Corvil

SUCCESS STORY

LEADING INSURER REDUCES RISK WITH CORVIL SECURITY ANALYTICS

10M+
ONLINE CUSTOMERS

LARGE INSURANCE FIRM
LEADING PROVIDER OF GROUP BENEFITS, WEALTH MANAGEMENT AND OTHER FINANCIAL SERVICES

1000+
REMOTE ASSOCIATES AND REPRESENTATIVES

CHALLENGE

Need for Improved Insight and Context to Protect Critical Digital Operations

The firm recognized it faced rising corporate risk from digital services and operations in the wake of recent high-profile breaches experienced by other financial services firms. While the security team were skilled forensic investigators, their security ecosystem had to be extended to address:

- Inadequate visibility across the network to effectively identify vulnerabilities and investigate suspicious activity
- Limited insight to efficiently investigate the source and scope of security incidents

SOLUTION

User-Centric Network Traffic Analysis Integrated with Existing Security Ecosystem

Using Corvil, the security team gained new insights and enhanced the protection fabric from the perimeter across the network and into the endpoint. Multiple data centers were instrumented to provide:

- User-centric network traffic analysis of digital operations for customers, employees and remote associates
- Uniquely granular and contextualized insights into user and host threat activity
- Additional visibility into vulnerabilities, including weak encryption for user authentication and other critical communications

To enable more effective, faster investigation and response, Corvil delivered integrated workflows that connected next-generation firewall, endpoint detection and response, network traffic analysis and SIEM solutions, delivering:

- Operationalized threat intelligence from multiple sources to expand and accelerate breach detection
- Unified single-click actions for file extraction, threat analysis, impact assessment, and mitigation
- Integrated workflow to track attack indicators from the network into an endpoint, accelerating identification of the source and extent of attacks

RESULTS

More Efficient and Effective Security Operations

▲ Scope of threat detection through more comprehensive visibility and rapid use of threat intelligence
▼ Mean time to detect and remediation with integrated workflows
▲ Security team productivity by minimizing the manual effort required for incident investigation
▲ Value of existing security ecosystem by delivering seamless, integrated workflows across best of breed products addressing multiple threat surfaces

Ecosystem Integrations

splunk> Carbon Black. paloalto proofpoint STIX TAXII

WWW.CORVIL.COM