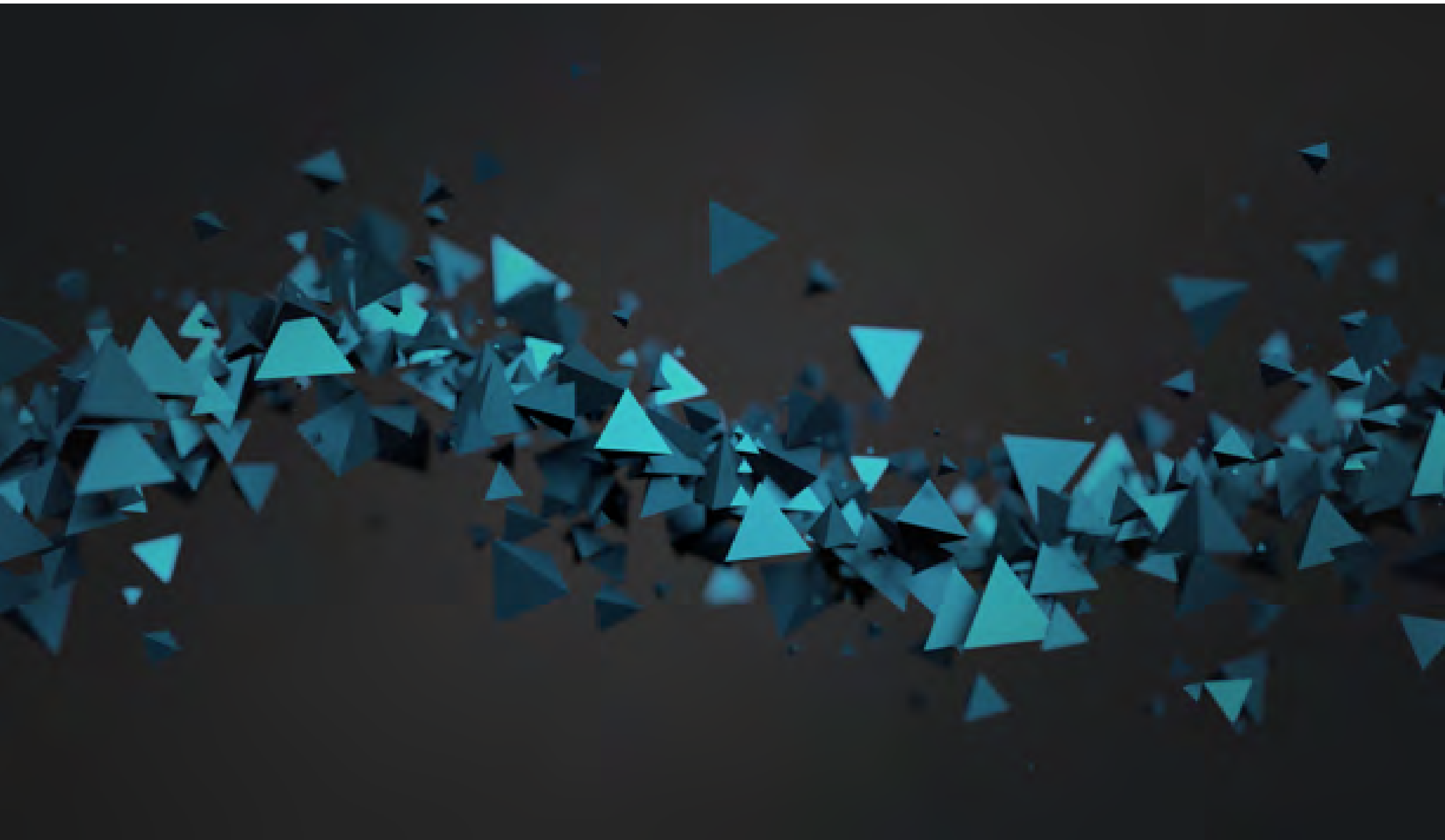
cybereason

The Next-Gen Endpoint Advantage

7 Unique Capabilities of the Cybereason Endpoint Detection and Response Platform



Cybereason’s fresh take on endpoint security

Detecting and effectively responding to advanced persistent threats requires obtaining ongoing, comprehensive endpoint visibility. Endpoints are at the heart of every cyber attack. They’re commonly exploited by hackers to perform penetration, lateral movement and persistence.

Endpoints are attractive targets for hackers since they’re vulnerable by nature and connected to users. This also makes it hard for security teams to develop and execute an effective endpoint security program. In many cases, intervening on the endpoint can easily impact user experience, affecting productivity and business continuity.

> *Many of our customers rolled out our platform on tens of thousands of endpoints within hours.*

At Cybereason, we believe effective security starts with real-time attack detection. Using continuous endpoint monitoring, advanced analytics and visualization of the detected attack story, detection and response are immediate. Here is our fresh approach to endpoint security:

1. Proven in complex enterprise environments

Advanced endpoint products shouldn’t interfere with other applications. They have to seamlessly and effectively work in existing IT environments without impacting business continuity or productivity.

We designed our endpoint data collection system keeping in mind the challenges enterprises face. We don’t interfere with the user experience or network flow, or burden IT and security departments with more work.

2. Zero end user impact

Cybereason Endpoint Silent Sensors observe without interfering and perform deep monitoring entirely from the user space. This unique approach developed by Cybereason provides kernel-level monitoring without a kernel component. Kernel-level code can lead to blue screens and system crashes. Our sensors will never cause a blue screen simply because they cannot. Our user-space implementation is designed to never disrupt the operating system or the processes running on the machine.

3. Speedy and simple rollout

Simplification is critical in today's complicated IT security environment.

Some security products are notorious for being difficult to deploy and maintain. Often, after a long deployment period, the solutions require maintenance and need to be adjusted to accommodate changes in the IT environment. In other cases, some hardware also needs to be installed, adding complexity and cost.

The Cybereason platform is operational immediately after being deployed. Many of our customers rolled out our platform on tens of thousands of endpoints within hours. SoftBank, for example, deployed Cybereason on several thousand endpoints in less than 48 hours.

Additionally, during the first 24 hours after deployment several customers detected an attack that had been compromising their network for a lengthy period of time. We discussed such a case in a **research paper.**

4. Zero system maintenance

After the Endpoint Silent Sensors are installed, businesses don't have to worry about maintenance. Unlike many detection platforms, Cybereason never requires any tweaking when your network architecture changes.

It seamlessly operates with any change in your environment. And most importantly, system updates are remotely deployed by us.

5. Complete attack visibility, endpoint and network

Cybereason's Endpoint Silent Sensors collect data beyond the endpoints. The combination of endpoint data, such as processes, files and user behavior, with network information, like inbound, outbound and internal communication, enables the Cybereason platform to detect and present a complete attack story.

6. Say goodbye to detection management

Many security products require constant manual updating to keep the detection engine aware of new threats. Whether done by internal teams or outsourced, security experts spend time and effort building parsing rules that issue alerts on specific indicators of compromise. They routinely update their queries based on new threat intelligence and attack methodologies.

> *You don't have to dig through historical logs and hope evidence is still there when investigating a breach. With our real-time collection, no piece of data is ever missing.*

Cybereason's malop detection engine removes the burden of keeping definitions and rules current. Based on a deep understanding of an attacker's methodologies and using machine learning, we build complex rules and queries that detect known and unknown threats.

In addition, our centralized platform completely offloads decision making from the endpoint to an advanced and robust detection engine. The process of updating the detection engine is fully managed by Cybereason and done on the detection server and not every endpoint, minimizing the need for endpoint management.

7. Enabling instant incident response

Incident investigations attempt to determine what happened at the endpoint in a thorough post-breach investigation. But why wait for a post-breach investigation? Why not collect endpoint data to begin with? At Cybereason, we continuously monitor and provide a real-time view of everything that happens. You don't have to dig through historical logs and hope evidence is still there when investigating a breach. With our real-time collection, no piece of data is ever missing. And our real-time analytics help you understand the complete picture of the attack as events unfold.

Our Incident Response Console visually presents the attack story, including the attack timeline, root cause, adversarial activity, communication and affected endpoints and users.

We leave no room for guessing: we tell you exactly what happened, when it happened and who was affected, so you can immediately plan and execute your response.

Cybereason.
Let the Hunt Begin.

Cybereason was founded in 2012 by a team of ex-military cybersecurity experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel.