

Sophos Cloud Native Security



Protect Cloud Environments, Workloads, and Identities

Sophos Cloud Native Security provides comprehensive multi-cloud security coverage across Amazon Web Services, Microsoft Azure, and Google Cloud Platform environments, workloads, and identities to detect and remediate security risks and maintain compliance.

Power-Up Security Teams

A single integrated cloud security platform to boost efficiency and incident response time. Sophos Cloud Native Security unifies security tools across workloads, cloud environments, and entitlements management to ensure the best visibility, security, and compliance outcomes. All integrated with SIEM, collaboration, workflow, and DevOps tools to increase agility across organizations.

Minimize Time to Detect and Respond

Identify and stop malware, exploits, misconfigurations, and anomalous behaviors with powerful extended detection and response (XDR) tools. Hunt for threats, receive prioritized detections, and benefit from automatically connected security events across AWS, Azure, and GCP environments to optimize investigation and response times.

Fast-Track Cyber Resilience

Cybercriminals are smart and creative. Your organization and cloud environments need to be tough, hard to compromise, and quick to recover. Our comprehensive and intuitive cloud security and remediation tools can be managed by your own security teams, through a Sophos Partner, or via the Sophos Managed Threat Response service to fast-track your cyber resilience to best meet the security incidents of today.

Partnership That Augments Your Team

The Sophos MTR service is the perfect complement to Sophos Cloud Native Security. This managed detection and response service can work with your teams, monitor your environment 24/7/365, respond to potential threats, search for indicators of compromise, and provide detailed analysis on events, including what happened, where, when, how, and why, to prevent sophisticated threats from targeting your data and systems.

Integrated Hybrid Cloud Security

Sophos goes beyond cloud native security with a unified management console for all of your Sophos hybrid cloud cybersecurity technologies, including endpoint, mobile, server, firewalls, switches, secure wireless, email security, and secure access. With real-time information-sharing between your products, central XDR datalake, and consolidated dashboards and alerts, Sophos Central makes cybersecurity easier and more effective.

Highlights

- ▶ Secure environments and workloads in AWS, Azure, and GCP
- ▶ Linux and Windows cloud workload protection
- ▶ Cloud security posture management
- ▶ Kubernetes security posture management
- ▶ Infrastructure as Code security
- ▶ Cloud infrastructure entitlements management
- ▶ Cloud spend monitoring

Complete Multi-Cloud Security

Visibility, Governance, and Compliance

Reduce your attack surface with visibility of multi-cloud environments to detect and remediate security risks and maintain compliance.

- Increase efficiency with cloud security posture management tools across AWS, Azure, GCP, Kubernetes, Infrastructure as Code, and Docker Hub environments in a single console.
- See it all. Asset inventories, network visualizations, cloud spend, and configuration risk.
- Automate compliance assessments and save weeks of effort with audit-ready reports.
- Reduce risk without losing DevOps speed with Infrastructure as Code and container-image security.
- Get peace of mind that resources are prioritized with risk-assessed and color-coded alerts.

Protect Cloud Workloads and Data

Protect your host and container workloads with lightweight Linux and Windows protection via agent or API for Linux.

- Protect it all. Cloud, data center, host, container, Windows, or Linux.
- Identify sophisticated Linux security incidents at runtime without deploying a kernel module.
- Secure your Windows hosts and remote workers against ransomware, exploits, and never-before-seen threats.
- Control applications, lock down configurations, and monitor changes to critical Windows system files.
- Streamline threat investigations and response with XDR to prioritize and connect events.

Enforce Least Privilege

Manage identities before they're exploited with our help to implement least privilege with cloud infrastructure entitlements management across multi-cloud environments.

- Ensure all identities only perform actions that are required for their tasks and nothing more.
- Visualize complex, interwoven IAM roles to quickly highlight and prevent over-privileged IAM roles.
- Pinpoint unusual user access patterns and locations to identify credential misuse or theft.
- Utilize SophosAI to connect disparate high-risk anomalies in user behavior to prevent a breach.

Extend to Network and Application Security

Secure networks and applications with Sophos Firewall. This integrated solution combines multiple leading security technologies, including IPS, ATP, URL filtering, and WAF in a single solution. Featuring high availability and flexible SD-WAN and VPN connectivity to connect anyone, anywhere. For auto-scaling, Sophos UTM Firewall offers a separate solution for highly dynamic environments.

Modernize Cybersecurity Procurement

Sophos cybersecurity range is available from Sophos, our trusted partner network, and via AWS Marketplace to help customers modernize procurement processes, while at the same time, count towards any cloud provider consumption commitments that are already in place.

Learn more or speak
with an expert