cybereason® | DATASHEET

XDR® POWERED BY GOOGLE CHRONICLE

POWERED BY GOOGLE CHRONICLE

Cybereason XDR

ACHIEVE 10X THE SECURITY RESULTS WITHOUT 10X THE WORK

PLANETARY-SCALE PROTECTION

AI-driven XDR combines the Cybereason MalOp™, which analyzes over 23 trillion security events per week to deliver instant detection and incident response, with Google Chronicle's unrivaled ability to ingest and normalize petabytes of data from the entire IT environment for planetary-scale protection.

OPERATION-CENTRIC DETECTION AND RESPONSE

Instead of being alerted about individual events, users can instantly understand the entire attack progression across every device, user identity, application and cloud deployment to end them immediately. The Cybereason MalOp provides automated and guided response actions to reduce human error, upskill analysts and achieve a 10x faster time to response than competing solutions.

PREDICT ATTACKER BEHAVIOR

Defenders can shift from a labor-intensive, alert-centric posture to a predictive, operation-centric model. Through context-rich correlations, Cybereason XDR identifies subtle signs of malicious behavior and predicts an attacker's likely next steps to anticipate and proactively block attacks.

Your employees, IT infrastructure, and supply chains are distributed all around the world. Meanwhile, increasingly sophisticated adversaries have gained a significant advantage over traditional approaches to threat detection and response. Today's siloed strategies are expensive, introduce blind spots, and ultimately result in ineffective coverage. This is where the promise of eXtended Detection and Response comes into play.

In partnership with Google Cloud, Cybereason XDR powered by Chronicle predicts, understands, and ends attacks at planetary scale.

XDR INTEGRATIONS

WORKSPACE AND IDENTITY

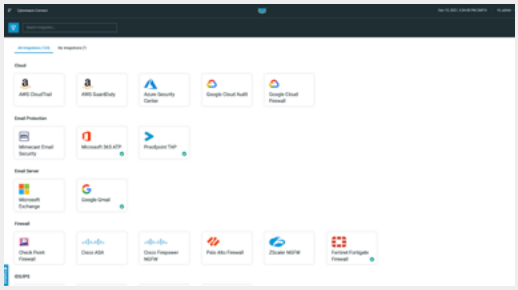
Protect Employees Anywhere | Cybereason XDR protects your employees with effective security far beyond the endpoint. Through native integrations with email, productivity suites, identity and access management, and cloud deployments, find undetected signs of compromise and end malicious operations.

CLOUD

Identity Monitoring and Workload Protection | With native integrations into Azure, AWS, and Google Cloud, Cybereason XDR monitors for signs of account takeover and data exfiltration, and can protect cloud workloads against emerging threats like exploitation of undisclosed vulnerabilities and zero-day attacks.

NETWORK

Deep Network Telemetry Correlation | Cybereason XDR integrates with leading firewall and NDR vendors to consolidate alerts, correlate network context with user and asset activity, and enable automated or guided response actions from the XDR console. Save on storage and analytics costs while upskilling your analysts with intuitive, extensible threat hunting.



cybereason® | DATASHEET

XDR
POWERED BY GOOGLE CHRONICLE

XDR FEATURES

BUILD AN EFFECTIVE, SCALABLE APPROACH TO SECURITY OPERATIONS.

Infosec teams today are facing burnout and overload from low-context alerts, of which more than half are typically false positives. As organizations expand and add assets and data sources, log management and SIEM solutions struggle to scale and become increasingly cost-prohibitive. Cybereason XDR provides a unified investigation and response experience that links together the diverse ways we work: on remote endpoints, mobile devices, cloud platforms, and email to prevent, end, and predict malicious operations.

PROTECT YOUR EMPLOYEES ACROSS ALL THE WAYS THEY WORK

To an attacker, anything connected to the internet is part of a company's attack surface. For Defenders, we must rely on siloed solutions each monitoring a specific part of our network. With diverse and deep integrations, Cybereason XDR delivers enhanced correlations across Indicators of Compromise (IOCs) and Indicators of Behavior (IOBs), the more subtle signs of network compromise. Out-of-the-box, Cybereason XDR provides Predictive Ransomware Protection and automatically blocks malicious executions and activity. Cybereason XDR allows analysts to understand how a malicious operation unfolds across email, cloud, endpoint, and network -- and exactly what to do about it.

IMPROVE INCIDENT RESPONSE TIMES FROM HOURS TO MINUTES

Despite spending millions of dollars on cybersecurity tools over the past few years, most organizations still can't detect or respond to cyber attacks in a reasonable timeframe. Cybereason XDR breaks down the data silos that attackers rely on to remain undetected by unifying device and identity correlations for faster, more effective threat detection and response while unlocking new predictive capabilities that enable defenders to anticipate and end future attacks before they begin.

ALERTING ISN'T ENOUGH. THAT'S WHY WE BUILT THE MALOP™

Cybereason delivers actionable context, so you can achieve 10x the results across your security operations without 10x the work.

PLANETARY-SCALE PROTECTION

Cybereason AI-driven XDR distinguishes between benign and malicious behavior, and links those behaviors across assets and identities for faster root cause analysis and incident scoping. Shift away from chasing false positives to identifying broader MalOps, analyzing all possible attack sequences, and ending attacks.

OPERATION-CENTRIC DETECTION AND RESPONSE

Cybereason XDR enables comprehensive monitoring across the entire attack surface to identify patterns and predict potential threats on a broader scale—connecting the dots between seemingly disparate or innocuous events to recognize indicators or behavior and take action to prevent or stop threats.

PREDICT ATTACKER BEHAVIOR

Cybereason XDR provides security teams with a multi-layer response framework, ranging from automatic prevention of threats like ransomware to guided response on what to do for each part of a detected malicious operation across endpoints, identities, and networks.

10X FASTER RESPONSE TIMES

Cybereason XDR breaks down traditional data silos that attackers use to remain undetected by unifying device and identity correlations for faster, more effective threat detection and response. Predictive analytics enable defenders to anticipate an attacker's next steps and proactively mitigate risk.

PROTECT WHAT MATTERS TO YOUR BUSINESS

Endpoint
- Prevent Ransomware
- Prevent Malicious Executions
- Malware Intrusion Lookback

Workspace & Identity
- Business Email Compromise
- Stolen User Accounts
- Data Theft & Malicious Behaviors

Cloud
- Dangerous Cloud Misconfigurations
- Crypto-Jacking & Malware
- API Misuse

Network
- Anomalous Connections
- Lateral Movement
- Anomalous Data Exfiltration

iOS

Barracuda · Office 365 · proofpoint · slack · mimecast · salesforce · okta · Active Directory · zscaler · netskope · workday

AWS

CISCO · F5 · JUNIPER NETWORKS · DARKTRACE · FORTINET · McAfee · paloalto NETWORKS · Check Point