cybereason | **PRODUCT BRIEF**

CYBEREASON XDR

Future-Ready Extended Detection and Response

KEY BENEFITS

- **Prevent:** Block common and stealthy attacks with a multi-layer approach
- **Ransomware:** Defeat unknown malware that attacks any of your global endpoints
- **Investigate:** Save time every investigation with the full attack story
- **Response:** Take action and prepare for the future with guided remediation

KEY INTEGRATIONS

WINDOWS MAC & IOS ANDROID LINUX

okta

EARLY ACCESS

aws Microsoft ORACLE

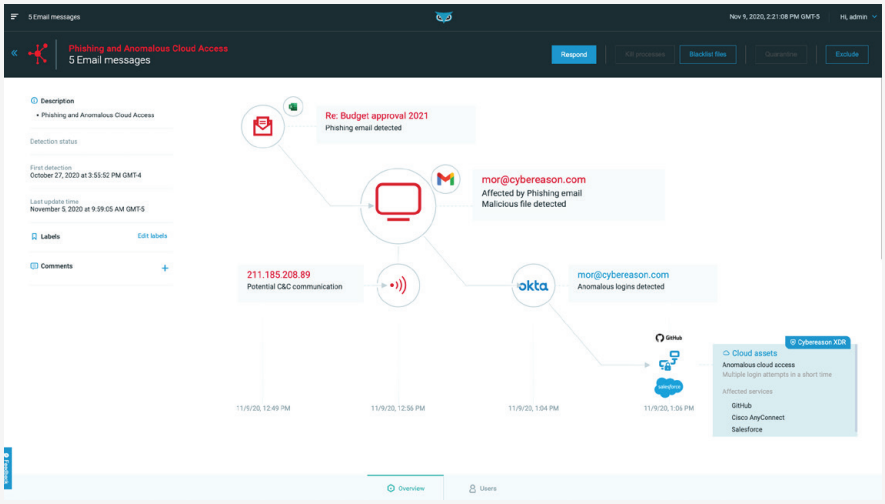
We are in a new world. Over the past year, your company network has likely already experienced massive change. Through 2024, an estimated 30% of all employees working remotely will permanently work from home. Employees need anywhere, anytime access, all while the quantity of cyber attacks we face have ramped up in number and ferocity. Ransomware attacks have increased, but so have data exfiltration and cryptomining attacks across cloud services and infrastructure.

If you're dealing with a single attack on a single asset, today's endpoint detection and response (EDR) tools are all up to task. But can your endpoint technology or SIEM correlate, and more importantly, **stop** an attack across identities, entities, and endpoints?

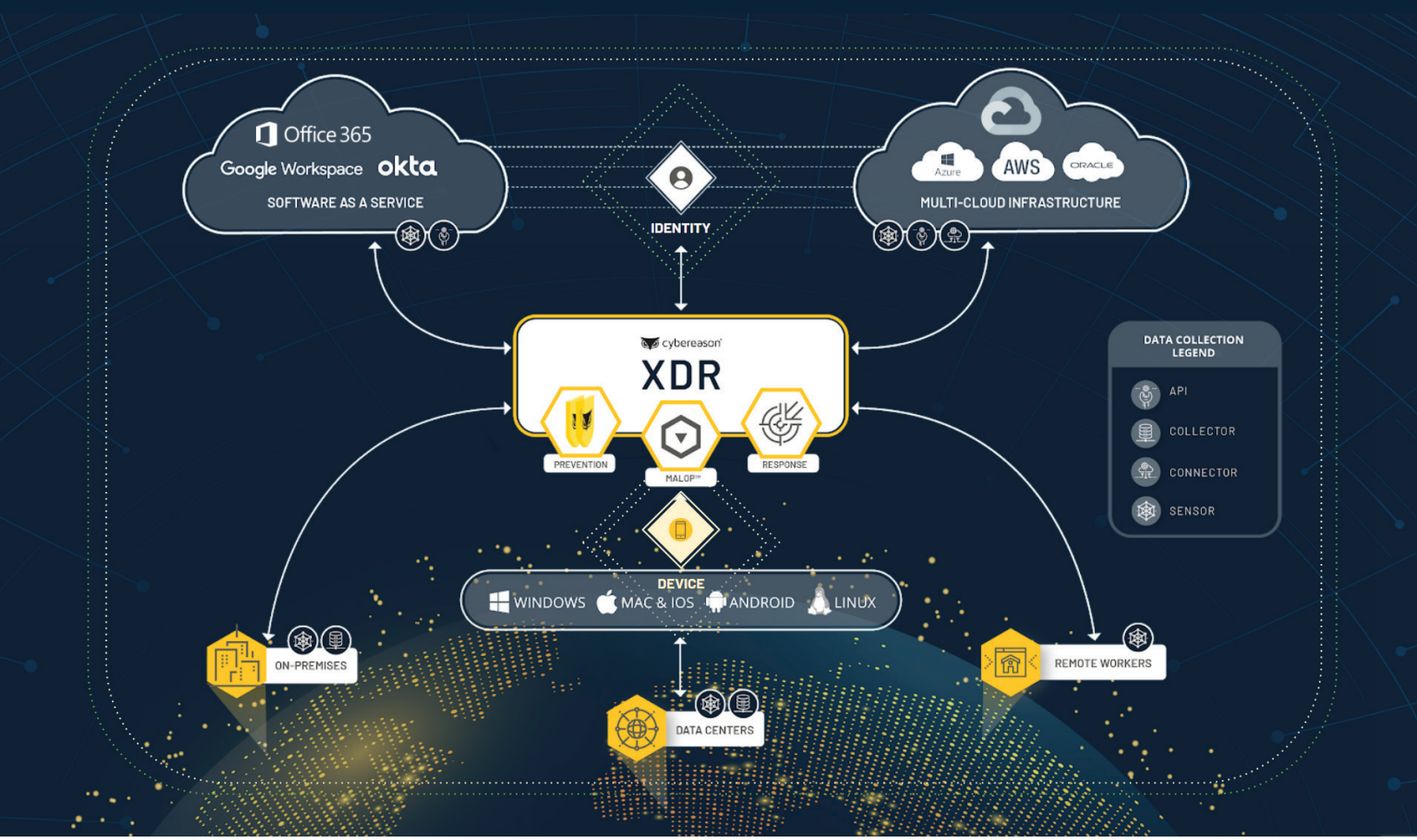
Cybereason XDR is built so you can pinpoint, understand, and end sophisticated attacks wherever they start on your network. By fusing together endpoint telemetry with behavioral analytics, you can protect your users and assets wherever they are in the world.

The Power of the Malop™

Instead of generating alerts or alarms, the Cybereason Defense Platform is *operation-centric*. The focus is to detect, expose, and end persistent **Malops** (malicious operations). With XDR, you can reduce false positives, investigate quickly and visually, and break the silos with complete remediation.



Save time and reduce human error with every investigation, whether it's a common or targeted attack.



What makes Cybereason XDR future-ready?

Understand Threats Beyond the Endpoint

Security begins with knowing what to protect. The Cybereason platform empowers analysts of all skill levels to quickly dig into the details of an attack without complicated queries or syntax. Cybereason XDR extends your detection and response capabilities from the endpoint to critical SaaS services, email, and cloud infrastructure.

Detections Ready Today, Extensible for Tomorrow

With Cybereason XDR, our Malop visualization delivers enhanced correlations across Indicators of Compromise (IOCs) and key Indicators of Behavior (IOBs), the more subtle signs of network compromise. XDR comes with hundreds of pre-built detections to identify suspicious user access and insider threats. Unlike SIEM and UEBA correlations, Malops have a much higher true-positive rate and augment the intuitions of your SOC team.

Guided Response that Understands the Business

Cybereason XDR is the only solution that makes it easy to understand the full attack story. Remediation actions, such as kill process, quarantine asset and remote shell, can be automated or accomplished remotely with a click. Further automation and playbooks are supported with our **Managed Detection and Response** and **Deep Response** module.

Security for All

With Cybereason XDR, there are no special skills required. New team members can investigate and remediate without calling on senior team members, and advanced teams can leverage intuitive investigation and remediation tools to pivot from one attack to another and spend more time hunting and less time triaging. The intuitive UI of Cybereason XDR was designed to increase SOC efficiency by automating common tasks and empowering any member of the SOC to quickly understand the scope and impact of threats so that they can act immediately.