ALERT LOGIC®

PCI DSS

PRIORITIES FOR PCI DSS COMPLIANCE PREPAREDNESS

The Payment Card Industry Data Security Standard (PCI DSS) applies to companies of any size that store, process and transmit cardholder data.

PCI DSS has 12 requirements made up of a set of security controls that businesses are required to implement to protect credit card data and comply with the PCI DSS Standard. The goals of the standard include:

DEVELOPING A VULNERABILITY MANAGEMENT PROGRAM

REGULARLY MONITOR AND TEST NETWORKS

MAINTAINING AN INFORMATION SECURITY POLICY

ENSURE YOU HAVE THE EXPERTISE

or the dedicated staff required to keep pace

MAINTAIN SECURE systems, applications and an information security policy

69%

of respondents say their security teams are understaffed.

ISACA State of Cybersecurity 2019

63%

of the organizations assessed did not maintain all PCI DSS controls.

Verizon 2019 Payment Security Report

IDENTIFY THE SAFEGUARDS

for administrative and technical security

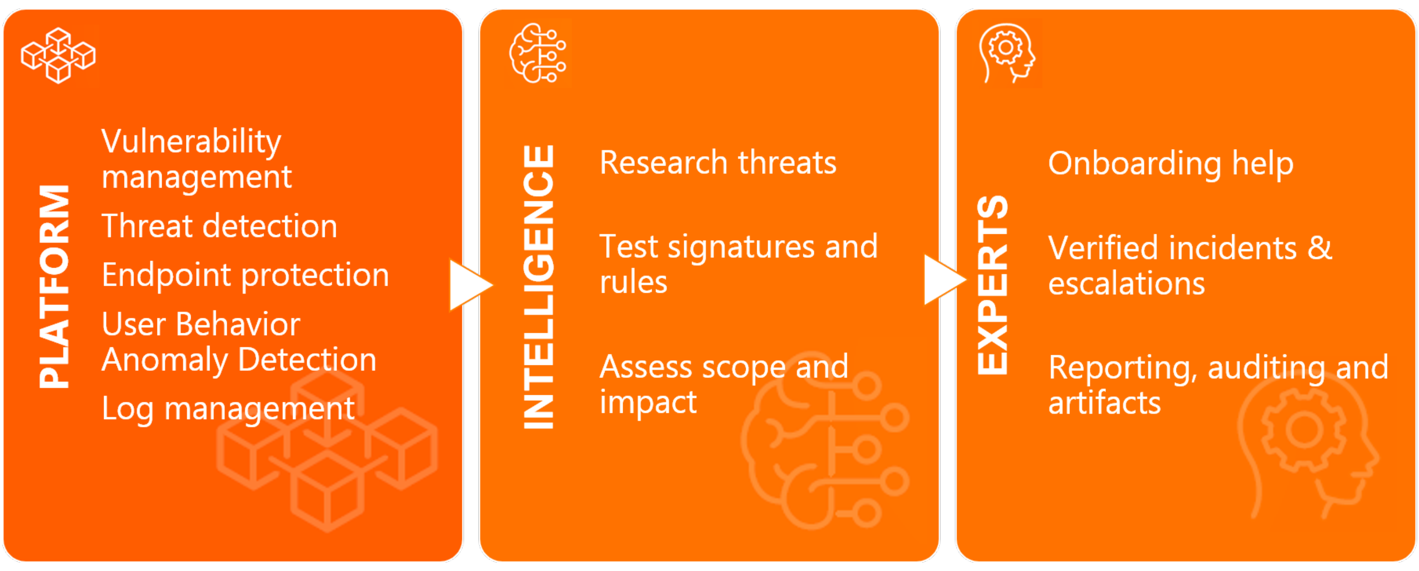
- Detect and prevent network intrusions
- Identify vulnerabilities and misconfigurations that might expose cardholder data
- Find suspicious- or active-breach activity

DEPLOY AUTOMATED SECURITY CONTROLS TO streamline assessment and detection of vulnerabilities and suspicious behavior

OFFLOAD THE DAILY TASKS related to meeting the PCI DSS requirements onto security experts

CONNECT PLATFORM, THREAT INTELLIGENCE, AND EXPERT CAPABILITIES

to deliver optimal coverage across your environments.



PLATFORM

- Vulnerability management
- Threat detection
- Endpoint protection
- User Behavior Anomaly Detection
- Log management

INTELLIGENCE

- Research threats
- Test signatures and rules
- Assess scope and impact

EXPERTS

- Onboarding help
- Verified incidents & escalations
- Reporting, auditing and artifacts

SUCCESSFUL PCI DSS COMPLIANCE PROGRAM USING ALERT LOGIC RESULTS

1. **ADVANCE** your PCI DSS compliance program in record time and quickly understand your state of compliance without hiring new staff.
2. **REDUCE** your risk with an improved security posture, reduced attack surface and risk of data breach.
3. **PROTECT** customer data from network and OWASP Top 10 attacks with web application scanning, a robust vulnerability library, and access to experts 24/7 to keep data safe.
4. **PREPARE** for audits, anytime with audit preparedness reporting that helps IT staff stay one step ahead of requirements, mandates and auditors.
5. **FREE UP RESOURCES** and implement compliance best practices with informed advice and remediation steps from our compliance experts.

LET'S GET STARTED

SCHEDULE A DEMO | TRY IT NOW | CONTACT SALES

CONNECT WITH YOUR ACCOUNT MANAGER TODAY TO LEARN MORE

ALERT LOGIC®