings with this easy-to-use virtual firewall ROI calculator based on the Forrester Consulting study.

And we're here to help you mitigate risks. Our security experts will be happy to give you a personalized demo and answer your questions about public cloud security. Schedule your demo today.

---

1 Chapter 1: Zero Trust Fundamentals, from Zero Trust Networks
2 The Total Economic Impact™ of Palo Alto Networks VM-Series Virtual Firewalls, Forrester Consulting, Commissioned by Palo Alto Networks, October 26, 2021
3 A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)2 Cybersecurity Workforce Study, 2021.
4 Ibid.
5 The Total Economic Impact™ of Palo Alto Networks VM-Series Virtual Firewalls, Forrester Consulting, Commissioned by Palo Alto Networks, October 26, 2021

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