cybereason®

PROTECT YOUR GOOGLE DEPLOYMENT WITH Cybereason XDR

Cybereason XDR is the only platform that predicts, understands, and ends cyber attacks at planetary scale. Built in partnership with Google Cloud, XDR transforms petabyte-scale data into visual attack stories: MalOps™.

The Benefit: Out-of-the-box threat protection, unified, operation-centric threat detection, and planetary-scale data ingest & retention. Achieve 10x the security results without 10x the work.

INTEGRATION USE-CASES	PROTECT YOUR REMOTE WORKFORCE	PROTECT GOOGLE WORKSPACE	PROTECT GOOGLE CLOUD	PROTECT CLOUD WORKLOADS
Supported Environments	iOS			kubernetes
XDR Module	**XDR for Endpoints**	**XDR for Workspace**	**XDR for Multi-Cloud Environments**	**XDR for Cloud Workloads**
How It Works	■ **Single, do-no-harm sensor** supports Windows, Mac, Linux, mobile devices, including legacy OS ■ **Out-of-the-box effective** against ransomware, ransomware, and 0-day threats ■ **MalOp Detection Engine** reveals stealthy attacker activity in an easy-to-understand, visual attack story ■ Used by **leading partners for Incident Response**, malware analysis, and to power Managed Detection and Response offerings.	■ XDR **connects via API to Google Workspace** to ingest, enrich, and analyze key events & activity. ■ **User activity** across authentication, email, and file sharing is **fused with behaviors across global endpoints.** ■ Malicious activity, such as **malware, account takeover, and data exfiltration** is visually presented in real-time MalOps.	■ XDR **connects via API to Google Cloud** to ingest, enrich, and analyze key events & activity. ■ Anomalous & malicious activity, such as **signs of a compromised user, malware, and exposed credentials & buckets,** is presented in real-time MalOps. ■ XDR supports **Google Cloud in addition to Microsoft Azure & Amazon Web Services** for unified multi-cloud protection.	■ XDR uses a combination of **lightweight sensor & Kubernetes integration** for immediate Security Operations visibility without impacting DevOps. ■ XDR **protects workloads and containers wherever they reside** or move across infrastructure. ■ XDR uses a **multi-layer approach** that includes runtime detection, static AI detection, and identification of container-specific behaviors to identify threats.

cybereason

CYBEREASON X GOOGLE CLOUD SECURITY

Better Together

The Cybereason XDR platform integrates with powerful Google Security technologies for a unified investigation, hunting, and security workflow experience.

Product Offering	Unified NGAV & Endpoint Detection & Response (EDR)	VirusTotal Enterprise	Security Information & Event Mgmt (SIEM)	Extended Detection & Response (XDR)	Security Orchestration Automation & Response (SOAR)	BeyondCorp Enterprise	reCAPTCHA Enterprise
Solution Value	PROTECT YOUR GLOBAL ENDPOINTS	PLANETARY SCALE THREAT INTELLIGENCE	CLOUD-NATIVE DETECTION, ANALYTICS & RESPONSE	PREDICT, UNDERSTAND & END ATTACKS	SECURITY WORKFLOW OPTIMIZATION	ZERO TRUST ENTERPRISE SECURITY	WEBSITE FRAUD PROTECTION
Core Use-Cases	Prevent ransomware & malicious executions across global endpoints Operation-centric MalOp Detection Guided Incident Response	Automate alert triage Expedite and augment incident response Discover unknown threats Track adversaries & implement proactive defense	Threat Detection Threat Hunting & Investigation Security Visualizations	Protect Workspace, Identity, Multi-Cloud, and Network Operation-Centric (MalOp) Detection 24/7 SOC Monitoring	Reduce Analyst Caseloads Raise Analyst Productivity Create & Automate SOC Workflows	Secure Access to Corporate Resources Prevent Unintentional Data Loss & Exfiltration Connect to Legacy Applications	Protect your websites from fraud, spam, and abuse Lower friction for valid users Tune reCAPTCHA to your website's needs with customizable risk analysis engine
Key Differentiation	**Undefeated Ransomware Protection** Multi-layer prevention stops unknown ransomware & zero-day attacks. Top results in MITRE ATT&CK evaluations. **MalOp Detection Engine** eliminates alert fatigue & focuses analysts on what matters.	**Rich, actionable** crowdsourced threat intelligence platform.	**Infinitely elastic** Built on core Google infrastructure. **Cloud-native** Index massive amounts of telemetry and threat hunt at subsecond speeds.	**Built on Chronicle** Speed, scale, and cost-effective retention. **MalOp Detection Engine** fuses signals from the complete enterprise into actionable attack stories.	**Powerful for Engineers; Intuitive to Analysts** with a code-free playbook builder & support for python-based IDE. **Automate up to 98% of Tier 1** tasks to free up time for strategic initiatives.	**Scalable, reliable Zero-Trust** delivered via Chrome Browser. **Extensible Support for Existing App** & Endpoint Investments.	**Risk Analysis Engine** returns a score from 0.0 to 1.0, from abusive to likely good interaction. **Take action in the context of your site** by enforcing actions like two-factor authentication or email verification.
Cybereason XDR Integration	XDR natively supports Cybereason NGAV & EDR. Universal EDR support available Q2 2022.	XDR MalOps present threat intel findings, including VirusTotal, as part of broader attack stories. [Use-Case for VT Enterprise]	Cybereason XDR is built on Google Chronicle: Chronicle is fully embedded in Cybereason XDR.	XDR integrates with leading Workspace, Identity, Multi-Cloud, and Network technologies used across organizations today.	Cybereason MalOps can trigger Siemplify SOAR for scalable, end-to-end workflows.	BeyondCorp data & alerts can be sent to XDR for investigation & response. Available Q3 2022.	reCAPTCHA data & alerts can be sent to XDR for investigation & response. Available Q3 2022.
More Resources	Cybereason XDR for Endpoints	VirusTotal Enterprise	Chronicle Security	Cybereason XDR Product Brief	Siemplify SOAR	BeyondCorp Enterprise	reCAPTCHA Enterprise