TARGETED ATTACK PROTECTION

Avoid Business Disruption and IR Costs Through Integrated Protection Across Network and Endpoint

CHALLENGE

INCREASING DIVERSITY AND COMPLEXITY OF ATTACKS

Attackers are using sophisticated and customized malware and malwareless attacks to evade detection and achieve their objectives. Targeted attackers are creative, persistent, and often well-funded, gathering knowledge about an organization's defenses and IT infrastructure to extend their reach, while hiding within enterprise networks. In addition to defeating a continual stream of known attack techniques, enterprises must assume that their networks are already compromised by motivated, targeted attackers capable of bypassing traditional signature-based defenses.

SOLUTION OVERVIEW

STREAMLINED INVESTIGATION AND INTEGRATED PROTECTION ACROSS NETWORK AND ENDPOINT

With granular visibility and automated investigation across users, network and endpoint, Corvil and Endgame provide comprehensive protection and empower security teams to do more.

The joint solution combines Corvil's context-enriched, real-time visibility into network communications and user activity with Endgame's full-stack endpoint protection of the hardware, kernel, and memory to stop targeted attacks. The integration enables automated actions and integrated intelligence sharing across network and endpoint data sources to reduce blind spots and provide extensive and accurate detection, investigation, and precision response.

With automated data correlation, key security use cases spanning prevention, detection and response, and hunt are informed by real-time context. Workflow enhancements, including single-click investigations, empower analysts to rapidly investigate and stop active threats, such as anomalous user behavior or covert back-channel communications. Analysts can visualize and investigate communications for a given endpoint and gain deeper insight into host roles – relevant context for assessing risk.

By integrating endpoint threat protection with visibility into network traffic, user activities, and other traditional security blindspots, Endgame and Corvil enable customers to stop targeted attacks before damage and loss occurs.

HIGHLIGHTS

- Comprehensive visibility across user, network and endpoint
- Combined deep packet analysis with full stack endpoint defense across hardware-level, kernel, and memory
- Automated threat hunting through single-click pivots
- IOT and uninstrumented host threat identification
- Intelligence correlation and sharing across surfaces
- Surgical response to neutralize threats without disruption
- Detailed forensics
- Virtual security chatbots to elevate security analysts

> *"The Endgame - Corvil partnership provides the combination of deep shared insights across attack surfaces with automation and integrated workflows creating focused response needed to help ebb the rising frequency and costs of today's cyberattacks. It promises to provide relief to overburdened security teams who would otherwise be forced to work across fragmented toolsets."*
>
> EMA

KEY CAPABILITIES

Streamlined Integration

Simplified workflows combine the strength of network visibility and analysis with automated endpoint investigation and response. For example, one-click action to initiate hunts on new devices communicating as domain controllers or other key hosts that may be automatically discovered through their network communications.

Comprehensive Visibility

Granular visibility across network packet payload inspection and endpoint kernel and memory. The endpoint agent rapidly detects advanced attacker techniques such as privilege escalation, defense evasion, malicious persistence, and credential access, while network traffic surfaces tunneling, encryption and certificate weakness, remote control activity, and details of remote user actions to provide full depth of the attack.

Earliest Protection

Protection to stop targeted attacks by detecting ongoing malicious communications and advanced attacker techniques across the breadth of the attack lifecycle without relying on known indicators of compromise.

Precision Response

Precision response prevents damage and loss by blocking exploits, malware, and malwareless attacks, prohibiting adversaries from gaining a foothold in the enterprise.

Automated Triage

Automated alert triage by leveraging contextual dimensions of user, endpoint hunt results, and threat intelligence to minimize alert noise and prioritize analysts' efforts more effectively.

OUTCOMES

- Streamlined SOC operations and improved analyst productivity
- Lower adversary dwell times through early prevention and precision response
- Reduced IR costs through pre-loss threat neutralization and automated investigation

Combining Corvil's experience in safeguarding businesses of leading financial services and Endgame's heritage in protecting critical infrastructure from nation-state adversaries.

ENDGAME.

Endgame's converged endpoint security platform is transforming security programs - their people, processes and technology - with the most powerful endpoint protection and simplest user experience, ensuring analysts of any skill level can stop targeted attacks before information theft. Endgame unifies prevention, detection, and threat hunting to stop known and unknown attacker behaviors at scale with a single agent.

Corvil

Corvil is the industry leader for deriving Security, Operational, and Business intelligence from network data. As companies adopt faster and smarter machine technology, it becomes critical to tap into richer and more granular machine data sources to safeguard the transparency, performance and security of critical infrastructure and business applications. The Corvil streaming analytics platform captures, decodes, and learns from network data on the fly, transforming it into machine-time intelligence for network, IT, security and business teams to operate efficiently and securely in this new machine world. Corvil uses an open architecture to integrate the power of its network data analytics with the overall technology ecosystem providing increased automation and greater operational and business value outcomes for its users. The Corvil solution is trusted by leading financial institutions to safeguard their businesses across the globe involving 354 trillion messages with a daily transaction value in excess of $1 trillion.

CDS-180717