What's New: Sophos Cloud Native Security

Complete multi-cloud security coverage across environments, workloads, and identities

SOPHOS
Cybersecurity delivered.

A Single Integrated Cloud Security Solution

The shift to cloud technology like hosts, containers, storage services, and Infrastructure as Code means organizations must increase their visibility to protect against misconfigurations, malware, ransomware, breaches, and more.

Sophos Cloud Native Security unifies the tools needed to provide that visibility and make your cloud environments tough, hard to compromise, and quick to recover. A single integrated solution available for Amazon Web Services, Microsoft Azure, and Google Cloud Platform, Sophos Cloud Native Security combines Sophos Cloud Optix and Sophos Intercept X Advanced for Server XDR.

With the Sophos Central console's single management view, you gain the power to hunt for multi-cloud threats, receive prioritized detections of incidents, and benefit from automatically connected security events to optimize threat investigation and response times – all in one place.

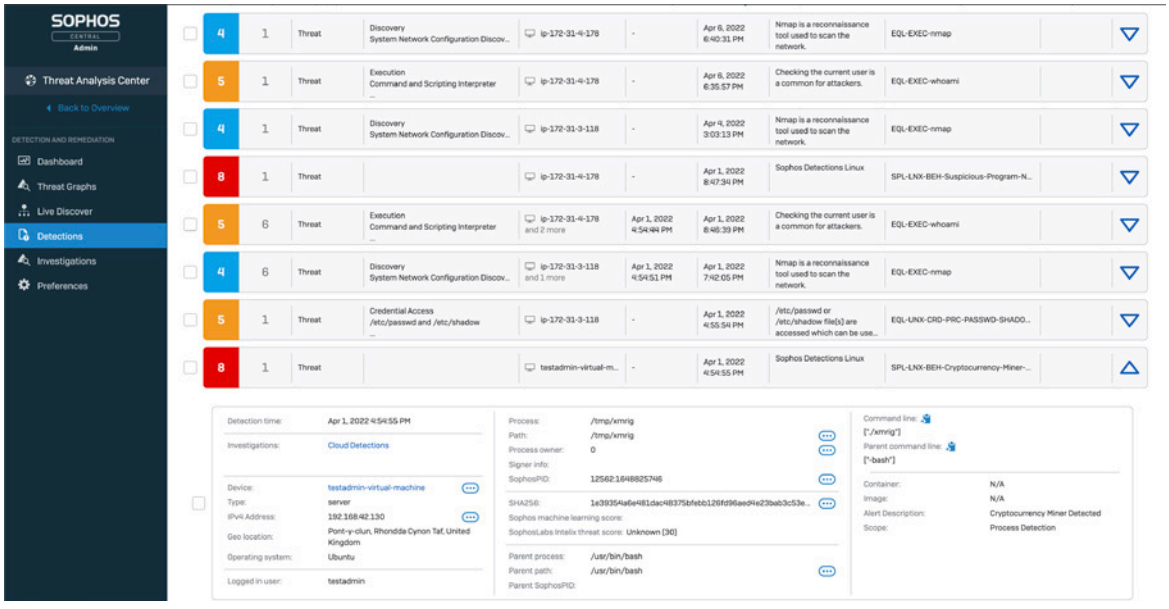
The Next Evolution of Sophos Server Protection

To secure your server workloads in the public cloud, Sophos has extended its trusted Windows protection to secure Linux deployments – one of the most prolific operating systems in the cloud.

Earlier this year, Sophos server protection for cloud workloads saw a major evolution in Linux and container capabilities with new behavioral and exploit runtime threat protection to identify sophisticated Linux security incidents as they happen.

Sophos Cloud Native Security provides the workload protection capabilities needed to protect your infrastructure and data now and as it evolves in the cloud.

- Protect it all. Cloud, data center, host, container, Windows, or Linux.
- Get performance and uptime with lightweight Linux and Windows host protection via agent or API for Linux.
- Identify sophisticated Linux and container 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 extended detection and response (XDR) to prioritize and connect events.



Example of Sophos XDR Linux runtime threat detections in the Sophos Central console.

Cloud Workload Protection Deployment Options

Sophos Central Management – This lightweight Linux agent gives security teams the critical information they need to investigate and respond to Windows and Linux behavioral, exploit, and malware threats in one place. Monitoring the host, this deployment option allows teams to manage their Sophos solutions from a single pane of glass, seamlessly moving between threat hunting, remediation, and management.

API Integration – The Sophos Linux sensor is a highly flexible deployment option that is fine-tuned for performance. The sensor uses APIs to integrate rich runtime threat detections in host or container environments with your existing threat response tools. It provides a greater level of control to create custom rule sets containing only the runtime behavioral detections needed to meet a specific security use case.

In addition to the Sophos Linux agent, the Sophos Linux sensor provides:

- More detections: Access to additional detections for application and system exploitation
- Configuration and tuning: Options to modify allow, and block lists for default detections
- Resource tuning: Configuration options to help optimize host resource utilization

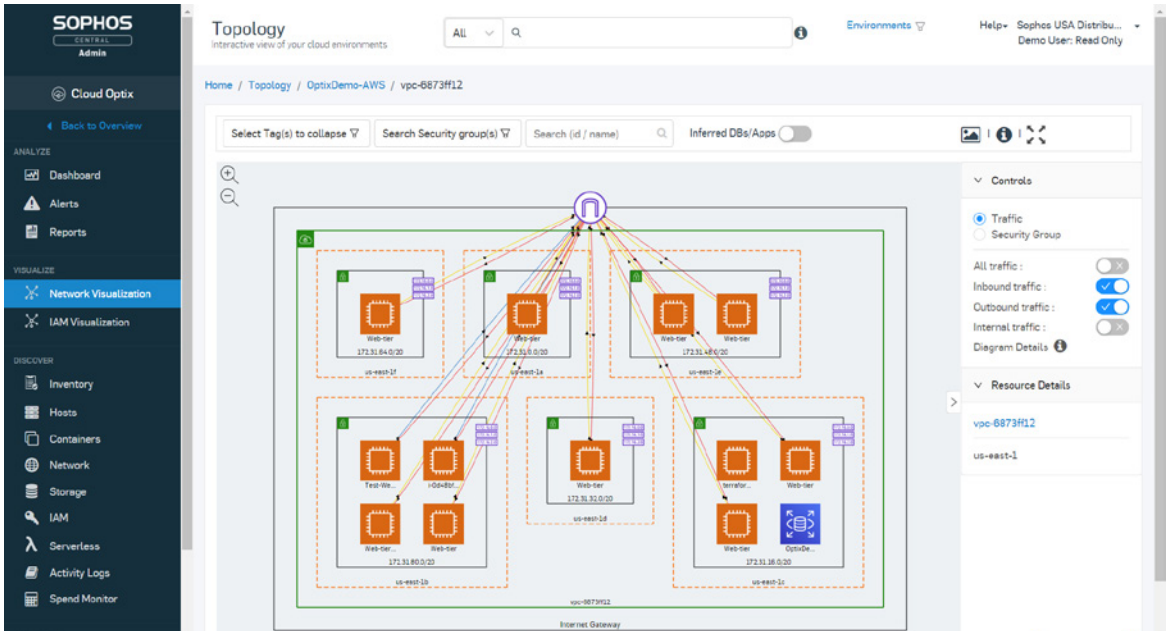
See More of What You Need to Protect

Reducing your entire attack surface across AWS, Azure, and GCP environments goes beyond protection and detection of cloud workload threats. That's why Sophos Cloud Native Security consolidates your security toolkit with one tool to include cloud security posture management, Kubernetes security posture management, Infrastructure as Code security, cloud infrastructure entitlements management, and cloud spend monitoring.

Get Multi-Cloud Visibility, Governance, and Compliance

Increase efficiency with agentless visibility and remediation tools across AWS, Azure, GCP, Kubernetes, Infrastructure as Code, and Docker Hub environments in a single console.

- Get the big picture with on-demand asset inventories and exportable network topology visualizations.
- Integrate cloud provider security services in a single view, including Azure Advisor, Azure Sentinel, AWS Security Hub, Amazon GuardDuty, AWS CloudTrail, AWS IAM Access Analyzer, Amazon Detective, Amazon Inspector, AWS Systems Manager, and AWS Trusted Advisor.
- Stop shadow IT with automatic asset discovery and visualization of Sophos workload protection agents and firewall deployments.
- Prevent and remediate configuration risks across hosts, containers, Kubernetes, serverless, storage and database services, and network security groups.
- Continuously monitor and maintain security and compliance standards with policies that automatically map to your environment and save weeks of effort with audit-ready reports. Policies include CIS Foundations Benchmark, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2, and Sophos best practices.
- Track cloud costs for multiple AWS and Azure services side-by-side on a single screen to improve visibility. Receive recommendations to optimize cloud provider spend from Sophos or integrate with AWS Trusted Advisor or Azure Advisor services.
- Reduce alert fatigue and efficiently detect quick wins and critical issues with risk-assessed and color-coded alerts showing detailed remediation steps.

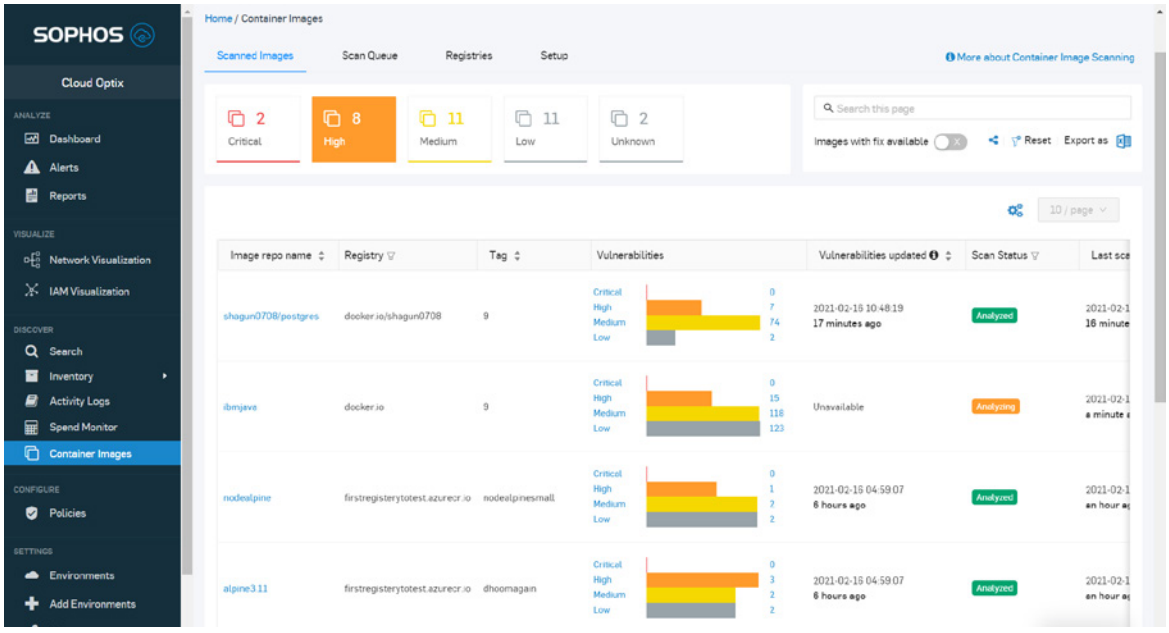


Example of Sophos network topology visualization for AWS with security group analysis.

Reduce Risk Without Losing DevOps Speed

Enable fast and secure development with integrated security configuration and compliance checks at any stage of the development pipeline.

- Automatically detect misconfigurations, embedded secrets, passwords, and keys in Terraform, AWS CloudFormation, Ansible, Kubernetes, and Azure Resource Manager template files.
- Prevent deployment of containers with operating system vulnerabilities and identify available fixes. With support for Amazon ECR, ACR, Docker hub registries, Infrastructure as Code environments, and images in build pipelines.
- Seamlessly integrate with GitHub and Bitbucket to receive on-demand scan results in Sophos Central or use the REST API to scan Infrastructure as Code templates and container images at any stage of development.

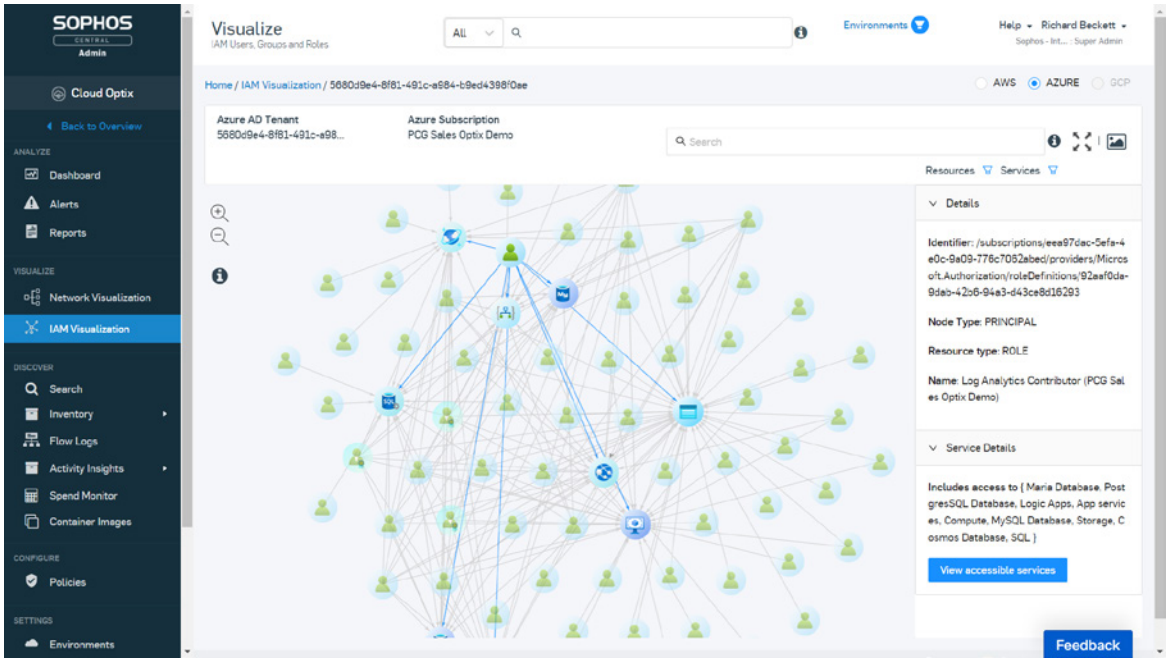


Example of Sophos container image scan vulnerability assessment results summary.

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.
- Pinpoint unusual user access patterns and locations to identify credential misuse or theft.
- Highlight orphaned, unmanaged, and outdated Microsoft Azure IAM roles used to gain access to environments.
- Visualize complex, interwoven AWS IAM roles to quickly highlight and prevent over-privileged IAM roles.
- Utilize SophosAI to connect disparate high-risk anomalies in AWS environment user behavior to prevent breaches.

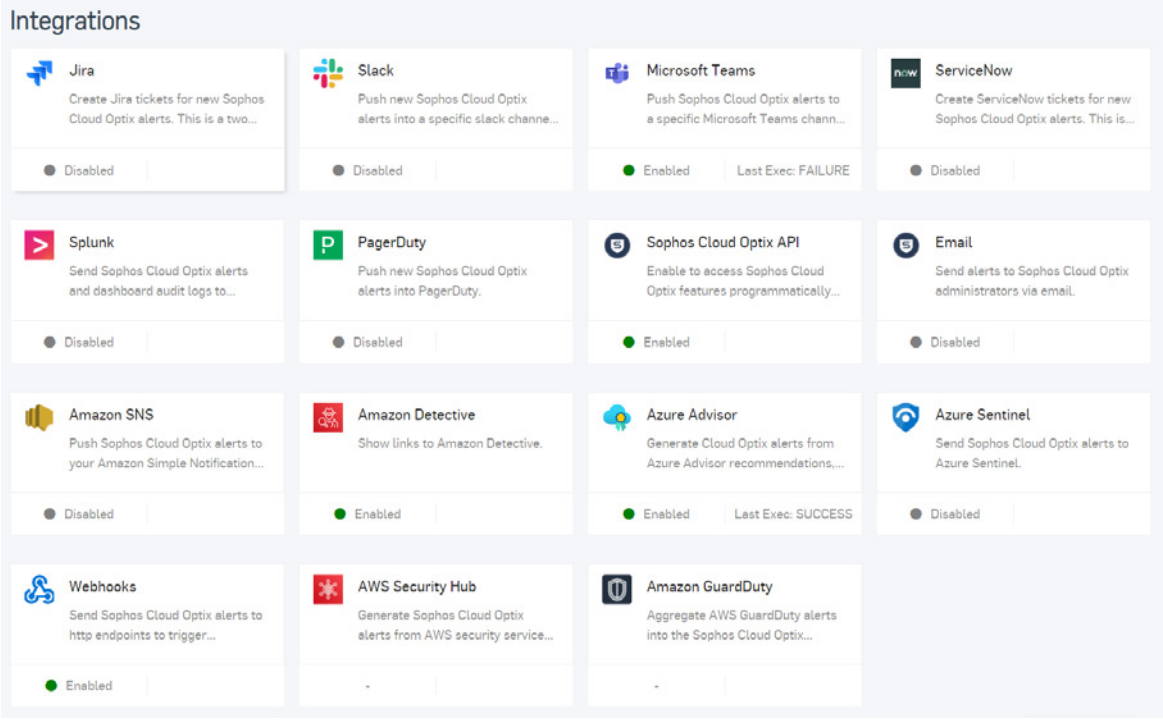


Example of Sophos IAM visualization for Microsoft Azure.

Streamline SecOps and Improve Collaboration

Increase agility across organizations with cloud environment security posture alerts integrated with popular SIEM, collaboration, workflow, and DevOps tools in just a few clicks.

- Security Operations: Integrate with Splunk, Azure Sentinel, and PagerDuty to receive instant notifications about of security and compliance events.
- Collaboration Tools: Send instant alerts to Slack, Microsoft Teams, or the Amazon Simple Notification Service (SNS) to collaborate on topics.
- Workflow Management: Embed alert response into standard workflows by creating JIRA and ServiceNow tickets from Sophos Central with two-way integration to avoid duplicate tickets.



Example of popular Sophos integrations to manage cloud security posture management alerts.

Partnerships That Augment Your Team

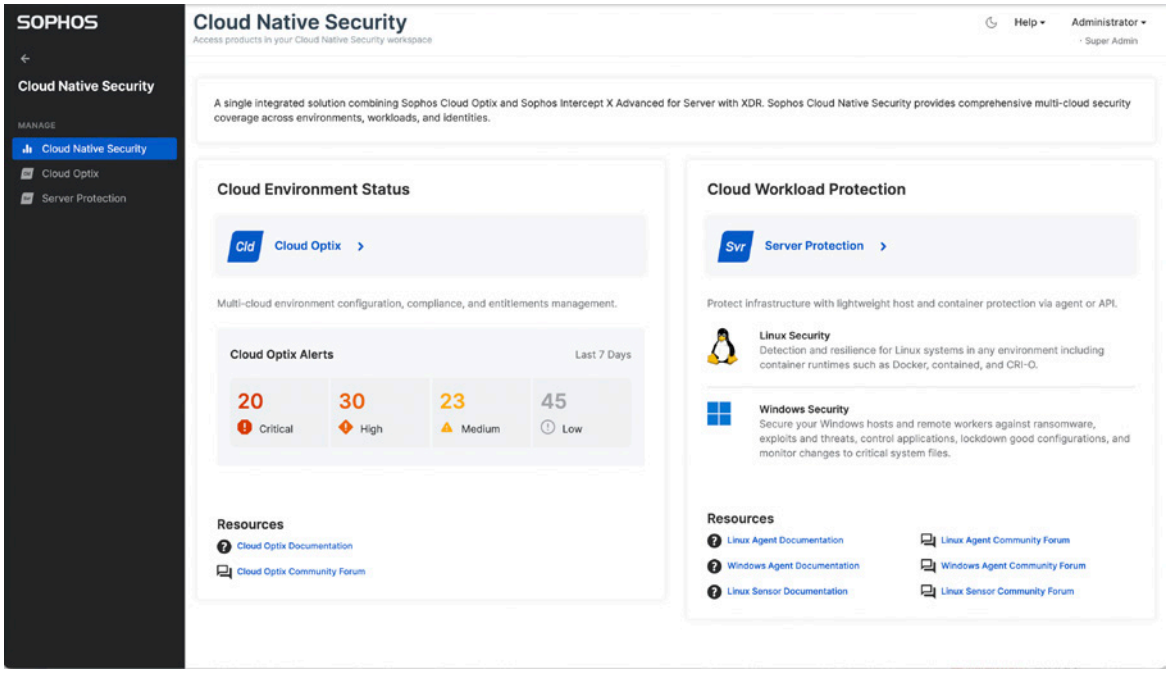
Manage protection your way – with your own security team, with the help of a Sophos partner, or via the Sophos Managed Threat Response (MTR) service to ensure 24/7 monitoring and response.

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

Sophos Cloud Native Security Availability

This new combined package is available to all customers and can be upgraded to from Intercept X Essentials for Server, Intercept X Advanced for Server, and Intercept X Advanced for Server with XDR.

Once activated in Sophos Central customers and partners will find a new 'CNS' item in the left-hand navigation. This links to a new Cloud Native Security summary dashboard providing access to Sophos Cloud Optix and Intercept X Advanced for Server with XDR products.



Example of Sophos Cloud Native Security dashboard in the Sophos Central management console.

Try it now for free

Register for a free 30-day evaluation at sophos.com/cloud

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

22-07-06 EN (DD)

SOPHOS