cybereason® | DATASHEET

Cybereason XDR

A SINGLE POINT OF VISIBILITY, DETECTION, AND RESPONSE FOR THE ENTERPRISE

UNIFIED VISIBILITY, WITHOUT CHANGING YOUR SECURITY STACK

Cybereason XDR provides unrivaled breadth and depth of coverage by integrating with endpoints, applications, identities, networks, workspace, cloud sources, and operational technology. Cybereason's open XDR provides a vendor-agnostic architecture that allows you to bring your existing security stack.

UNCOVER MALICIOUS ACTIVITY THAT OTHER SOLUTIONS CAN'T

Cybereason XDR correlates and enriches data to uncover threats that siloed solutions miss. The Cybereason MalOp creates actionable attack stories of an attacker's malicious operation in a single correlated view.

RESPOND TO THREATS IN AS LITTLE AS 30 MINUTES

Cybereason reverses the adversary advantage with a managed XDR offering. Expanding the prowess of our managed detection and response capabilities across your entire technology stack, not just endpoints.

The modern security stack is overly complex, with many different tools and processes. Attackers move through the gaps of these siloed tools, and there is a desperate need to unify security operations.

XDR INTEGRATIONS

The legacy approach can't cut it, and Defenders need a new generation of capabilities purpose-built for the world in which they operate. Cybereason XDR fuses varied telemetry sources into a centralized console to create industry-leading efficiencies.

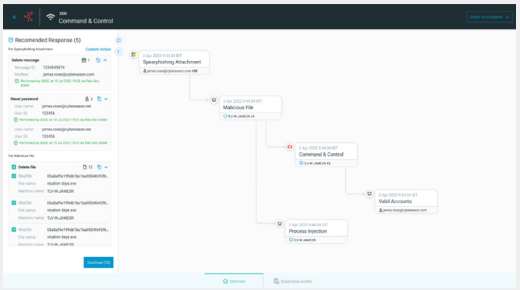
WORKSPACE	Cybereason XDR ingests data from workspace sources to extend protection beyond the scope of foundational tools in the traditional security stack, such as EDR. Native integrations with email, SaaS applications, and productivity suites enrich the overall intrusion story, including phishing attempts, email compromise, and attacker pivots to the endpoint.
IDENTITY	Cybereason XDR exposes signs of adversary activity by ingesting and correlating identity and access management data alongside endpoint and other sources. See the complete attack picture, including brute force attempts, suspicious logins, credential dumping, and attacker pivots to the endpoint.
NETWORK	Cybereason XDR includes broad integration options with firewall and NDR vendors to bring together the widest aperture possible of threat activity. Network context, firewall indicators, suspicious network connections, and suspicious data uploads/downloads are tracked, correlated, and prioritized based on severity.

CREATE ORDER FROM CHAOS WITH CYBEREASON XDR

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

The Cybereason XDR MalOp enables you to see the holistic attack story and defend against the most devastating class of cyber attacks.

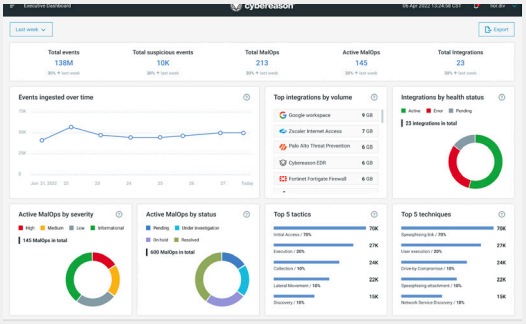
- A single attack story reduces the time to detect
- Correlation across all ingested data reduces the time to investigate
- Initiate response actions to cross-domain sources



TODAY'S COMPLEX ENVIRONMENTS DEMAND A CLEAR VANTAGE POINT

The Cybereason XDR Dashboard illuminates alert consolidation impact. Low-quality alerts are confidently deprioritized, and true-positive alerts are correlated with other attacker steps.

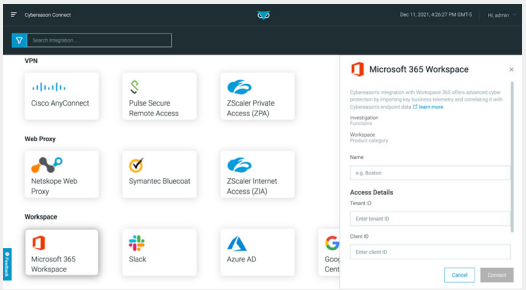
- Get a complete view of threats quickly by MITRE classification and focus on the right issues
- Contextually drill-down to MalOp & Investigation for actionable details
- Track operational metrics such as health of integrations and the number of MalOps triaged and resolved.



CLARITY COMES FROM VISIBILITY

Cybereason Connect allows you to quickly integrate relevant telemetry sources to create a full-scope detection and response platform for your environment.

- Add tenant details, client details and the credentials and the integration setup is complete.
- Select from integrations across identity, workspace, network, cloud, endpoint, mobile, OT and others.



CREATE A SINGLE SOURCE OF TRUTH

Cybereason XDR is a purpose-built platform for detection and response, purpose-built to ingest data from a wide range of telemetry sources and reduce MTTR.

REDUCE FALSE POSITIVES

Ingested alerts are often low quality and false positives. Cybereason uses enrichment and correlation, determines the veracity and severity of ingested alerts, and correlates those individual alerts into a broader operation-centric view.

REDUCE COMPLEXITY IN THE STACK

Creating a unified detection and response platform without XDR requires legacy strategies and an army of personnel to tune and manage the solution and can be overly expensive. XDR unifies detection and response while also streamlining operations and creating efficiencies.

ACCELERATE RESPONSE

Cybereason XDR is bi-directional to include responses to non-endpoint data sources through the MalOp console. End attacks efficiently from a central console.

RANSOMWARE & APT DEFENSE

Cybereason is undefeated against ransomware and delivers unrivaled MITRE ATT&CK coverage of adversary behaviors and tactics.

VENDOR AGNOSTIC DATA INFRASTRUCTURE

No limitations based on geography for backend data infrastructure and data normalization.