aws | SOPHOS
Cybersecurity delivered.

Optimize Your Cloud Security Journey

How Sophos Helps You Every Step of the Way

Gartner predicts that by 2026, public cloud spending will exceed 45% of all enterprise IT spending, up from less than 17% in 2021.[1]

Organizations are moving to the cloud faster than ever, adopting new, agile technologies and processes that transform the business and enhance remote working experiences. As they move or expand into the cloud, security is crucial. Organizations need to build security into their migration plan to secure data, infrastructure, and employees—no matter where they are.

When preparing for a migration, organizations are looking to optimize security, increase control, and ensure efficient use of cloud resources for the best value. But they are often unsure which goals to prioritize first.

With this guide, you'll assess where your organization is in the process, and take actionable next steps to get you where you want to go.

[1] Gartner, Gartner Says Four Trends Are Shaping the Future of Public Cloud, 2 August 2021, Contact: Meghan Rimol, https://www.gartner.com/en/newsroompress-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud

The first step to ensuring your organization's security is to understand your current situation. Answer the following questions to determine which phase to start with.

01

Are you new to the cloud and need to build a secure foundation that gives you full visibility into your environment?

Start at Part 1

02

Do have the foundations of cloud security down but are unsure how to scale?

Jump to Part 2

03

Have you been leveraging cloud services for a while and need to improve your security posture and optimize costs?

Skip ahead to Part 3

Part 1
Beginning—Cloud Security Foundations

If you are new to the cloud, begin by creating your cloud security foundation. This process will provide a scalable approach from which everything else will grow. The following steps will help you design your environments to meet best practice standards, ensuring you have complete visibility and control.

Reduce risk and vulnerabilities by adopting Cloud Security Posture Management (CSPM) solutions that provide complete visibility to your environment.

CSPM solutions like Sophos Cloud Native Security (CNS) enable you to:

- Detect unsecure configurations and deployments across cloud environments.
- Stay compliant by automatically analyzing your cloud infrastructure against cloud security best practices and regulatory compliance standards.
- Visualize interwoven Identity and Access Management (IAM) relationships and simplify management of privileges.
- Reduce the cost and complexity of compliance with policies that automatically map to your environments.
- Prioritize alerts based on risk level and receive guidance on remediation.

Identify and respond to threats before they become breaches, through continuous monitoring and detection.

Amazon GuardDuty helps detect unusual behavior or threats across your environment and sends an alert. Sophos CNS seamlessly integrates with Amazon GuardDuty, helping you avoid alert fatigue by aggregating and prioritizing alerts in a single dashboard. The three primary threats include:

Attacker reconnaissance

Stop attackers before they enter by identifying failed login patterns, unusual API activity, and port scanning.

Compromised resources

Monitor for key changes in patterns or unusual traffic spikes that may indicate cryptojacking.

Compromised accounts

Isolate instances of compromised access such as API calls from an odd location or attempts to disable AWS CloudTrail governances.

Choose a security solution that leverages cutting-edge technology to stay ahead of the latest threats and easily apply updates.

- Deploy Cloud Workload Protection of cloud server instances to stop never-before-seen threats. Sophos Intercept X leverages deep learning AI that scrutinizes file attributes from hundreds of millions of samples.
- Activate patch status management services, such as AWS Systems Manager, to automate operational tasks, shorten the time to resolve issues, and improve visibility and control.

Part 2
Intermediate—Cloud Security Efficiency

Once you have a secure foundation, you can start looking for ways to improve your workflows and processes. Ensuring your team is focused on what matters most is critical. For many IT teams, regardless of size, it's difficult to maintain vigilant security 24/7, and those gaps leave you open to risk.

Adopt Managed Detection and Response (MDR) solutions with an expert team that supports your security 24/7.

- Dedicated teams of security experts leverage machine learning (ML) to continuously monitoring AWS environments to disrupt, contain, and neutralize advanced threats and alert you to suspicious behavior.
- AI-powered security automation and cross-product detection identify suspicious signals that take advantage of dispersed but interconnected systems.
- Aggregate cloud environment data sources including AWS CloudTrail and Amazon GuardDuty.

Still using multiple tools to monitor your environment? Learn how CSPM solutions can help.

Collaborate with a trained response team to prioritize alerts, decide what action to take, and when to escalate.

Stay in complete control of threat remediation, while freeing up internal teams to focus on identifying system shortcomings and IT projects that support company growth.

Integrate seamlessly with security products and AWS Cloud services to maximize visibility.

Streamline security operations and improve collaboration with Sophos integrations.

Recommended AWS Cloud services

- Amazon GuardDuty
- AWS Systems Manager
- AWS CloudTrail

64% of organizations surveyed stated that MDR will help them gain faster detection of intrusion.[2]

[2] Gartner, Gartner Says Four Trends Are Shaping the Future of Public Cloud, 2 August 2021, Contact: Meghan Rimol, https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud

Part 3

Advanced—Cloud Optimization

With a strong security foundation and your team set up for success, you can start to refine, modernize, and optimize your processes. Focus efforts on improvements that will increase efficiency, save costs, and help you dynamically scale your business.

Leverage more efficient application delivery strategies with containers and infrastructure-as-code templates.

- Shift left to prevent pre-production vulnerabilities created in software development pipelines which attackers are increasingly targeting.
- Seamlessly integrate security and compliance checks at every stage of the development pipeline to scan container images and infrastructure-as-code templates such as AWS CloudFormation.

Make more efficient use of resources.

- Track spend of multiple services side by side to improve visibility and optimize AWS resources for the best value.
- Deploy resources where they are needed most.
- Experience peace of mind knowing you are working with a team whose entire focus is cybersecurity. Reduce the risk of security breaches and compliance penalties while redirecting saved time and energy to strategic projects.
- Increase your level of security protection without increasing headcount.
- Utilize a cloud security management platform that will provide a comprehensive view into the security of your environment, which enables easy configuration and management.

Develop an IT team focused on business goals and bringing value to the company.

- Train your team to become experts who proactively deploy solutions for improved performance.
- Leverage solutions to maintain a strong defense and discover new ways to solve business challenges.

Customer Story: Celayix

About Celayix

Celayix, Inc., is headquartered in Vancouver, British Columbia. Since 2000, Celayix has been delivering tailored-to-fit employee scheduling software and time-and-attendance solutions to organizations with anywhere from 10 to over 10,000 employees, contractors, and volunteers.

Customer Story

The team at Celayix also believe in automating tasks and working smarter. And so it was reassuring when Sophos MDR signaled unusual activity when applying scripts or changing release processes. It's proof that the Sophos service is working as it should, while also enabling their team to go faster.

The Sophos Managed Detection and Response service team receive telemetry from all Sophos products deployed in AWS (i.e., CSPM, workload protection, firewalls), and it also receives intelligence from AWS Cloud services including Amazon GuardDuty, AWS CloudTrail, and AWS Security Hub—enabling 24/7 threat protection, monitoring, and response across the AWS environment.

Conclusion

Migrating to the cloud is a unique and challenging opportunity for each company. It's a process that takes time, the right solutions, and the support of experts who know your environment. Wherever you are in your cloud journey, Sophos is here to make it a success by helping you:

- Build a strong security foundation.
- Increase the efficiency of your IT team.
- Modernize and optimize your environment.

Learn more in our MSSP listing

Sophos Managed Detection and Response

Sophos Cloud Native Security

aws | SOPHOS Cybersecurity delivered.