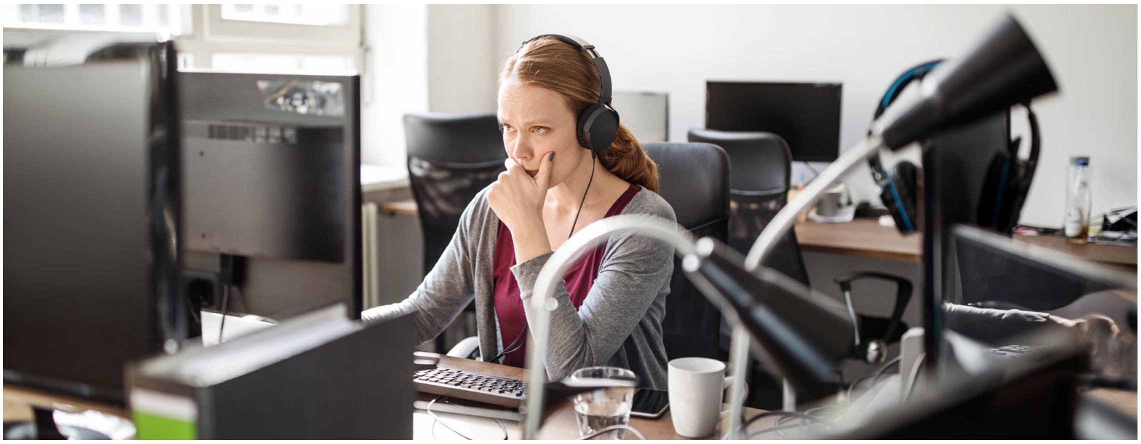
SOLUTION BRIEF

Maximize Cloud Readiness with Secureworks® and AWS



Take advantage of Amazon Web Services (AWS) cloud efficiencies with security in mind. Our solutions help you outpace and outmaneuver adversaries with precision, so you can adapt and respond to threats with confidence. We provide a combination of AWS security, AI-powered insights, and continuously updated Threat Intelligence with advanced correlation and analytics. Experience better security, improved visibility, and rapid remediation in the cloud, so you can get back to business.

Cloud Migration Challenges

The adoption of cloud based environments presents a new set of challenges when it comes to security, leaving organizations to balance the benefits and speed of cloud adoption with processes to secure assets and data from an ever-changing threat landscape. A sound security posture is a must, regardless of whether data is stored on-premises or in the cloud, but on-premises security skills and knowledge do not translate directly to cloud environments. We are all aware of the challenges organizations face finding and keeping skilled security analysts, but finding people who are knowledgeable about cloud security is even more difficult.

Organizations must understand which of their existing security tools also protect their cloud environment and assets. You need the ability to detect vulnerabilities and weaknesses in the cloud, identify the potential impact of any security issues discovered, and to make sure cloud security programs continue evolving and improving. Applying security best practices provides long-term benefits by not only safeguarding assets today, but also providing a framework for cloud security policies moving forward. This includes ensuring cloud configurations are optimized

Cloud Security Challenges

- Security skills shortages are exacerbated since on-premises security knowledge and experience do not directly translate to cloud security.
- Cloud enables business growth but requires additions and changes to your security program before, during and after cloud migrations.
- Lack of time and knowledge to correlate cloud security data with endpoint and network security data reduces ability to detect advanced threats.
- Multiple security tool management consoles add complexity and diminish security analyst efficiency and effectiveness.

with security in mind and performing an accurate security posture assessment of resources in the cloud.

AWS provides scalable cloud infrastructure for hosting, running, and managing business applications. Flexibility via on-demand deployments helps you respond quickly to shifting market demands, driving new and expanded cloud workloads. A vast catalog of AWS platform services can be used in conjunction with infrastructure services to speed development so you can go to market faster than ever before. However, it is important to include security as you plan your cloud journey. AWS advocates its shared responsibility model where AWS provides security of cloud data centers and access controls, but you are responsible for deploying, configuring, and maintaining the security of your resources in the cloud.

Reduce Risk in the Cloud with Secureworks

Whether you are just starting to migrate workloads to the cloud or have seen the benefits and are moving more of your business from on-premises to the cloud, Secureworks can help. Our wide range of solutions provide security to help you reduce business risk by identifying and prioritizing vulnerabilities; applying security analytics and correlating telemetry across endpoint, network, and cloud security solutions; and offering cloud security architecture assessments and configuration reviews.

Secureworks® Taegis™ XDR is an open cloud-native platform that combines the power of human intellect with insights from security analytics to unify detection and response across endpoint, network and cloud environments for better security outcomes and simpler security operations. XDR is an extended detection and response solution that consolidates best-of-breed security components into a holistic approach of proactive protection against complex cyber threats. The solution boosts the analyst experience with operationalized threat intelligence and automation capabilities that improve visibility and accelerate investigation and response. The XDR "Ask an Expert" live chat feature provides access to Secureworks analysts so your analysts can ask questions and enhance their cloud security skills.

Secureworks Taegis XDR provides a single view across your on-premises and cloud security. Our automatic correlation of security data across endpoint, network, and cloud identifies more threats while reducing alert fatigue. Our XDR Detectors integrated with continuously updated Threat Intelligence strengthen the capabilities of your analysts and support your cloud migration journey while delivering improved operational productivity. Secureworks® Taegis™ ManagedXDR is available for organizations without the ability to manage XDR themselves.

Better Together - Secureworks and AWS

Taegis XDR leverages data from multiple AWS solutions so you can move to the cloud with confidence. We identify security issues related to audit logs, S3 and EBS storage, EventBridge, IAM controls, VPC and network access and injection attacks on web applications.

Secureworks Differentiators

20+
Years of attack & threat data

1,400
IR engagements performed in the last year

300+
Expert security analysts, researchers & responders

52,000
Database of 52k unique threat indicators managed & updated daily

XDR ingests data from the following AWS solutions:

1. **Amazon GuardDuty:** Amazon GuardDuty provides threat detection monitoring for potentially malicious behavior in AWS accounts. GuardDuty looks for specific data in CloudTrail audit logs, S3 storage data logs, VPC Flow logs, and DNS logs. Amazon GuardDuty alerts are displayed in the Taegis XDR console to enable investigation and response across endpoint, network, and cloud from a single console.

2. **AWS CloudTrail:** AWS CloudTrail audit logs provide traceability into user and system initiated lifecycle and configuration actions on AWS resources, including calls from the AWS Lambda serverless service. Taegis XDR ingests logs from CloudTrail for automated analysis and threat detection and displays the data in the XDR console to enrich investigations. Taegis XDR can alert on a wide variety of lifecycle events on critical AWS resources like S3, EC2 instances, VPCs, etc.

3. **AWS Web Application Firewall (WAF):** AWS WAF provides HTTP access logs that can be used to guard against and monitor common methods of injection attacks that often target web applications. Taegis XDR ingests logs and alerts from AWS WAFs and provides supporting investigative evidence for a variety of attacks that target web applications.

4. **Application Load Balancer (ALB):** ALBs are used to distribute web application traffic across logical application servers in AWS. Similar to WAFs, they provide telemetry that can be used to monitor and alert on injection attacks, including those originating from within the same or other accounts in AWS. Taegis XDR ingests logs from AWS ALBs and alerts on a variety of injection attacks that target applications.

5. **VPC Flow Logs:** VPC Flow logs capture information about the IP traffic going to and from Amazon Virtual Private Cloud (VPC) network interfaces. VPC Flow logging provides a history of high-level network traffic flows within entire VPC, subnets, or specific network interfaces (ENIs). This makes VPC Flow Logs a useful source of information for detection teams focused on collecting network instrumentation across large groups of instances. They can also be used for training and spotting anomalous traffic as an indicator of a potential threat. Taegis XDR ingests VPC flow logs to provide investigative support and alerting when specific traffic patterns are observed like port scans, network enumeration attempts and data exfiltration.

6. **S3 Data Events:** S3 Data events can be optionally configured for tracking in CloudTrail. Data events provide detail on operations performed in the context of S3 buckets. Taegis XDR analytics can spot specific data-plane activities that help with determining data exfiltration risks and threats.

Customer Benefits

- Cloud assessments & configuration reviews reduce cloud breach risk.
- AI-based detections reduce the number of alerts and false positives.
- Save time with intuitive investigation workflows and single view across endpoint, network, and cloud.
- Be more confident in the cloud with integrated Threat Intelligence from the Secureworks Counter Threat Unit™ research team that continuously tracks 150+ active threat actor groups

XDR ingests data from the following AWS solutions (continued):

7. **Endpoint Agents and AWS Data Collectors:** You can instrument your Windows and Linux operating systems running on AWS (EC2) instances with endpoint agents that provide Endpoint Detection and Response (EDR) telemetry and alerts. Most automated Taegis XDR Detectors leverage EDR data to help identify potential threats so Secureworks includes our endpoint agent with XDR, or you can use any supported EDR agent. Taegis collectors may also be deployed to send telemetry originating from third-party soft appliances and supported syslog sources in AWS environments.

aws partner network

Advanced
Technology Partner

Public Sector Partner

Amazon Linux 2

Enable your Digital Transformation with Secureworks and AWS

Find Secureworks solutions that enable a more secure journey into the cloud on the AWS Marketplace. Take advantage of simplified software licensing and procurement with consolidated billing and flexible pricing options to help you unlock the best price. A growing number of AWS Marketplace customers across virtually every industry and geography are using AWS Marketplace to find, and quickly purchase, a wide variety of software and solutions to speed migration to the cloud.

About Secureworks
Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

About Amazon Partner Network
Secureworks is an Advanced Technology Partner, Public Sector Partner and Independent Software Vendor (ISV) in the Amazon Partner Network (APN). AWS ISV Partners provide software solutions that run on or are integrated with AWS. Secureworks leverages resources such as the AWS Well-Architected Framework to promote AWS best practices and AWS Foundational Technical Reviews validate the architecture and security of our customer-facing solutions.

Secureworks staff have more than 200 AWS Certifications, including AWS Certified Solutions Architect – Professional, AWS Certified DevOps Engineer – Professional and AWS Advanced Security certifications. Secureworks Taegis XDR is an Amazon Linux 2 Ready Product.

For more information, visit **secureworks.com**

Secureworks®