deepwatch + cybereason

Deepwatch & Cybereason Joint Solution Brief

ENDPOINT DETECTION AND RESPONSE

JOINT SOLUTION BENEFITS

- ✓ Next-generation Antivirus Protection
- ✓ Host-level Firewall Management
- ✓ Endpoint Threat Detection and Response
- ✓ Rich Threat Context for Rapid Response
- ✓ Reduced MTTD and MTTR
- ✓ Streamlined Investigation
- ✓ Single Agent | Cross-Platform
- ✓ Low CPU & Data Cost

Joint Solution Overview

After rigorous testing and customer feedback, Deepwatch has chosen Cybereason as the foundational cyber technology platform to deliver Managed Endpoint Detection & Response (MEDR) services to our customers.

With Cybereason, Deepwatch has the most powerful data engine in Cyber to protect customer networks and root out threats. Cybereason's platform will power Deepwatch's managed endpoint threat detection and response program. Cybereason is fully integrated with Deepwatch's Cloud SecOps Platform, enabling Deepwatch to manage endpoint detection, behavioral analysis, and response to eliminate threats attempting to breach the endpoint.

Deepwatch and Cybereason Use Case Overview

With Cybereason, Deepwatch's best-of-breed security services are now powered by the fastest data engine providing customers with faster, smarter endpoint threat detection, investigation and response. Deepwatch customers are able to redeem maximum value from Cybereason technology as Deepwatch seamlessly manages implementation, followed by continuous monitoring, tuning, and response services. Deepwatch addresses a number of important use cases that bring tremendous value to our customers. **These include:**

NEXT-GENERATION ANTIVIRUS PROTECTION (NGAV) AND HOST LEVEL FIREWALL MANAGEMENT

With Cybereason Deepwatch replaces legacy Antivirus solutions to up-level customer endpoint threat detection to seamlessly prevent against known and unknown threats - across platforms and attack vectors. Deepwatch also manages customer firewalls at the host level and enhances firewall threat detection and mitigation across platforms with threat intelligence and custom detection rules.

INTELLIGENCE, FORENSICS, HUNTING, AND AUTOMATED THREAT REMEDIATION

With Cybereason, Deepwatch analysts utilize advanced real-time telemetry, behavioral detection and interactive search across current and historical data on the endpoint (enterprise & BYOD) to protect customer networks. Deepwatch turns endpoint data into rich threat context (fueled by Cybereason Nocturnus threat research) so that customer security teams are quickly alerted to what happened, how, and what to do to stop the threat from moving laterally within the environment. Deepwatch configures specific rules across customer endpoints, as well as automated response policies to detect and resolve security incidents before they cause damage. Automated response policies are deployed to isolate hosts, delete files, execute commands and kill processes, leading to lower mean time to detect and respond.

SECURITY COVERAGE ACROSS ALL ENDPOINTS IN 1 UI (INCLUDING MOBILE)

Customers benefit from low CPU usage, no blue screens or system interrupts, an agent will not interfere with kernel, and no disruption to existing applications or security. While other vendors claim kernel access is required for full visibility, Cybereason developed a way to do so. While CPU can average 15-25% with traditional AV vendors, Cybereason's agent never exceeds 5%, averaging around 2%.

cybereason

ABOUT CYBEREASON

Cybereason is a full-stack cyber technology firm founded by elite military cyber experts with renowned expertise in targeted cyber-offense operations. Cybereason foresaw the future of Cyber was in data and thus Cybereason's Cyber Defense Platform was born. The platform collects, processes, correlates, and investigates more data, faster with greater insight than any other cyber technology bar-none. The Cybereason Defense Platform was purpose-built to protect organizations from the world's most advanced cyber attacks using 1 agent, 1 console, 1 award winning UX.

deepwatch

ABOUT DEEPWATCH

Deepwatch secures enterprises via its unique, highly automated cloud based SOC platform backed by a world class team of experts that protect your network and digital assets 24/7/365. Deepwatch extends your team and proactively improves your cybersecurity posture via our proprietary maturity model. Deepwatch's managed security services are trusted by leading global organizations.

CONTACT US

sales@deepwatch.com
7800 E Union Ave, Suite 900
Denver, CO 80237
855.303.3033
www.deepwatch.com