cybereason

Rapid Deployment and Immediate Detection

The Cybereason Detection and Response Platform was purposely built to be an easy-to-deploy and easy-to-manage solution. Deployed and ready to hunt within 24 to 48 hours, the platform immediately provides military-grade defense capabilities through continuous, real-time monitoring, automated detection, complete situational awareness and a deep understanding of attacker activities.

Cybereason Sensors

Cybereason Sensors, our unique data-gathering agents, are quickly deployed on end user machines and servers. End User Sensors collect data from Windows and Mac OS X endpoints. When malicious incidents are detected, End User Sensors can execute response actions, allowing for swift containment. Server Sensors provide visibility into your Windows and Linux server environments, enabling detection of malicious activities.

How the Sensors work

The Sensors collect detailed telemetry information to determine changes in processes, users, machines, memory, registry, network connections and other events. The information is forwarded continuously and in real time to the Hunting Engine, the in-memory graph and "brain" of the Cybereason Platform. When a malicious event is spotted, the Sensors perform remediation actions like isolating infected machines from the network, terminating processes, quarantining files and deleting registry keys.

Minimal business operations interruption

Cybereason Sensors run continuously in user space, not kernel space. This greatly reduces the risk of affecting endpoint performance or user experience, while continuously gathering all the essential data for detection and response. The Sensors are installed without a system restart, minimizing potential interruption to business operations.

The Sensor size is less than 5MB, uses 50MB of memory on average and transfers less than 10MB of data per day. It only adds a processing overhead of approximately 1-3%.

Zero configuration deployment

The Cybereason Sensors are preconfigured with all connectivity options, so that you do not need to make configuration changes. The Sensor can be either downloaded from the Cybereason server, or through software distribution using IT endpoint management solutions like Microsoft Systems Center.

Pre-built detection engine

The Hunting Engine comes pre-built with a wide range of detection models designed to identify known and unknown elements of an attack and new attack techniques, with no up-front configuration or tuning. This means that you can start detecting and responding to security threats as soon as the Hunting Engine begins to receive data from the Sensors.

Cloud-based and on-premises deployment

The Hunting Engine is offered as a cloud service, enabling immediate implementation and provisioning. This lets you focus on identifying and terminating malicious operations quickly and easily. You can be detecting and responding to incidents within 24 hours.

Cybereason uses Amazon Web Services to host its cloud services, giving you control over the AWS Regions (geographical data center clusters) where you want to deploy. This helps alleviate latency concerns as well as satisfy data sovereignty requirements. Using AWS also gives you more cost-effective strategies for resiliency and disaster recovery. Moreover, deploying in AWS has significant security advantages, since AWS data centers are built to satisfy the security requirements of the world's most security sensitive organizations.

If you prefer to host Cybereason on-premises, Cybereason provides an Open Virtualization Image (OVA) that you can deploy in a virtual infrastructure. A single Cybereason server can support up to 30,000 endpoints.

About Cybereason

Founded by members of the Israeli military's elite cyber-security corps, Unit 8200, Cybereason's technology is based on their deep understanding of complex hacking operations. The Cybereason Endpoint Detection and Response Platform leverages big data, behavioral analytics and machine learning to uncover, in real time, complex cyber attacks designed to evade traditional defenses. It automates the forensic investigation process, connects isolated malicious events and visually presents the full malicious operation. Cybereason is privately held and headquartered in Boston with offices in Tel Aviv, Israel and Tokyo, Japan.