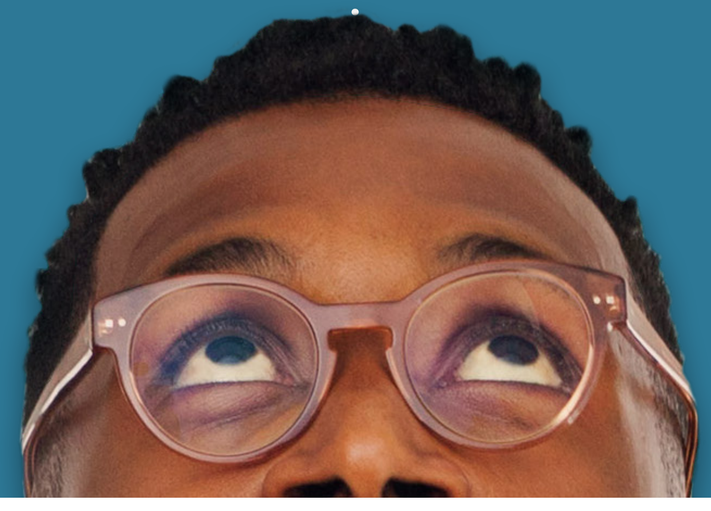
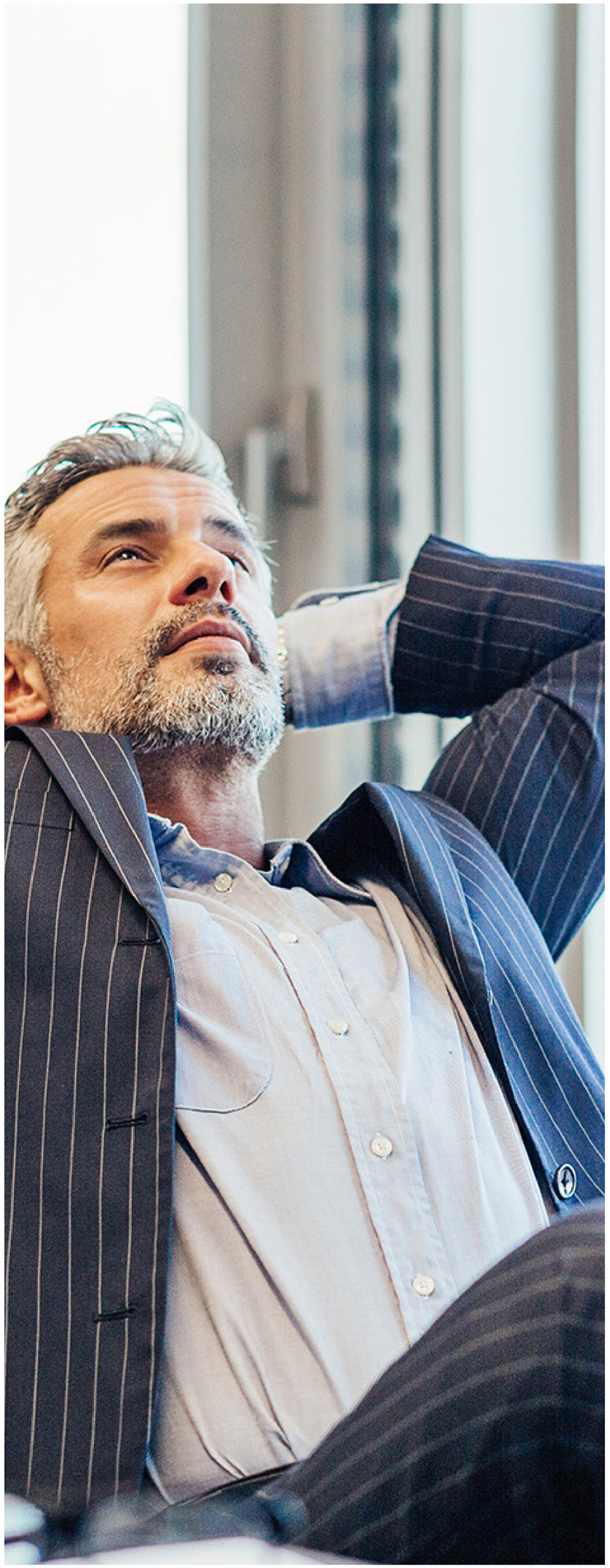
CLOUD SECURITY
FOR A GOOD NIGHT'S SLEEP

SECURITY STRATEGIES FOR MODERN COMPUTING



Microsoft | paloalto NETWORKS



INTRODUCTION

Whenever technology makes an advance, criminals and bad actors are already there, waiting to capitalize on it. And you can be sure, hackers are already in the cloud, waiting to plunder the unprepared and the careless. In just the last year or two, the cyberthreat landscape has shifted dramatically with accelerated adoption of cloud and modern computing solutions. Applications and data are everywhere now. Laptops, tablets, smartphones, even everyday devices on the internet of things are being used as gateways for illicit access. But many organizations are still trying to get cloud security off the ground.

In 2017, the occurrence of security incidents specific to the public cloud increased dramatically. A visit to the dark web would uncover thousands of pre-compromised resources for sale. These assets include hacked servers running in customer accounts. They sell for tens of thousands of dollars because they provide easy access to user and admin rights within valuable target companies. This is one way hackers are monetizing access to data and apps unlocked within public cloud platforms. Compromised applications and services exposed data from nearly 27,000 compromised instances across all cloud environments. In another example, a commonly used search engine was found to be compromised and serving up PoS malware created and used in 2012, highlighting the efficiency with which hackers will operate. Then there were the 200 million voter records exposed from a well-known public cloud storage service. The list goes on. We've heard it in the news and we will continue to do so as we move forward.

But with all the technological advances and all the evolving threats and tales of cybercrime, the basic job and goal of IT security professionals has not changed:

Protect your data and sleep soundly.

That goal of worry-free security requires that we all learn from and adapt to threats that will keep evolving.

WHO'S THE SHERIFF OF THE CLOUD? YOU.

We know what the IT security professional's job is. Let's talk a little about the hacker's job. Unless we know what they want, we won't be able to stop them. The answer is simple: Like any criminal, they want to take things and make money, things like information, data, access, and control. As Michael Corleone said in *The Godfather*, "it's business."

Cyberthieves don't care where the data is, or whose it is; if they can get at it and pluck it out without getting caught, they will. And they'll do it like any burglar. They will opportunistically get on your network, connect to a resource, and execute their end goal: steal data, commandeer compute resources to harvest bitcoin or run a malware campaign, or otherwise damage your environment.

And here's where a lot of organizations fail on their cloud journey. They don't realize one critical fact:

It's your responsibility to protect your data and applications from attack.

We want to be clear here. When you move up to the cloud through Microsoft Azure and other platforms, you'll get plenty of help and resources. They'll keep the infrastructure secure—Azure is one of the safest infrastructures there is.

But when it comes to applications and data you run or store on the Azure infrastructure, it's up to you. Your cloud environment will help you secure your resources, **but it is *your* responsibility to configure them properly.**

For example, in Azure, when you put together a Resource Group, by default all its ports are completely open to the internet. You have to configure the group to shut down and lock down access where you don't want it. All the breach examples we mention above can be attributed to someone on the victim's side not following best practices for security. Someone failed to install an update patch, or misconfigured the service or feature, leaving it exposed. Again, the list goes on.

Here's a quick overview of who's responsible for what in the Microsoft Cloud Shared Responsibility Model from on-premises to the cloud. The layered approach to security would look like this:

- **For on-premises solutions,** you are both accountable and responsible for all aspects of security and operations.
- **For infrastructure as a service (IaaS) solutions,** the elements such as buildings, servers, networking hardware, and the hypervisor should be managed by your platform vendor. You are responsible (or you have shared responsibility) for securing and managing the operating system, network configuration, applications, identity, clients, and data.
- **For platform as a service (PaaS) solutions,** which build on IaaS deployments, your provider is also responsible for managing and securing the network controls. You're still responsible (or you have shared responsibility) for securing and managing applications, identity, clients, and data.
- **For software as a service (SaaS) solutions,** a vendor provides you the application and abstracts your organization from the underlying components. Nonetheless, you continue to be accountable. You must ensure that data is classified correctly, and you share responsibility for managing your users and end-point devices.

If the public cloud is connected to your network, then whatever resources are there are fair game. Hackers will attempt to compromise your network through tactics like phishing attacks and drive-by downloads. They'll get on the network and navigate laterally to a resource on Azure, Office 365, or even the datacenter down the hall. Whether your resources are 100% on-premises, hybrid, or all up in the cloud, your security is only going to be as strong as your weakest link.

And the cost when cyberthreats are successful can be enormous. The Ponemon/IBM report, **2017 Cost of Data Breach Study**, found that the average price of a breach was $3.62 million. No organization among the 419 Ponemon surveyed had not experienced a data breach. And these hard costs don't include the damage a breach does to the marketplace's trust in an organization or its brand. There are countless examples of security incidents resulting in incalculable loss of public trust; and trying to appraise the cost of damage to the brand is impossible. Because of the newness of the cloud, security breaches there can cause even deeper rifts in trust. These events make it even harder to answer the question, "Why move to the cloud? Everyone knows it's not secure."

FROM PORT-BASED SECURITY TO TRUE CLOUD SECURITY

It's surprising how many organizations still rely on 20th-century security technologies, even after they have moved to cloud computing platforms that clearly need different approaches. If you're going to be involved in discussions about your cloud security options, be prepared to hear some of the following ideas, and be aware of their weaknesses and strengths.

PORT-WATCHING LEAVES YOU UNGUARDED

Port-based security is just classic stateful inspection. It truly is a 20th-century solution. It will look at ports and protocols—that's all. With it, opening up port 80 or port 443 for updates is the same way you'd manage a firewall in the 1990s. According to the **research firm Mitre**, ports 80 and 443 and many of the same ports used in a cloud deployment are the same ones used to evade security. Once the attacker has gained access to your coveted resources, many of the same ports used to evade detection are commonly used for data exfiltration: TCP/80, TCP/443, TCP/25, TCP/53, and TCP/22.

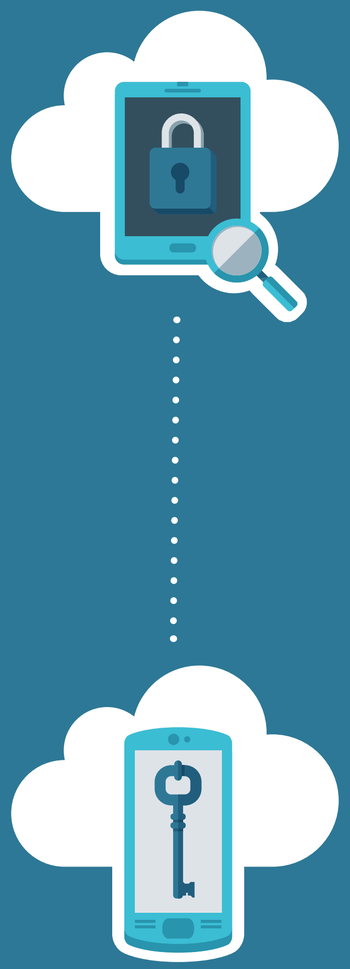
Often, an application will use more ports, operating dynamically so they need to be left open. Microsoft Lync, for example, uses about 80 ports; so an attacker has all those ways to access the network and hide in plain sight.

Even if you use Azure Network Security Groups and lock down ports 80 and 443, you're still allowing in almost 500 applications. Of those, the ones carrying the highest risk are proxies, remote access, and encrypted tunnel applications. And if you're running a web app, it may require other services, such as SSH, RDB, DNS, NetBIOS, or SMB. Shutting down everything but 80 and 443 is inadequate.

NEXT GENERATION OPTIONS—A NEW APPROACH

There are two ways to go forward. Customers create applications in the public cloud that use resources residing in the public cloud. These applications might reside in a Resource Group on Azure. We also see them use services that might reside outside of those environments, like Azure Storage. These might be thought of as a combination of infrastructure as a service (IaaS) and platform as a service (PaaS). Given that, there are two equally good ways to go: (1) Install a next generation virtual firewall, such as Palo Alto Networks VM-Series. The VM-Series sits within those environments as an inline device or virtualized firewall and, without friction, monitors all traffic going in and out of the public cloud. Or, (2) deploy a cloud access security broker (CASB), such as Palo Alto Networks Aperture, which supports a wide range of SaaS applications and PaaS services.

THE FOUR KEY ELEMENTS OF NEXT GENERATION SECURITY



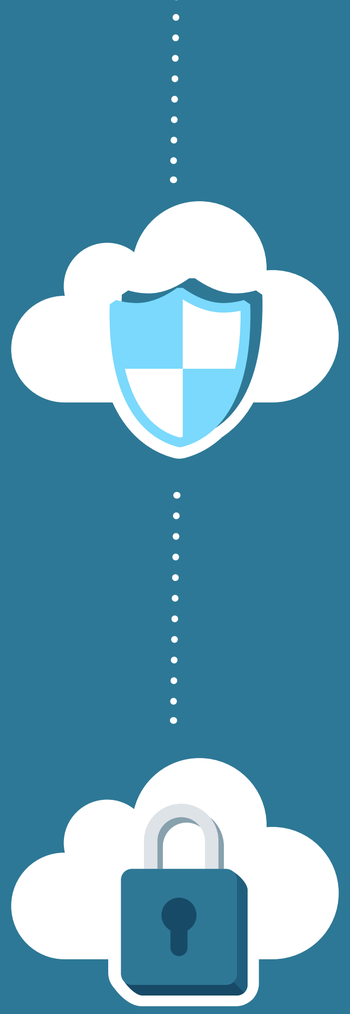
1. COMPLETE APPLICATION VISIBILITY

Traffic classification should be based on applications, not ports. That is, when you do look at port 80, you're really seeing and evaluating hundreds of applications. You should be identifying and examining them, and you should set firewall policies that allow authorized applications through, but deny all others.

One of the things you miss when you simply watch a port is clear context on each bit of traffic coming through. You need to see where files are coming from, what protocols they use, who the users are, the types of file, country of origin, and more. IT needs all this context to make good security decisions. If it's suspicious, you can block it. With a product like VM-Series, you have visibility to all traffic quickly and easily, so you can translate the context you see into policies. Geoblocking is a good example of this. If you know you shouldn't be getting any traffic from certain countries, you can block all traffic to and from that region.

2. GREATER CONTROL AND SEGMENTATION TO REDUCE THREAT FOOTPRINT

A firewall is a positive control model. Its job is simple: allow what you want to allow, and deny all else. But now, with application-based security, you use policies to segment—or whitelist—and separate database traffic from web front-end traffic. This does two important things: it improves security posture and achieves compliance.



3. PREVENTING THREATS AND DATA THEFT

Once the threat footprint has been reduced, you can then apply threat prevention policies to allowed traffic and protect your applications and data—a kind of one-two punch that blocks both known and unknown threats. Known threats such as exploits, malware, and viruses are blocked within the application flows in real time. Unknown threats (commonly referred to as zero-day) are prevented by sending suspicious files to Palo Alto Networks WildFire service, which analyzes potentially malicious files based on 200 known behaviors. That will indicate whether the file in question represents a threat. The admin is immediately given a confirmation of malware and protection is delivered on the fly to that user as well as others. All in a matter of minutes.

The behaviors observed are used for more than generating protection measures. The information collected during malware analysis is used to improve other threat prevention components. If the malware reached out to a malicious website, we add that URL to our filtering component. We can also learn the malicious DNS activity it was executing and apply those to DNS signatures and protection mechanisms to the IPS. This feedback loop allows us to continually improve the prevention capabilities of all the Palo Alto Networks next-generation firewalls. This also ensures consistent security policies from the network to the cloud.

4. AUTOMATED DEPLOYMENT AND CENTRALIZED MANAGEMENT

For administrators to have the context and control they need, they must centrally manage configuration and policy across the enterprise and the cloud. When you can automatically generate and share security objects you might use in the cloud, you reduce admin effort and increase your policy consistency—a very powerful tactic. When you use things like bootstrapping to create a golden config of your virtualized firewall, you can then store that config in an Azure repository. Then, you can reference the golden config using Azure functions or third-party tools like Terraform and Ansible to fully automate the deployment. For example, many organizations are moving all their applications, development, and testing into the cloud, and need protection. With automated deployment, they can create a completely touchless development environment secured by VM-Series. When a developer starts a project, they just hit “go” and an ARM template creates the development resource group. Other scripts reach out and connect with the tools the dev needs. The VM-Series is deployed from a bootstrapped image, completely configured with routing, content, licensing, and policies. This strategy allows your security teams to be confident that they’re consistently protecting applications and data in the public cloud. Meanwhile, DevOps can iterate and innovate at the speed of the cloud and deliver the faster iterations that business demands. That’s how security should work with automation and the power of the cloud.

CLOUD SECURITY MUST-HAVES

1 COMPLETE APPLICATION VISIBILITY

- Identify all applications regardless of port
- Application control to reduce exposure
- Apply whitelisting/segmentation policies

2 PROTECTION OF APPLICATIONS AND DATA

- Block known and unknown threats within app flows
- Prevent lateral threat movement
- Stop data exfiltration

3 AGILITY TO KEEP PACE WITH THE CLOUD

- Fully automate deployment and policy updates with native features and third-party tools
- Ensure policy consistency with central management

Microsoft Azure + paloalto NETWORKS

BE SECURE IN THE CLOUD

More IT organizations are moving up to modern cloud computing, yet many still rely on decades-old security paradigms. Working with Microsoft Azure, Palo Alto Networks is making cloud environments more than the next generation in computing.
We're working to make the cloud the safest environment for all kinds of computing, data, applications, and storage.

Take advantage of an array of **cloud computing resources** and find out how moving up to the Azure cloud puts your organization on the road to improved business performance.

MOVE UP TO THE CLOUD.

CONNECT WITH PALO ALTO NETWORKS ▶

Microsoft