cybereason® | SOLUTIONS

Cybereason Private Infrastructure Protection

FOR UNIVERSAL DEPLOYMENT

IT environments are diverse and varied, with no standard boilerplate to a network structure. This diversity complicates the task of securing the endpoint. It may also be cost-prohibitive or impossible to update legacy IT systems to something with more security options. There are many good reasons to not fully commit to a public cloud for all IT needs, and many organizations are maintaining at least a portion of their environment as private infrastructure. Cybereason adapts deployment around your specific needs, with universal compatibility with legacy and niche IT systems.

Deploy Anywhere with Cybereason

Private Cloud | Public Cloud | Hybrid Environment | On-Premises Data Center | Air-Gapped Environments | Specialized, Niche IT Systems | Legacy OS | Standard OS - Windows, Mac, Linux

Maintaining a private infrastructure makes sense for a variety of reasons and having more of an on-premises IT stack is in a Renaissance period, with many large and heavily regulated organizations keeping more data and operations under the same roof. Virtualization and containers have made local assets more efficient than ever, and this newfound productivity means that physical IT assets will always make up an important portion of the network configuration.

The way you do business is unique to you. Every environment is like a fingerprint or a snowflake - unique, specialized, and like no other.

Protection should adapt around the Defender and your way of doing business, not the other way around, and without added expense or pressure to change.

IDEAL FOR

HIGHLY REGULATED BUSINESSES

While regulations have obvious benefits and exist for a reason, compliance requirements undoubtedly complicate security. Many organizations are required to keep data and certain parts of IT on-site, or maintain an auditable trail of IT activity.

FEDERAL ORGANIZATIONS

Certain Agencies have requirements to meet maximum security needs, like an air-gapped environment and strict data controls.

FINANCIAL SERVICES

Large FinServ organizations are simultaneously the most attacked and the most regulated sector, with PCI-DSS, GDPR, FINRA, SOX and other compliance mandates that impact IT.

MANUFACTURING

Manufacturing organizations often have incredibly specific IT needs, and could maintain specialized IT systems that require security and are essential to day-to-day business.

REGION-SPECIFIC DIRECTIVES

Under GDPR, organizations in the EU must keep data within the EU. Many organizations follow region-specific guidelines related to IT and data security, and those systems need a higher level of protection due to their sensitivity.

HIGH COMPUTE COMMITMENTS

Customers of public cloud providers with large contracts and high compute commitments can deploy Cybereason and count towards the usage.

CYBEREASON PRIVATE INFRASTRUCTURE PROTECTION

Ultimate Flexibility in Deployment | Deploy to anything with universal coverage options for any data source or specialized IT system.

Protect On-Site Assets | Leverage existing infrastructure and protect on-premises endpoints and air-gapped environments.

Single Sensor, Single Console | Low impact sensor for high visibility into difficult-to-monitor areas with all data fed into a single, easily managed console.

Meet Compliance and Auditing Requirements | Keep data in-region and maintain an auditable trail of detection and response activity to meet compliance needs.

Fully Supported | Private Infrastructure Protection technology is backed by a fully supported team to guide you through a tailored deployment and innovate future enhancements. Dedicated support team for

The Cybereason Difference

UNDEFEATED PREVENTION	CONTEXTUALIZED VISIBILITY IN THE FULL OPERATION	ENRICHMENT VIA THREAT INTELLIGENCE
Aggressively prevent threats with industry leading efficiency. Predict pre-executed threats, block based on behaviors, and end ransomware.	Alerts mean little without context. Cybereason delivers actionable visibility, correlated and contextualized and displayed in our MalOp™ view for efficient response.	Enhance detections with open-source threat intelligence, 3rd party threat feeds, and intelligence that surfaces from our in-house Nocturnus team

STREAMLINED RESPONSE AND RECOVERY	RICH TELEMETRY AND LENGTHY DATA RETENTION	ARTIFICIALLY INTELLIGENT ENDPOINTS
Guided, one-click remediation that addresses all aspects of an active threat to restore systems to a trusted state. Full forensic toolkit and DFIR options as needed for more sophisticated InfoSec teams.	Cybereason aggregates the most telemetry of any EDR vendor and retains that data for longer periods for a full-scope analysis of the environment and threat hunting over a protracted period of up to 18 months.	Detect the sublest signs of attack activity through deep learning and graph analysis. Predict, analyze, validate and improve.

Business Value

Count towards compute commitment with public cloud providers	Secure what's unique to you without expensive migrations or hardware changes	Don't compromise security due to nonstandard IT systems

We deliver the highest security value available in the unique configuration of your environment, with industry-leading results that you can rely on in the fight against cyber adversaries. We offer a white glove solution and service to fully deploy to any configuration conditions in a tailored way.