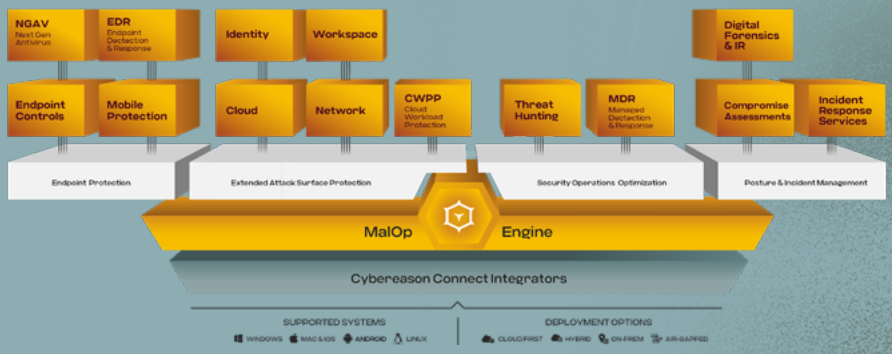
cybereason | DATASHEET

XDR
POWERED BY GOOGLE CHRONICLE



Cybereason XDR Platform

UNDEFEATED IN THE FIGHT AGAINST RANSOMWARE

KEY CAPABILITIES

Don't Chase Alerts, Intercept MalOps
Fully contextualized and correlated attack stories

Identify and End Attacks Faster
Improve detection and response intervals by 93%

Leverage All Your Event Data
Where other solutions limit data collected, Cybereason collects and analyzes 100% of event data

Remediate in Minutes, Not Hours
Save time on on every investigation with guided remediation

AI-Driven Security to Predict, Understand, and End Malicious Operations

The Cybereason XDR Platform moves beyond endless alerting to instead recognize, expose, and end malicious operations before they take hold. Using one agent, one console, and one team to defend all endpoints, the AI-driven Cybereason XDR Platform was designed to expose and intercept every MalOp (malicious operation). A MalOp is not an alert, but a contextualized view of the full narrative of an attack. Only Cybereason provides the actionable intelligence to outthink the adversary, the remediation speed to outpace their operations, and the insights to end any attack.

THE TOOLS YOUR TEAM NEEDS

The visibility to outthink

Track, visualize, and end malicious operations with the full attack story from root cause across every affected endpoint, device, user identity, application, and cloud deployment.

The speed to outpace

Analyze, adapt, and move faster than attackers, eliminating emerging threats in minutes rather than days. Whether a commodity attack or targeted threat, you'll understand the attack and remediate with confidence.

The precision to end attacks

Leverage automated and single-click remediation across the entire ecosystem to end attacks and dramatically reduce the need for lengthy analyst investigations.

PLATFORM MODULARITY

ENDPOINT PROTECTION

NGAV: Multi-Layered Prevention
Instantly block 0-day attacks, fileless attacks, new malware variants and other novel threats, ending lengthy investigations

EDR: End Advanced Threats
Get the complete story of a MalOp from start to finish, with contextualized and correlated insights that detect and end sophisticated attacks

ENDPOINT CONTROLS: Securely Manage Endpoints
Address security requirements and compliance with controls tied to different device types, implement personal firewall policies, and enforce disk encryption

MOBILE: Mobile Threat Defense
Protect your increasingly distributed perimeter by connecting both mobile and traditional endpoint risks into a single and complete view of a malicious operation

EXTENDED ATTACK SURFACE PROTECTION

WORKSPACE & IDENTITY: Protect Employees Anywhere
Find undetected signs of compromise through native integrations with email, productivity suites, identity and access management, and cloud deployments

CLOUD: Identity Monitoring and Workload Protection
Monitor for signs of account takeover and data exfiltration, and protect cloud workloads against threats like exploitation of undisclosed vulnerabilities and zero-day attacks

NETWORK: Correlate Network Telemetry Across Endpoints and Identities
Integrate with leading firewall and NDR vendors to consolidate alerts, correlate network context with user and asset activity, and enable guided response actions

CWPP: Cloud Workload Protection
Enhanced protection against malicious operations on cloud workloads, containers, and Kubernetes applications.

SECURITY OPERATIONS OPTIMIZATION

MDR: Accelerate Your Security Program
Fully managed security suite with proactive threat hunting, detailed monthly intelligence and reporting, and guided and active response actions

THREAT HUNTING: Proactive Mitigation
Search for evidence and suspicions tied with MalOps to identify unknown attacks and minimize damage or business disruption

POSTURE AND INCIDENT MANAGEMENT

DIGITAL FORENSICS & IR: Uncover Advanced Adversaries
Investigate events efficiently and effectively through end-to-end root cause analysis, real-time telemetry, and detailed forensics artifacts

COMPROMISE ASSESSMENTS: Identify Advanced Threats
Get a complete review of your organization's infrastructure to identify instances of compromise, undetected backdoors, unauthorized access, and any anomalous activities

INCIDENT RESPONSE SERVICES: Breach Containment
Immediate breach containment and expert remediation assistance includes in-depth investigations, root cause analysis, malware reverse engineering, and comprehensive incident reporting