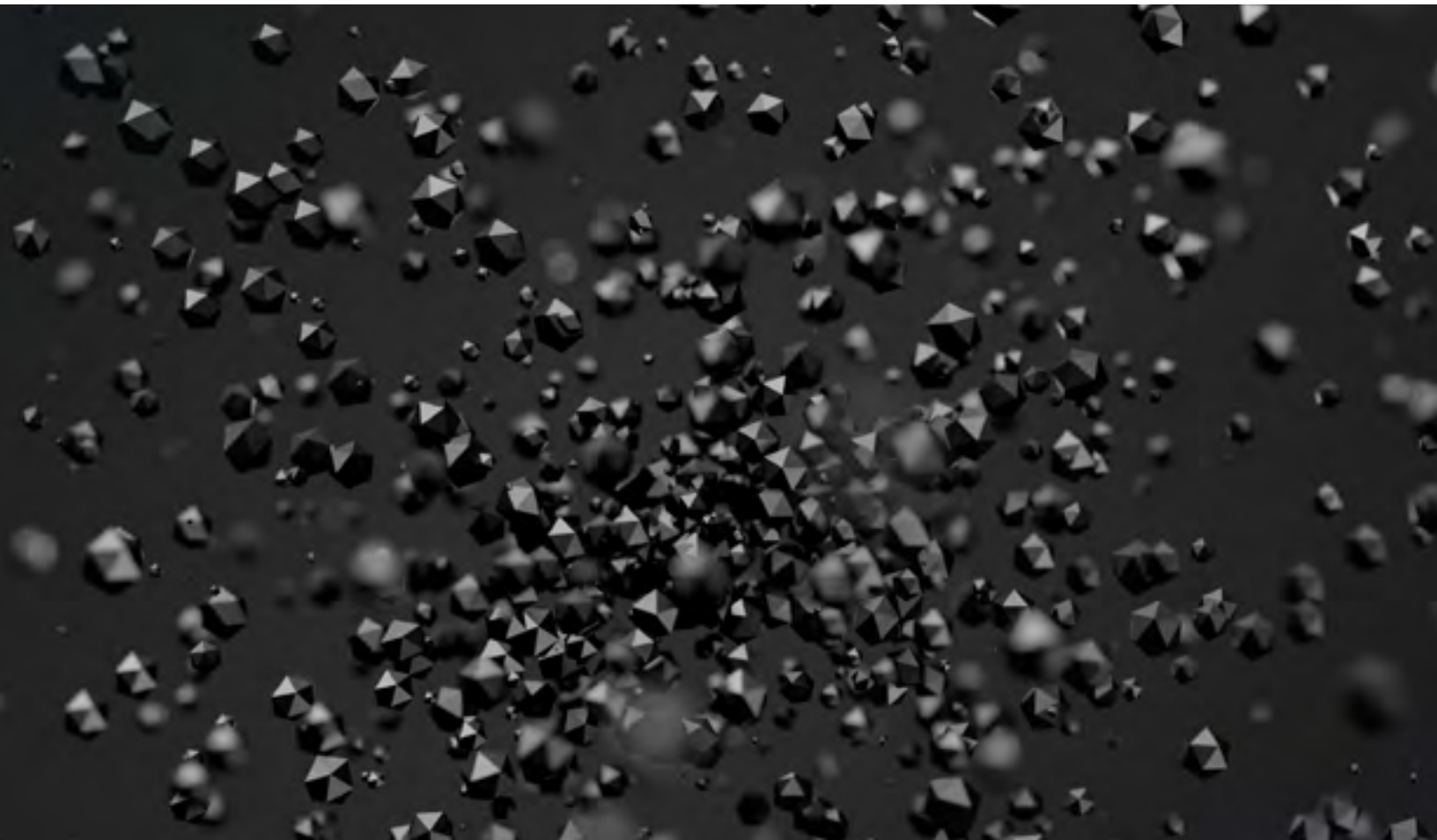




User-Space Endpoint Data Collection:

The Basis for Powerful, Unobtrusive
Detection and Response



Cybereason: Unobtrusive, effective endpoint data collection

Detecting complex cyber attacks requires vast quantities of real-time data.

Endpoints offers the most accurate information for detecting persistent, non-signature attacks. They provide critical information including process actions, file access information, network events and endpoint configuration changes.

Cybereason is the only endpoint detection and response solution based in the user space of the operating system.

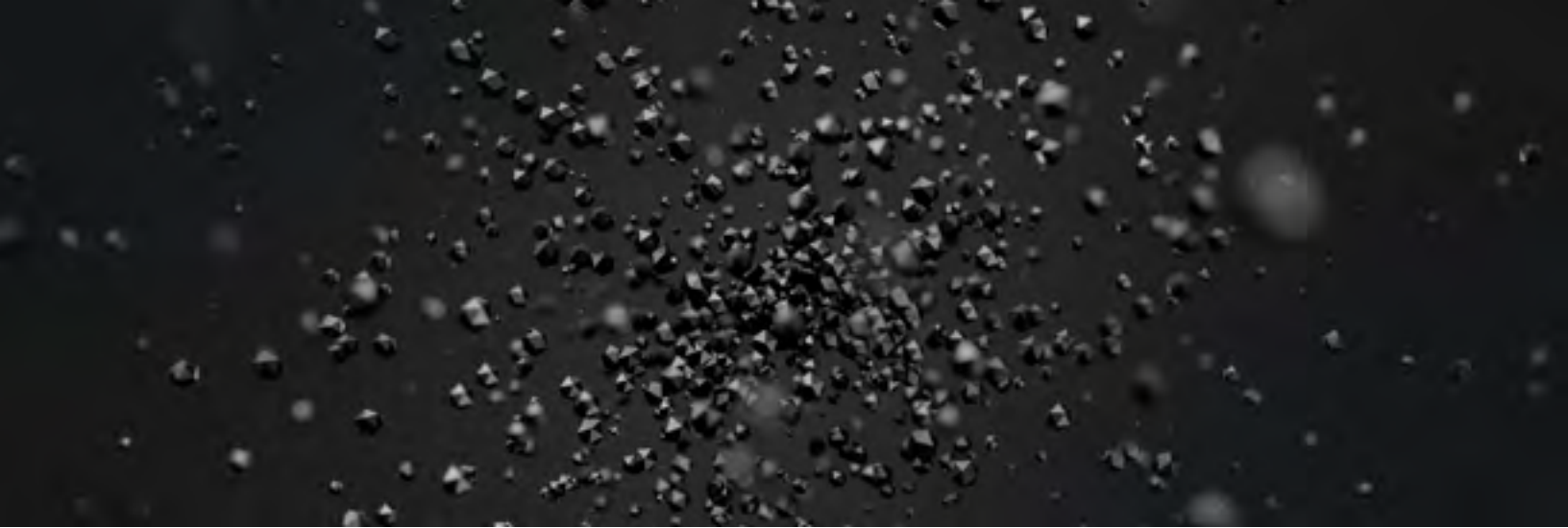
Despite the advantages of endpoint security solutions, many security professionals refrain from using them because they are notorious for crashing the operating system, adding agent management workload to the already overworked IT department and negatively impacting the user experience. Most of these issues are caused by agents running on the kernel. Those agents are difficult for IT to maintain and tend to interfere with processes running on the endpoints. At best, this causes reduced machine performance. At worst, the result is a blue screen and system crash.

Cybereason is the only endpoint detection and response solution based in the user space of the operating system. It is designed to enable high-quality, continuous data collection without interfering with the user experience.

Kernel-Level Deployment Is Less Than Ideal

When considering an endpoint solution, CISOs faces a difficult decision. They don't want to leave their endpoints completely unprotected but they're reluctant to deploy a kernel-level endpoint tool.

Kernel-level tools frustrate end users and IT departments because they disrupt the machine's operating system. Everyone has experienced it: a slow machine, a browser that doesn't respond, reduced battery life, blue screens or, even worse, a computer crash.



When broadly used, kernel-level tools may burden IT. For example, if a security tool pushes an update that crashes a computer, the updates must be uninstalled in an out-of-band process. In some cases, the updates can only be uninstalled in safe mode, which requires physical access to the machine.

Unfortunately, there's no way to build a kernel-level tool that won't interfere with machine stability and performance. Although all security vendors claim their kernel-level tools will be practically invisible to end users, implementations have shown otherwise.

Even Microsoft stumbled in this area. In an attempt to fix a security vulnerability, Microsoft released a patch for its kernel that caused BSOD crashes for everyone who applied it.

If a patch from Microsoft, which developed the operating system, can result in a crash, what would prevent a third-party security tool from bringing down a machine? This highlights a fundamental problem when working with kernel-level components: it doesn't take much to cause significant problems and interfere with the user experience.

Microsoft has a rigorous testing process and ample resources to make sure its patches don't take down computers. However, crashes still occur.

The fact is any tool that functions in the kernel can lead to a BSOD crash.

The Cybereason Approach: Do No Harm

Securing an organization without harming business operations is a common goal among the security industry. Yet most vendors have violated this principle for years by offering endpoint solutions that cause problems.

Cybereason strives to earn back the trust of end users as well as IT and security professionals. By design, the Cybereason platform was built to work alongside end users and not hinder their experience.

The combination of seamless zero-footprint collection with robust behavioral analytics gives Cybereason's platform the unique capability to detect a complete cyber attack in real time.

No Compromise on Security

IT professionals may be concerned that hackers can more easily attack user-space solutions compared to kernel-level deployments. In reality, kernel-level solutions are just as easy to exploit as any other code-based solution. Both kernel and user-space solutions can be exploited by adversaries and should have proper security measures implemented.

Cybereason's solution automatically flags any attempt to disable an endpoint sensor as malicious behavior. This allows security teams to closely monitor all future connections to and from the endpoint that was disconnected.

Frictionless Collection Without Security Compromises

Cybereason is the only endpoint security solution that runs completely in the user space, making it easy to deploy and maintain without impacting the user experience. By staying away from the operating systems' core, Cybereason ensures that business continuity won't be disrupted.

Cybereason leverages proprietary mechanisms in the user space to gain kernel-level data quality without using a kernel-level component.

Endpoint Collection Leads to Better Detection

Cybereason's unique user-level data collection component is the basis for the platform's detection and response capabilities. The endpoint components deployed across the organization's environment continuously feed [Cybereason's Malop Detection Engine](#) with a stream of real-time information including all the processes, hashes, behaviors, communications, users and authentication sessions. The Malop Detection Engine applies machine-learning and decision-making algorithms to this massive amount of data to spot malicious behaviors as they unfold.

The combination of seamless zero-footprint collection with robust behavioral analytics gives Cybereason's platform the unique capability to detect a complete cyber attack in real time.

Cybereason: Let the Hunt Begin.



cybereason

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.

© All Rights Reserved. Cybereason 2015

