SOPHOS

Securing the Public Cloud: Seven Best Practices

Sophos Whitepaper June 2019

Contents

Securing the Public Cloud: Seven Best Practices

What does success look like to you when it comes to securing applications in the public cloud?

Perhaps it's surviving the year without hitting the headlines for a data breach. Or being able to understand your organization's cloud infrastructure footprint so you can accurately secure it? Maybe you want to ensure compliance audits go off without a hitch? Or improve collaboration on security and compliance fixes with siloed compliance and development teams?

Whatever you want to do, this guide can help. It explores the seven most important steps in securing the public cloud, providing practical guidance that every organization can follow. It includes the results of threat research from SophosLabs into the frequency with which cybercriminals target cloud-based instances. This guide also explores how Sophos Cloud Optix enables organizations to address their security and visibility challenges.

Spinning up new instances in Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) is simple. The hard part for operations, security, development, and compliance teams is keeping track of the data, workloads, and architecture changes in those environments to keep everything secure.

While public cloud providers are responsible for the security of the cloud (the physical datacenters, and the separation of customer environments and data), responsibility for securing the workloads and data you place in the cloud lies firmly with you. Just as you need to secure the data stored in your on-premises networks, so you need to secure your cloud environment. Misunderstandings around this distribution of ownership is widespread and the resulting security gaps have made cloud-based workloads the new pot of gold for today's savvy hackers.

The Toughest Challenges in Cloud Security

Given the simplicity and cost-effectiveness of the public cloud, it's no surprise that more and more organizations are turning to Amazon Web Services, Microsoft Azure, and Google Cloud Platform. You can spin up a new instance in minutes, scale resources up and down whenever you need while only paying for what you use, and avoid high upfront hardware costs.

While the public cloud solves many traditional IT resourcing challenges, it does introduce new headaches. The secret to effective cybersecurity in the cloud is improving your overall security posture: ensuring your architecture is secure and configured correctly, that you have the necessary visibility into your architecture, and importantly, into who is accessing it.

While this sounds simple, the reality is anything but.

The rapid growth of cloud usage has resulted in a fractured distribution of data, with workloads spread across disparate instances and, for some organizations, platforms. The average organization already runs applications in two public clouds, while experimenting with another 1.8 public clouds [1]. This multi-cloud approach compounds the visibility challenge for IT teams who need to jump from platform to platform to get a complete picture of their cloud-based estates.

Lack of visibility into cloud-based workloads leads to both security and compliance risks:

Increased exposure

Greater agility and improved time-to-market for products and services are huge motivators for an organization to move to the public cloud. Doing this usually requires the agility and responsiveness of a DevOps approach. For many, this new approach to development and product releases entails multiple developers working across multiple platforms, and often in different time zones.

Keeping track of the workloads wasn't such an issue when development cycles lasted months or even years, but those days are over. You now need to keep up with multiple releases – sometimes on the same day. Tracking fast-paced architecture changes, configuration updates, and security group settings around the clock is near impossible. It all adds up to a recipe for increased exposure to cyber threats where vulnerabilities can be quickly exploited.

Threats to data, intellectual property, and services

Just as organizations enjoy the automation benefits that the public cloud offers, so too do cyber criminals. Today's attackers increasingly canvass cloud environments and take advantage of native cloud provider APIs to automate deployments on new instances, breach open databases, change security settings, and lock out legitimate users.

To quantify the issue, SophosLabs recently set up environments in 10 of the most popular AWS data centers in the world. The research revealed that:

- Within two hours, all 10 suffered login attempts [2]
- Each device saw an average of 13 login attempts per minute, or about 757 per hour

These startling results highlight the frequency with which cybercriminals are targeting cloud-based instances, using sophisticated, automated techniques. The challenge for security teams lies in identifying and securing potential vulnerabilities before the attackers, and identifying unusual (attacker) behavior in real time to stop an attack in its tracks.

Maintaining compliance standards

No matter where your infrastructure and data is held, you need to demonstrate compliance with relevant regulations, including CIS, HIPPA, GDPR, and PCI or risk regulatory non-compliance.

The challenge in the cloud is that environments change by the day, the hour, even by the minute. Whereas compliance checks every week or month may have worked for on-premises networks, they won't cut it for the public cloud. The need for continuous compliance analysis can be a huge resource drain for teams that are managing cloud environments manually or with native tools. What's more, once a compliance issue is identified, the fractured nature of security, development, operations and compliance teams within most organizations means it is often challenging to address the situation in a timely manner.

Seven Steps to Securing the Public Cloud

Step 1: Learn your responsibilities

This may sound obvious, but security is handled a little differently in the cloud. Public cloud providers such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform run a shared responsibility model – meaning they ensure the security of the cloud, while you are responsible for anything you place in the cloud.

Aspects such as physical protection at the datacenter, virtual separation of customer data and environments – that's all taken care of by the public cloud providers.

You might get some basic firewall type rules to govern access to your environment. But if you don't properly configure them – for instance, if you leave ports open to the entire world – then that's on you. So you've got to learn your security responsibilities.

Fig 1 provides an overview of these shared responsibilities – or if you prefer, watch the video here.

Shared Responsibility Security Model	On-Premises	Public Cloud	Why?
Users	■	■	Enforce authentication, define access restrictions, and track credential use.
Data	■	■	Stop data loss, define and enforce who can access what data, while ensuring compliance standards are met.
Applications	■	■	Prevent application compromise through policy, patching, and security.
Network Controls	■	◢	Track and enforce network access permissions.
Host Infrastructure	■	◢	Manage and secure operating systems, storage solutions and related systems to prevent unpatched bugs and privilege escalations.
Physical Security	■	■	Restrict physical access to systems and design redundancy to prevent single point of failure.

■ Customer ■ Platform Provider

Fig 1. Sophos summarized view of the shared responsibility model. For each cloud provider's specific version visit sophos.com/public-cloud.

Step 2: Plan for multi-cloud

Multi-cloud is no longer a nice-to-have strategy. Rather, it's become a must-have strategy. There are many reasons why you may want to use multiple clouds, such as availability, improved agility, or functionality. When planning your security strategy start with the assumption that you'll run multi-cloud – if not now, at some point in the future. In this way you can future-proof your approach.

Think about how you will manage security, monitoring, and compliance across multiple cloud providers, in separate systems and consoles. The easier the management experience the easier it is to cut incident response times, increase threat detection, and reduce compliance audit headaches. Not to mention aiding retention of valuable team members.

Look for agentless solutions that allow you to monitor multiple cloud provider environments within a single SaaS console, reducing the number of tools, time, and people needed to manage security across multiple cloud accounts and regions.

Step 3: See everything

If you can't see it, you can't secure it. That's why one of the biggest barriers to getting your security posture right is getting accurate visibility of your infrastructure.

Take advantage of tools that provide a real-time visualization of network topology and traffic flow, with a full inventory breakdown including hosts, networks, user accounts, storage services, containers, and serverless functions.

For enhanced visibility, look for tools able to identify potential vulnerabilities within your architecture so you can prevent a potential breach point. Potential risk areas include:

- Databases with ports open to the public internet that could allow attackers to access them
- Public Amazon S3 Simple Storage Services
- Suspicious user login behaviors and API calls – such as multiple logins to the same account at the same time, or a user logging in from different parts of the world on the same day

Step 4: Integrate compliance into daily processes

Moving workloads to the cloud introduces the challenge of meeting compliance regulations across a more distributed network, often involving regular development releases. To ensure compliance, you need to create accurate inventory reports and network diagrams of your cloud footprint, and ensure your compliance checklist is met in a dynamic environment.

When it comes to meeting audit deadlines, often organizations fall back on the short-term fix of diverting resources from profitable business projects. Yet this is not sustainable longer term and, as daily snapshots quickly become obsolete, this doesn't provide the continuous compliance monitoring needed for standards such as ISO 27001, HIPAA, and GDPR.

Look for solutions that allow you to raise compliance standards without added headcount by providing real-time snapshots of your network topology, and automatically detecting changes to your cloud environments in real time. You'll also want the option to customize policy to meet the specific needs of your sector or vertical.

Of course, reporting is only one aspect of compliance. You also need to be able to address compliance failures. The challenge is that it is often

hard to get the right people in operations, development, and compliance to work together due to lack of effective collaboration channels.

To make the process of addressing compliance failures run smoothly, find solutions that integrate with your existing ticketing solutions, including alert information that can be used to create, assign, and track issues to completion, ensuring important tasks are never lost, even during a release.

Step 5: Automate your security controls

The ability to automate processes is one of the joys of DevOps. But, just as your teams enjoy automating deployment of infrastructure templates and scripts, saving hours of development time, so you should also consider what security controls you can automate.

In the collaborative framework of DevOps, security is a shared responsibility, integrated from end-to-end. This mindset led to the coining of the term "DevSecOps," emphasizing the need to build strong security foundations into DevOps initiatives.

The need for automated security is clear as cybercriminals increasingly take advantage of automation themselves in their attacks – for example, using stolen user credentials to automate provisioning of instances for activities such as cryptojacking, changing account settings, or revoking legitimate users to avoid detection. Indeed, the canvassing of cloud environments for vulnerabilities in passwords, security group settings, and code are now commonplace.

The two main reasons why attacks on public cloud environments succeed are that the architecture configuration is not secure, and that threat response hasn't kept pace with attackers. Automation of security controls is key to addressing these issues.

To ensure the security of your public cloud environments, look for a solution that can:

- **Auto-remediate user access vulnerabilities and resources**, with ingress from any source on any port
- **Identify suspicious console login events and API calls** that suggest shared or stolen user credentials are being used by an attacker
- **Report anomalies in outbound traffic** to alert your organization to activities such as cryptojacking or the exfiltration of data
- **Reveal hidden application workloads** from the behavior of the host computer instance to highlight hidden exposure points (e.g. databases)

Step 6: Secure ALL your environments (including dev and QA)

While the public cloud data breaches that made headlines tend to be those that hit an organization's production cloud environment (the one your customers use), attackers are just as likely to come after your computing power – on your development and QA environments – for activities like cryptojacking.

You need a solution that can secure your all environments (production, development, and QA) both reactively and proactively. The solution should be able to ingest your activity logs (for example, VPC Flow logs and CloudTrail logs) to identify issues that have already occurred, such as when an undesired port is open in the firewall. At the same time, the solution should be able to proactively scan Infrastructure-as-Code (IaC) templates from your repositories like GitHub and integrate with your CI/CD pipeline tools such as Jenkins. This ensures that vulnerabilities introduced into code are detected long before it's rolled out to your servers – preventing a nasty news headline.

Step 7: Apply your on-premises security learnings

This may sound odd in a public cloud guide, but on-premises security is the result of decades of experience and research. When it comes to securing your cloud-based servers against infection and data loss, start by thinking about what you already do for your traditional infrastructure, and adapt it for the cloud:

- Next-gen firewall: Stop threats from getting onto your cloud-based servers in the first place by putting a web application firewall (WAF) at your cloud gateway. Also look to include IPS (to help with compliance) and outbound content control to protect your servers/VDI.
- Server protection: Run effective cybersecurity protection on your cloud-based servers, just as you would your physical servers.
- Endpoint protection: While your network may be in the cloud, your laptops and other devices are staying on the ground, and all it takes a phishing email or spyware to steal user credentials for you cloud accounts. Ensure you keep endpoint and email security up to date on your devices to prevent unauthorized access to cloud accounts.

Introducing Sophos Cloud Optix:

See everything, secure everything

Visibility is the foundation on which all public cloud security policies and activities are built. Sophos Cloud Optix makes it simple to monitor multiple cloud provider environments including Amazon Web Services (AWS) accounts, Microsoft Azure subscriptions, Google Cloud Platform (GCP) projects, Kubernetes clusters, and development code repositories. This superior visibility, layered with compliance and DevSecOps policies controls and alerts, enables teams to take control and build on their cloud security strategy with confidence.

An agentless, SaaS-based service integrating with native public cloud provider APIs, Cloud Optix automatically builds a complete picture of architecture, including a full inventory and real-time network topology visualization including hosts, networks, user accounts, storage services, containers, and serverless functions.

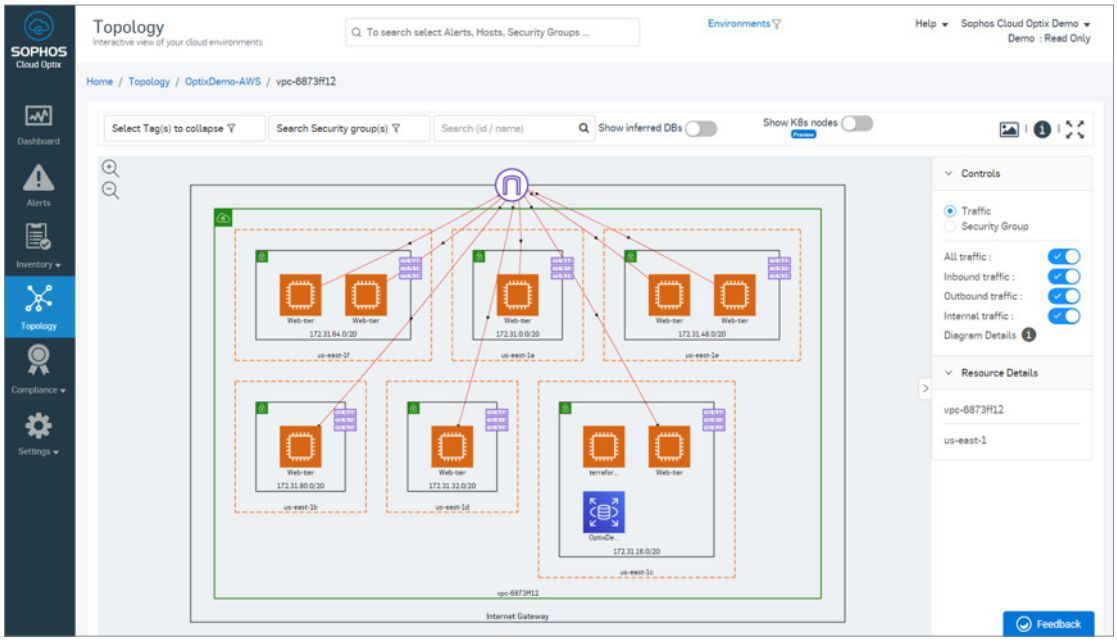

Fig 2. Sophos Cloud Optix network topology visualization showing ingress, egress, and internal traffic within an AWS environment.

More than simple configuration checks

Cloud Optix uses machine learning artificial intelligence to check for anomalies and security vulnerabilities across your platform – monitoring network traffic, resource configurations, user login events and API calls, compliance status, infrastructure-as-code (IaaC) repositories and more, with guardrails to automatically remediate accidental or malicious changes in network configuration.

While contextual alerts identify the root cause of security and compliance issues, allowing you to focus on the most critical areas that need security updates, with a description of the issue, remediation steps, and affected resources.

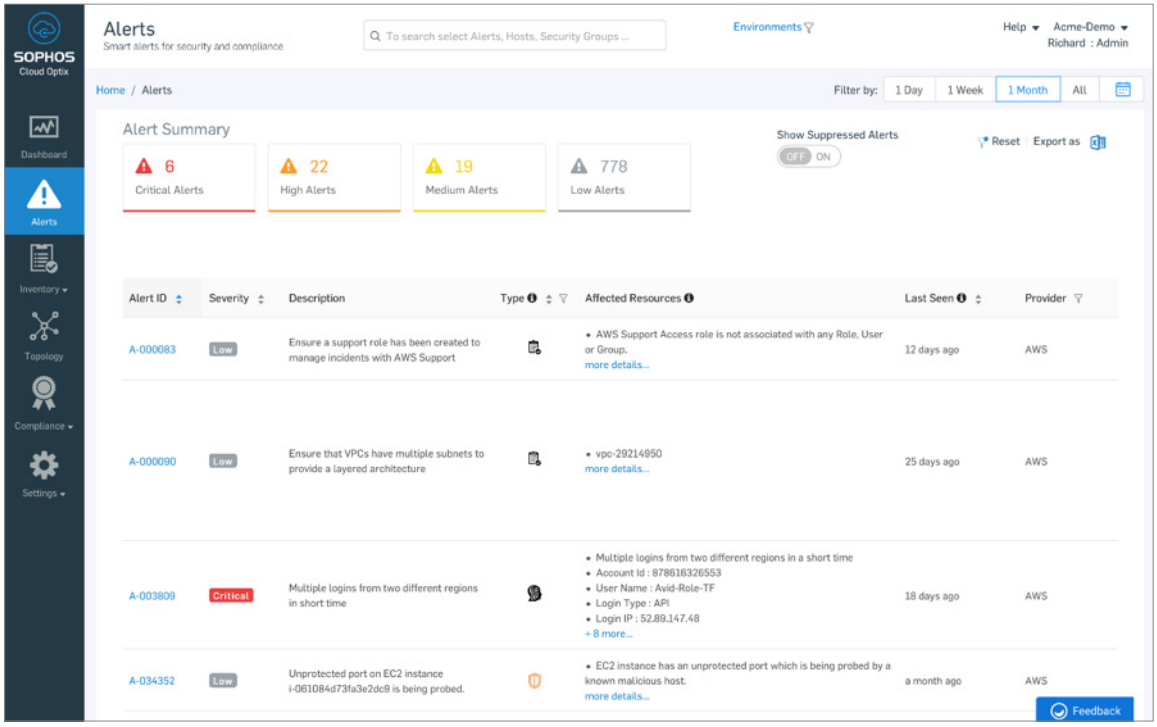

Fig 3. Sophos Cloud Optix alerts summary showing critical alert of multiple account logins from different regions at the same time.

Monitor and respond your way

Cloud Optix provides a Rest API, and integration with Splunk, PagerDuty, and Amazon GuardDuty to provide real-time alert information wherever you need it. While thanks to inbuilt integrations with Jira and ServiceNow, alert information can even be used to create tickets which can then be tracked to completion, ensuring important tasks are never lost, even during a release.

All-wrapped up with at-a-glance dashboards on on-demand reports, you'll save hours or even days of effort managing your cloud security posture – helping you achieve the seven most important steps in securing the public cloud.

Learn more

Sophos Cloud Optix is the ideal solution for organizations using or moving to the public cloud. By combining the power of AI and automation, it gives your organization the continuous visibility needed to detect, respond and prevent security and compliance vulnerabilities that could leave them exposed.

To learn more about Sophos Cloud Optix and to start a no-obligation 30-day trial on your own cloud environments, or an immediate online demo, visit www.sophos.com/cloud-optix.

Conclusion

Moving from traditional to cloud-based workloads offers huge opportunities for organizations of all sizes. Yet securing the public cloud is imperative if you are to protect your infrastructure and organization from cyberattacks. By following the seven steps in this guide you can maximize the security of your public clouds, while also simplifying management and compliance reporting.

Shared Responsibility Model: How Sophos Can Help

	On-Premises	Public Cloud	Why?	Sophos Assists
Users	■	■	Enforce authentication, define access restrictions, and track credential use.	XG Firewall and Sophos UTM enforce in/outbound authentication with SSO and 2FA and provide detailed access reporting. Sophos Cloud Optix tracks shared or unauthorized use of account credentials.
Data	■	■	Stop data loss; define and enforce who can access what data, while ensuring compliance standards are met.	Sophos Cloud Optix delivers compliance automation, governance, and security monitoring in the cloud, while Sophos Safeguard, DLP, and Sophos Mobile help secure data and determine access permissions.
Applications	■	■	Prevent application compromise through policy, patching, and security.	XG Firewall and Sophos UTM's IPS and Sophos Server Protection's HIPS and Lockdown protect against application attacks and unintended application exposure.
Network Controls	■	◪	Track and enforce network access permissions.	XG Firewall and Sophos UTM's easy to use interface, powerful packet inspection, and Synchronized Security (XG only) help secure and manage network access and enforce network privileges.
Host Infrastructure	■	◪	Manage and secure operating systems, storage solutions, and related systems to prevent unpatched bugs and privilege escalations.	Sophos Intercept X protects against zero-day threats by looking at exploit techniques. Sophos Server Protection Lockdown enforces runtime restrictions, and Sophos XG Sandstorm stops unknown code proliferation.
Physical Security	■	■	Restrict physical access to systems and design redundancy to prevent single point of failure.	Both XG Firewall and Sophos UTM have High Availability deployment options for both physical appliances and on cloud platforms.

■ Customer ■ Platform Provider

Fig 4. How Sophos helps with the public cloud shared responsibility model

'Sophos Cloud Optix gives our team the real-time, intelligent visibility into our AWS environments and configuration compliance status that we need at our fingertips. This enables a level of monitoring and alerting that was previously impossible in a single view. Having Sophos Cloud Optix gives us a holistic view of infrastructure activity, and lets us focus on comprehensive protections.'

Ryan Stinson
Manager of Security Engineering
HubSpot Inc.

1 RightScale 2019 State of the Cloud Report from Flexera

2 Automated attack data source: Exposed: Cyberattacks on Cloud Honeypots, Matt Boddy, Sophos, April 2019

Test drive Sophos Cloud Optix

www.sophos.com/cloud-optix

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

19-06-19 WP-NA (RP)

SOPHOS