ALERT LOGIC®

SOLUTION BRIEF:

ALERT LOGIC RISK AWARENESS

- Discover and easily visualize the assets across on-premises, physical, and virtual installations, hosted environments, public clouds, and container infrastructures
- Identify and prioritize vulnerabilities for remediation based on a personalized Threat Risk Index with vulnerability scoring and remediation advice
- Conduct a continuous exposure assessment through log management that provides prioritized remediation steps when changes are detected, to improve security posture
- Security incidents are consolidated in one console, giving you a single view into the security posture of your organization
- Protect Windows endpoints with an added layer of protection that can block attacks that traditional antivirus tools will miss
- It's difficult to gain visibility into assets and vulnerabilities in cloud and hybrid environments because services are constantly spun up and, instances are deploying and tearing down
- The changing nature of cloud and hybrid environments can result in configuration errors and, without the ability to regularly scan for misconfigurations it's difficult or impossible to ensure that these exposures have been remediated from the entire environment
- Traditional security tools can generate logs and reports, but manually sorting through hundreds or thousands of network security alerts and log entries to prioritize, and group exposures and vulnerabilities is time consuming
- Trying to protect endpoints with traditional tools is difficult due to the complexity of configuring these tools and, the overhead they require such as consuming CPU resources. Antivirus tools play an important role, but many attacks such as fileless techniques do not use a file, so there is nothing for the antivirus tool to scan for
- The top operational security headaches teams are struggling with includes misconfigured assets (40%) and lack of visibility (33%) [1]
- Organizations investigate only 56% of the security alerts they receive on a given day [2]
- 38% of attacks targeting companies would be fileless attacks [3]

40%
misconfigured

56%
investigated

38%
fileless attacks

TO ADEQUATELY ADDRESS RISK, YOU NEED TO PROTECT FROM THE OUTSIDE VIA THREAT MANAGEMENT AND, VULNERABILITY SCANNING. BUT YOU MUST ALSO IDENTIFY THINGS THAT MAY ALREADY BE INSIDE VIA LOG ANALYSIS AND EVENT PRIORITIZATION. AND, BECAUSE SOME ATTACKS TARGET ENDPOINT, YOU NEED PROTECTION THAT GOES BEYOND ANTIVIRUS TOOLS.

Alert Logic helps your risk awareness efforts with an integrated solution that combines software with advanced analytics and 24/7 expert services to improve your security posture and protect your data from breaches.

You'll be able to discover and visualize assets based on a continuous discovery process and find weaknesses with vulnerability scanning and health monitoring. We'll help you find malicious, inappropriate or accidental internal attempts to access data, applications and systems.

And, we'll round this out with the ability to thwart attack techniques that try to compromise Windows endpoints such as laptops, desktops and servers by recognizing techniques and stopping them before any damage is done.

WHY ALERT LOGIC FOR RISK AWARENESS?

- One solution that helps provide risk awareness related to attack from the outside, threats on the inside and that extends to your endpoints.
- Alert Logic provides a single view for your security projects that identifies software and application vulnerabilities, risky configurations and systems with encryption issues.
- Continuously ensure internal security with log management and application monitoring. Automated log Management collection and analysis to look for indicators of compromise, suspicious behaviors, or support incident response forensics. Web application log monitoring to identify and respond to suspicious application transactions, user behavior, and unusual transmission of personal data.
- Easily visualize the assets in an environment based on a continuous discovery process across on-premises, physical, and virtual installations, hosted environments, public clouds, and container infrastructures.
- Discover weaknesses in deployed assets and cloud-configurations with regular vulnerability scanning and health monitoring. Identify and prioritize vulnerabilities for remediation based on a personalized Threat Risk Index with vulnerability scoring and remediation advice.
- Visualize enterprise environments with an interactive asset topology that makes it easy to drill-down into an asset view to better understand the security picture.
- Threat risk index provides a personalized score across assets, networks, deployments, and tracks improvements over time. This report gives you the ability to leverage Alert Logic's security intelligence and public vulnerability severity data to gain insights into potential attack risk.
- Receive support, triage advice, and remediation guidance based on vulnerability scoring, asset exposure and proximity to the internet, whether an active exploit for the vulnerability is in the wild, and real-world attack potential.
- Incident reports included – so you don't have to create them. Cybersecurity experts review incidents and enrich with additional information and remediation actions.

bcs The Chartered Institute for IT

"We also use Alert Logic to monitor security groups for admin access roles; so, if something gets changed, we're alerted. In addition, we were alerted via the Alert Logic system to an RDP (Remote Desktop Protocol) protocol which was open in Azure. Alert Logic tipped us off to this and allowed us to patch this vulnerability before it became a more serious problem."

Cam Smith, Infrastructure Manager at BCS

ALERT LOGIC RISK AWARENESS BENEFITS

- Achieve regular vulnerability scanning and health monitoring
- Discover and easily visualize the assets based on a continuous discovery process across on-premises, physical, and virtual installations, hosted environments, public clouds, and container infrastructures
- Conduct a continuous exposure assessment through log management that provides prioritized remediation steps when changes are detected, to improve security posture
- Identify and prioritize vulnerabilities for remediation based on a personalized Threat Risk Index with vulnerability scoring and remediation advice
- Security incidents are consolidated in the same Alert Logic console, giving clients a single view into the security posture of your organization
- Protect Windows endpoints with an added layer of protection that can block attacks that traditional antivirus tools will miss
- Simple to use deployment tools make it easy for customers to extend security into new environments
- There's only one security solution to deploy, learn, and manage .

eComchain
Connecting Businesses to Consumers Online

"Alert Logic's offering is a better approach that helps us understand where we have risk, monitors and alerts us when there are threats, and provides us with the right level of security at a cost that makes sense for our business."

Hayes, Business Development Director, eComchain

[1] *Cybersecurity Insiders 2019 Cloud Security Report*
[2] *Cisco 2017 Annual Cybersecurity Report*
[3] *Ponemon 2018 State of Endpoint Security Risk*

ALERT LOGIC®