TOP 10 PUBLIC CLOUD SECURITY RECOMMENDATIONS

The move to the public cloud is the biggest computing paradigm to unfold since the early 2000s, when the internet boom first exploded. According to the 451 Group®, enterprise IT executives expect 60 percent of workloads will run in the cloud by 2018.[1] Driving this growth are greater agility and scalability, higher performance, and faster access to innovative technologies, all of which enable organizations to gain a competitive edge.

Just as the nascent adoption of the public cloud introduces new business, productivity and agility opportunities, so too does it expose potential security risks. There are two well-understood facts about the public cloud. First, it is essentially someone else's computer – a set of virtualized resources (compute, networking and application) that you control yet are operating on a system owned by a third party. Second, the public cloud is an extension of your network. Less understood is just how secure your applications and data are in the public cloud. While the cloud service provider infrastructure is likely highly secure, your applications and data in the public cloud are only secure with your help.

Attackers are location-agnostic. Their intent is to compromise your network to steal user data, intellectual property or computing resources, whether in the public cloud, private cloud or physical data center. It is your responsibility to take the necessary steps to protect your applications and data in the public cloud – a fact not always clear to the business groups and DevOps teams driving public cloud adoption. This paper is intended to arm security teams with the information they need to engage early, ask appropriate questions and work toward protecting the public cloud as vigilantly as the data center.

1. https://451research.com/blog/764-enterprise-it-executives-expect-60-of-workloads-will-run-in-the-cloud-by-2018

Contents

Top 10 Considerations for Securing Your Public Cloud Workloads

Outlined below are 10 key considerations to effectively protect data and applications in the public cloud from a multitude of ever-evolving security threats that often mirror those faced in a traditional, on-premise data center.

Embrace the Shared Security Model

Public cloud providers, such as Amazon® Web Services (AWS®) and Microsoft® Azure®, make it clear security is a shared responsibility. In this model, the provider is responsible for ensuring the platform is always on, available, up to date and so on.

In fact, most believe the cloud provider's global data center infrastructure is more secure than their own. What gets lost is the fact that you, the customer, are responsible for protecting your own applications and data running within the public cloud.

Figure 1 highlights the responsibility breakdown. Securing your workloads in the public cloud (shown in red for clarity) is no different from securing them on-premise. You are in complete control of what security to implement and must take steps to safeguard your content, be that customer data or intellectual property.

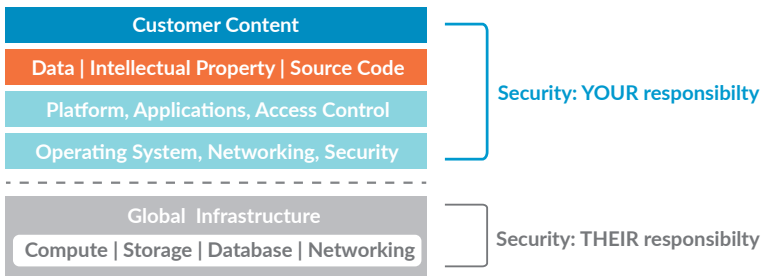


Figure 1: Public cloud shared responsibility model

Engage With Business Groups and DevOps Early

Many public cloud projects are driven by business groups, such as DevOps, that quickly spin up new products or functional prototypes. Challenges arise based on two things: general availability of new application approaches, and the security team, which is often brought in to assist with deployment. Both identify possible architecture-based security holes.

Ideally, security and DevOps should work in tandem to understand the scope of public cloud projects and ensure the architecture of the application deployments meets business development needs while mitigating security risks.

Know Your Potential Exposure

Public cloud usage is often referred to as "shadow IT," given how easily an account can be established. Employees doing what is "right for the business" may create security holes if the environment is not configured properly. It is imperative to know who in your organization is using the public cloud and to ensure the environment is configured correctly.

- **Monitor Public Cloud Usage:** Perhaps the quickest and most accurate way to determine usage is to call the local public cloud provider sales representative and ask how much your organization is using AWS or Azure. Alternatively, you can use network visibility tools that provide insight into the usage based on network application traffic.

- **Ensure Proper Configuration:** Configure the environment with security best practices in mind. For example, each AWS service has a public-facing set of application programming interfaces (APIs) that should be disabled if not in use. Many new AWS users may not be aware that Amazon Simple Storage Service is a public-facing service, exposing anything stored within to the internet unless locked down by policy. On Azure, when establishing an initial VNet within a resource group, users should understand that all outbound ports are open by default, introducing potentially unwanted exposure.
- **Enforce Two-Factor Authentication:** According to the latest Data Breach Investigations Report from Verizon, 81 percent of hacking-related breaches leveraged either stolen credentials or weak passwords. To minimize the risk of an attacker gaining access using stolen credentials, two-factor authentication should be applied.
- **Lock Down SSH:** Secure Shell® is a preferred method to securely control cloud services, yet this is often left exposed in AWS and Azure environments. Often, organizations do not have a clear understanding of encryption key and certificate inventories, exposing vulnerabilities cybercriminals are well-versed in utilizing. A cybercriminal with SSH access can easily use an organization's cloud infrastructure to launch his or her own botnet-based attacks.

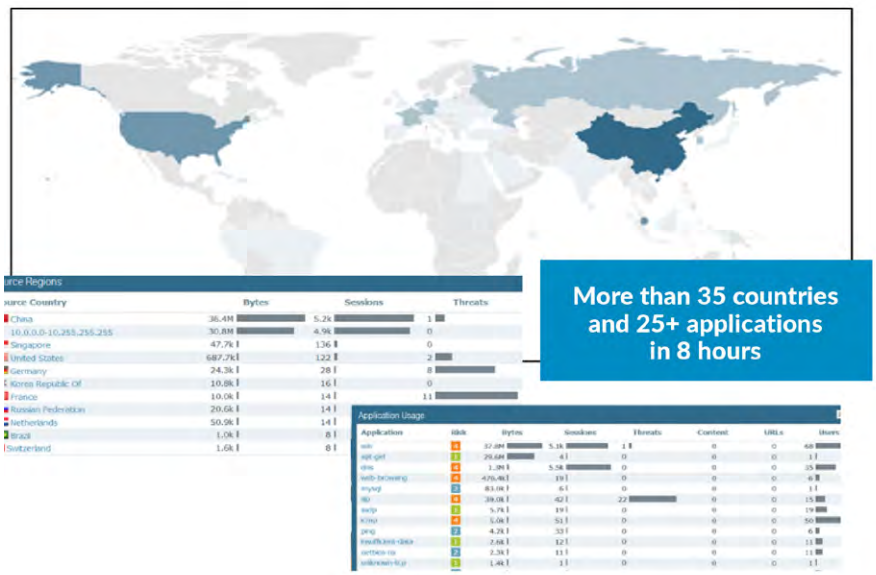


Figure 2: Public cloud automation test environment

Understand the Attacker

Attackers leverage automation to find potential targets within minutes. Once identified, they look for weaknesses, checking default passwords, probing for SSH misconfigurations and so on.

To highlight the effects of attackers' automation capabilities, a test environment with instances of an SQL database and a WordPress® server was spun up in the public cloud. As shown in Figure 2, the environment was probed from more than 35 countries with more than 25 different applications – all within eight hours. Unlike in a private data center, where there is less concern about public exposure, resources in the public cloud are widely exposed. This example serves as a reminder of the importance of security in the public cloud.

Evaluate Your Security Options

There are several security options to choose from when moving to the public cloud, most of which are similar to the options for physical networks.

- **Native Public Cloud Security:** Cloud service providers offer native security services including security groups and web application firewalls (WAFs). While these tools help reduce the attack surface, there are security gaps.
  - Security groups are essentially port-based access control lists, providing filtering capabilities. However, you will not be able to identify or effectively control the specific applications being allowed, nor will you be able to prevent threats or control file movement.
  - WAFs only protect HTTP and HTTPS applications, and ignore all other traffic. They are also not always required, whereas a firewall is always critical. WAFs cannot protect applications, such as Microsoft Lync®, SharePoint® or Active Directory®, that use a wide range of contiguous ports to function properly. Further, they are not an effective means of identifying and controlling remote management or access tools, such as SSH or Microsoft RDP.
- **Point Products:** One of the more common approaches to securing the public cloud uses a host-based point product to detect and prevent threats. The popularity of this approach is driven by the notion that native security, combined with an IDS or an IPS, is sufficient to protect your deployment. In reality, an IDS is counterintuitive to the speed and agility of the cloud as it requires manual intervention and remediation. An IPS only looks at known threats, and may miss zero-day or unknown threats. Neither provides a holistic view of your public cloud environment.
- **Do-It-Yourself Security:** Some organizations choose a DIY approach to securing public cloud workloads, using scripting and visibility tools to protect deployments. Potential disadvantages to this strategy include inadequate resources, lack of expertise to manage the security implementation and operations, and nonexistent support in the event of a security breach.

Organizations that rely on internal personnel to manage public cloud and security deployments must be prepared for attrition. Typically, only a few engineers know the environment well, but they don't necessarily have time to keep proper documentation or manage knowledge-sharing requirements. If even one of those engineers leaves the company, the organization may not be well-positioned to effectively manage security needs moving forward.

- **In-Line Virtualized Appliances:** An in-line virtualized appliance, such as a virtualized next-generation firewall, provides a foundation to gain visibility into all traffic in your cloud deployment. By employing integrated next-generation security, organizations can elevate protection for applications and data in the public cloud, using application-, user- and content-based identification technologies to understand exactly what is being accessed, by whom and for what purposes. With this understanding, dynamic security policy can be enforced to safely enable applications, content and users regardless of location, as well as protect data and applications in public cloud deployments from targeted and inadvertent threats.

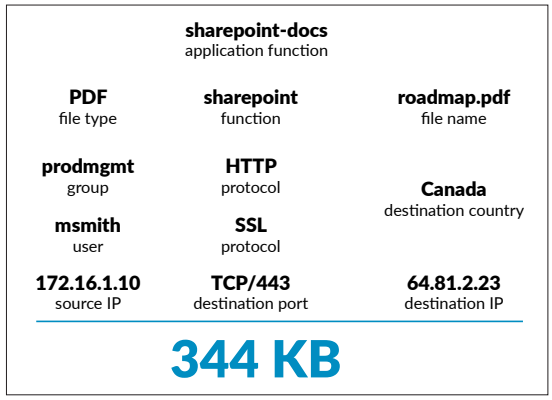


Figure 3: Complete traffic flow context

Knowledge Is Power

Personal branding consultant John Antonios once said, "knowledge plus action is power." In public cloud security, knowledge begins with safely enabling all traffic traversing your environment, spanning mobile, network and cloud.

The magnitude of digital data traversing these environments is immense. By utilizing a virtualized next-generation firewall as part of a natively integrated, comprehensive security platform, organizations gain necessary insight into traffic identity and characteristics so they can make more informed policy decisions to protect applications and data from threats.

Native public cloud tools provide little visibility at the application layer. Further, in some cases, in-depth networking knowledge is required to interpret the data accurately. Even with accurate interpretation, knowing that 344KB of data is flowing from a source IP address and port to a destination address and TCP 443 is of limited value when it is well-known that hundreds of applications can utilize TCP 443.

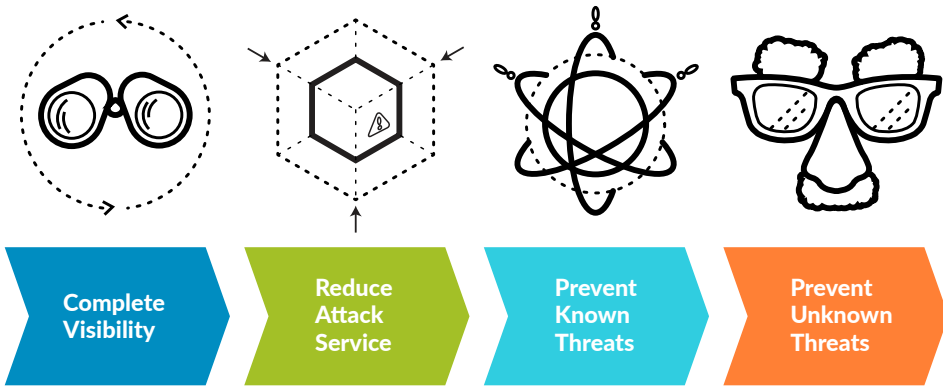
In some hybrid deployments where the public cloud is connected to corporate via an IPsec VPN, the use of port-based controls to limit access to only TCP 80 and TCP 443 is viewed as sufficient, the argument being that exposure is limited only to that which is coming from corporate. This is a fundamentally flawed position.

- At least 500 applications, many of which are remote access tools, circumventors and proxies, can use TCP 80 and TCP 443.
- In many cases, the applications in use need added protocols and services, such as DNS, NetBIOS and possibly SSH, all of which require their respective ports to be open.
- The most common development tools, Chef and Puppet, require a wide range of open ports:
  - Chef external-facing ports: 80, 112, 443, 4321, 5432, 5672, 8000, 8983, 9683, 9090, 15672, 16379, 7788–7799
  - Puppet external-facing ports: 25, 443, 8081, 8140, 61613

The reality is that port controls provide an initial level of control but no contextual awareness of the application traffic, the content within or the user. As displayed in Figure 3, understanding the complete context of traffic flow, including the source/destination IP and country; protocol(s); user or user group facilitating the activity; URL category; application identity and specific application functions in use; and specific filename and type can help you make more informed security policy decisions.

Believe in Prevention

There are those who believe the attackers have already "won," and thus choose to implement a detection and remediation approach. However, with complete awareness of your environment, a prevention philosophy is indeed possible. Enabling the prevention of successful cyberattacks in the public cloud requires four key capabilities:



Complete Visibility

The combination of knowledge and enforcement is a powerful security tool. It's critical to identify applications on the network and in the public cloud – irrespective of port, protocol, evasive tactic or encryption – as well as identify application characteristics, specific application functions in use and relative risk. With this knowledge, a more consistent security policy can be deployed globally to protect your network from known and unknown attacks.

Reduce the Attack Surface

Using application identity as a means of enforcing a positive security model reduces the attack surface by enabling only allowed applications and denying all else. You can align application usage to business needs, control application functions (e.g., allow SharePoint documents for all but limit SharePoint administration access to the IT group), and stop threats from gaining access and moving laterally within your network.

Prevent Known Threats

Applying application-specific threat prevention policies to allowed application flows is a key step in adhering to a prevention philosophy. Application-specific threat prevention policies can block known threats, including vulnerability exploits, malware, and malware-generated command-and-control traffic.

Prevent Unknown Threats

Unknown and potentially malicious files are analyzed based on hundreds of behaviors. If a file is deemed malicious, a prevention mechanism is delivered in as few as five minutes. Once the prevention technique has been delivered, the information gained from file analysis is used to continually improve all other prevention capabilities.

Take a Cloud-Centric Approach

The public cloud enables your organization to address business challenges with an agile, more scalable approach. To take full advantage of the cloud, recommended best practices include "applying the concepts of the data center to your deployment, while leaving the traditional constructs behind." This way, organizations can achieve high availability and scalability.

Using traditional two-device high availability as an example, we can assume that the premise behind HA should be applied to your public cloud deployment. However, the advantage of hardware-based acceleration for sub-second failover is lost when operating in the public cloud because you are operating on someone else's computer. To execute failover from one device instance to another, the process is accomplished in software. This may take up to 60 seconds depending on the environment, and might not span different regions. The cloud-centric approach utilizes the cloud provider fabric and its inherent resiliency features, such as load balancing, to quickly and seamlessly accomplish the end goal of HA.

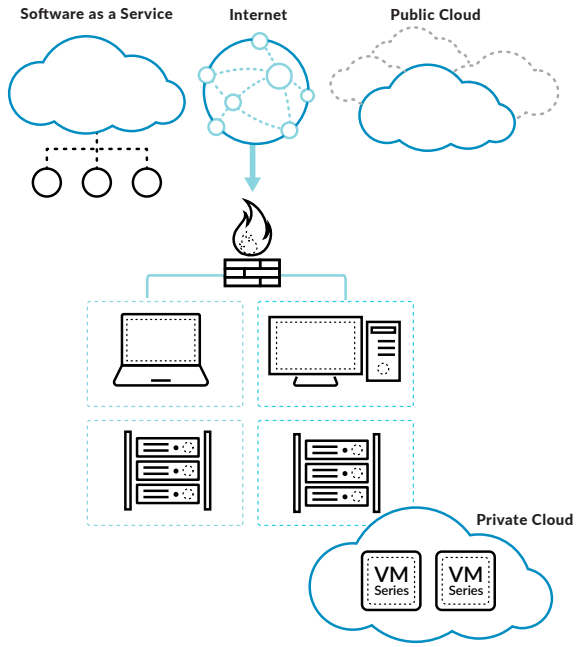


Figure 4: A Cloud-centric approach

Use Automation to Eliminate Bottlenecks

Automation is a central tenet of the public cloud, where rapid change is common. When security best practice change control is followed, the delay may induce friction, slowing deployments or, worse, weakening security if the deployment does not "wait" for change control to work. By automating security in the public cloud, organizations can eliminate security-induced "friction" and take advantage of the flexibility and agility benefits offered in the public cloud. Automation tools that organizations should look for in their public cloud security include:

- **Touchless Deployments:** Features such as bootstrapping enable a fully configured firewall to be deployed in minutes so you can secure isolated virtual networking environments in the public cloud (e.g., Azure resource groups and AWS virtual private clouds).
- **Bidirectional Integration With Third-Party Resources:** API-driven integration with third-party tools and data helps streamline security operations. For example, you can integrate with ServiceNow® to efficiently generate service tickets and workflows.
- **"Commitless" Policy Updates:** Automation features like XML API and Dynamic Address Groups allow you to drive dynamic security policy updates as workloads change. Organizations can operate at the speed of the cloud with faster, more accurate security policy updates based on changes in the environment.

Enforce Policy Consistency Through Centralized Management

To maintain effective security for data and applications in the public cloud, policy consistency is essential. Controlling your distributed network of firewalls, physical and virtualized, from one central location and applying a single, consistent security rule base from the network to the public cloud is critical to maintaining security functionality and efficiency. Centralized management provides insight into traffic and threats network-wide, simplifying management and helping you minimize security policy lag as workloads in the public cloud change.

Summary

Organizations are boarding the public cloud train to achieve more efficient time to market, improve overall business and continue carving a competitive edge. However, as business-centric groups continue to drive adoption, security teams are not always involved in the process. Based on common experiences, these security considerations are designed to be educational and informative. Ideally, the goal is to encourage dialogue between the security and business groups to achieve a public cloud architecture and deployment that accounts for both groups' demands.

To learn more, check out the following resources:

- **Webpage:** Securing Your Public Cloud
- **White Paper:** Securely Enabling a Hybrid Cloud in Microsoft Azure
- **White Paper:** VM-Series for AWS Hybrid Cloud Deployment Guidelines

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

top-10-public-cloud-security-recommentation-eg-072017