ALERT LOGIC

ALERT LOGIC® THREAT MANAGER™
NETWORK INTRUSION DETECTION SYSTEM (IDS) AND VULNERABILITY MANAGEMENT FOR CLOUD AND HYBRID ENVIRONMENTS

Threat Manager protects your hybrid infrastructure, applications, and cloud workloads. It combines a network intrusion detection system (IDS) with vulnerability management into a single managed security-as-a-service.

Reduce your attack surface with visibility into vulnerabilities hidden at all layers of your application stack

Identify suspicious activity in your network traffic

Meet compliance requirements faster by streamlining reporting of assessment results

Get 24x7x365 monitoring by GIAC-certified security analysts who are on the lookout for threats across your environments

PROTECTING YOUR BUSINESS FROM CYBER ATTACKS REQUIRES IDENTIFYING THREATS FROM THE OUTSIDE. AND, FINDING THE SECURITY GAPS YOU MAY HAVE INADVERTENTLY CAUSED ON YOUR OWN.

The internet is a double-edged sword for businesses. You need it to reach and interact with customers, but it also exposes you to a persistent array of network-based threats. The need to stay ahead of competitors and meet customer demand has created a culture where new apps need to be deployed constantly. Rapid development cycles can lead to mistakes being made that leave you exposed to attack. And the use of third-party and open source components during development can result in vulnerabilities being inherited through no fault of your own.

everbridge®

"Alert Logic solutions provide increased security and improved vulnerability assessment while at the same time delivering cost savings and eliminating the management burden of other solutions."

Doug Dearing, Technology Operations, Everbridge

KEY FEATURES AND BENEFITS

FIND THE THREATS THAT MATTER TO YOU

- Collect and analyze ingress, egress and lateral network traffic from across all your cloud and hybrid environments

- Compare your network traffic with our growing list of 97,000+ signatures that detect a wide array of attack methods, including exploits in web app frameworks, app stack components, and attack methods included in the OWASP Top 10

- Identify lateral movement, brute force attacks, privilege escalation, ransomware, and command & control exploits

- Detect cyberattacks that target your AWS containers with real-time detection of known and unknown exploits for AWS-deployed Docker, Kubernetes, Elastic Beanstalk, CoreOS, and Elastic Container Service (ECS)

- 24x365 security monitoring, expert incident analysis and live notifications of critical attacks by security analysts in our global SOCs by including ActiveWatch™ with your Threat Manager subscription

Full Stack Assessment & Detection Analytics

24 x 7 x 365 Expert Monitoring

Verified Incident Report

Live Notification and Help Within 15 Minutes of High-Severity Incident

Threat Manager + Active Watch

## IMPROVE YOUR VULNERABILITY MANAGEMENT MATURITY

- Identify 91,000+ security vulnerabilities and 8,600+ software configuration issues across all your environments

- Find security vulnerabilities on the perimeter of your cloud and hybrid environments before adversaries can launch exploits

- Identify OWASP Top 10 web application vulnerabilities in custom-built or commercial apps with PCI ASV-level scanning

- Get a complete list of missing security patches, unauthorized applications, and risky network configurations using non-intrusive, authenticated vulnerability scanning
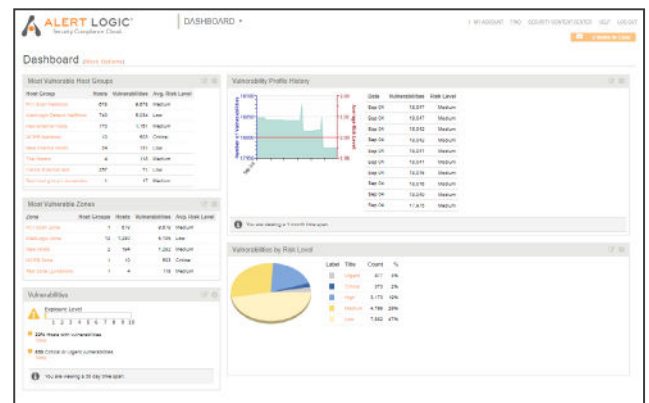
Demonstrate progress, and monitor the vulnerability status of your environments, specific hosts groups, zones, and services with our customizable dashboard and automated reporting.

ALERT LOGIC®

MEET AND MAINTAIN COMPLIANCE AT A FRACTION OF THE TIME AND COST OF TRADITIONAL SECURITY TOOLS

- Automate delivery of customizable compliance reports for PCI, HIPAA, SOX, and more

- Intuitive dashboard to view compliance status and drill-down a prioritized list of actions needed to maintain compliance

- Work with PCI ASV Certified experts anytime to ensure readiness for PCI audits and provide quarterly Attestation of PCI Scan Compliance
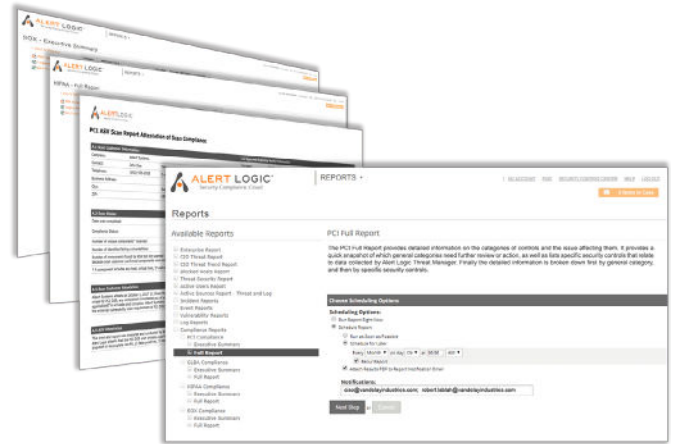
Automate report delivery for compliance officers and auditors—add tags, assign owners, and track progress over time
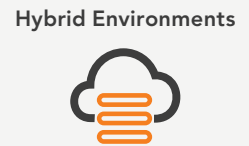
PLUG INTO READY-TO-USE SERVICES

- Get advanced security at a fraction of the time and cost of tool-only and outsourcing approaches

- Pre-built automated deployment capabilities get you up and running quickly – start seeing threats and vulnerabilities in just minutes

GET STARTED TODAY

On-Premise   Hybrid Environments
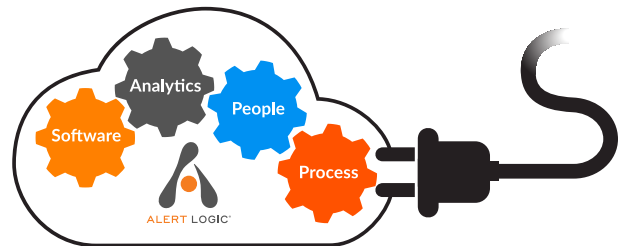
Learn more or schedule a demo at

www.alertlogic.com/solutions/network-intrusion-detection-system-ids/