cybereason | PRODUCT BRIEF

CYBEREASON PREVENTION

Move Beyond Legacy A/V With Multi-Layered Prevention

KEY BENEFITS

- Reduce the risk of unknown threats with real-time behavioral prevention
- Eliminate ransomware threats with behavioral and deception techniques
- Prevent fileless and in-memory attacks with deep script visibility
- Consolidate multiple agents into a single, lightweight agent
- Deploy effortlessly, in as little as 24 hours
- Shorten lengthy investigations with correlated threat information via an intuitive UI
- Leverage Endpoint Controls to satisfy access and compliance security needs
- Remediate at scale with a single click

How Defenders Outthink and Outpace Threats

New and sophisticated malware is detected every day, which presents huge threats to security and IT teams. With both legacy and nextgen solutions, security teams often suffer from overly complex workflows, gaps in detection, and resource-heavy agents. These factors contribute to a poor overall defense posture, high levels of fatigue, and the need for yet more tools and resources to support.

Cybereason Prevention combines signature-based, behavioral, and machine-learning approaches to end threats in real-time – including known, never-before-seen and fileless threats. Teams can deploy in a matter of hours with a single, lightweight agent for all operating systems and endpoint types. From there, investigation is easy, with full context available to analysts directly from a single UI within the platform – now less time is wasted switching between screens, and more is spent investigating threats.

Stop Any Threats in Real Time

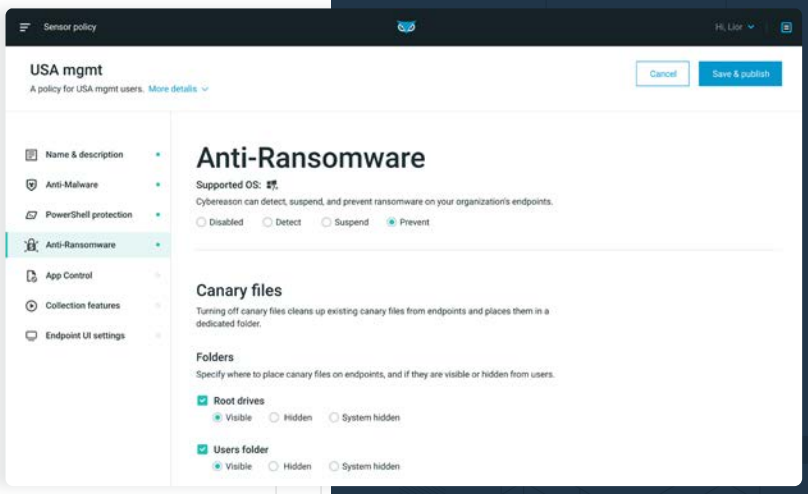
Cybereason Prevention employs a multi-layered approach through intelligence-based conviction capabilities to block known threats and machine learning algorithms that analyze behavioral and static attributes to instantly block fileless attacks, new malware variants, and other novel threats, eliminating lengthy investigations. The machine learning algorithms analyze both behavioral and static attributes of processes and files – blocking the execution of fileless attacks, new malware variants, and never-before-seen threats, instantly. Behavioral prevention of unknown threats ensures gaps in defenses are addressed.

Deep Visibility into Fileless Attacks

Modern threats require that security products have deep visibility. To enable security teams to counter the growing risks of fileless attacks, Cybereason Prevention leverages the same agent used in its Endpoint Detection and Response product in order to achieve unparalleled efficacy into malicious processes and scripts. First in the market to block malicious .Net execution, the Cybereason Defense Platform provides high fidelity detection of PowerShell scripts, .Net abuse, Macro scripts, and other challenging threats to reduce investigation workloads and time required to respond for resource-constrained security teams.

Stop Ransomware Before Harm Occurs

More and more, organizations are facing a slew of ransomware attacks. This trend represents a considerable risk. Cybereason has developed a unique combination of deception and behavioral techniques to stop ransomware before damage is done. Cybereason Prevention can automatically detect and block unknown, fileless, and even MBR-based ransomware strains. This allows teams to leverage automatic behavioral prevention, in conjunction with deception techniques, to ensure legitimate files are not encrypted during an attack.



Reduce Investigation Time with An Intuitive UI

Prevention is necessary but it is often only the first step in an attack. Understanding the root cause of an attack, and addressing it, is the real battle. With Cybereason Prevention, security teams are able to use a single interface to view, prioritize, investigate, and remediate alerts for all impacted devices. From any alert, analysts are able to go further in a few clicks, easily acquiring the context they need to take action, and eliminating the need for complex workflows between different products.

Remediate on All Devices with A Single Click

When a threat is discovered and blocked, Cybereason Prevention allows analysts to quickly take action with a myriad of remediation choices. If more than one endpoint is affected, analysts can easily remediate all affected devices quickly and easily, with a single click.

A Single, Lightweight Agent for All Functionality

Cybereason Prevention offers multi-layered prevention combining NGAV and Endpoint Controls with minimal impact on speed and resources, all without the need to deploy multiple agents. The Cybereason Defense Platform combines endpoint prevention (EPP) with our industry leading Endpoint Detection and Response (EDR) solution and proactive threat hunting to deliver comprehensive security through a single lightweight agent and intuitive user interface.

About Cybereason

Defending against today's threats requires security teams to prevent and cut the noise against known attacks, while quickly detecting and remediating advanced attacks. The Cybereason Defense Platform combines endpoint prevention, detection, and response all with one lightweight agent. Multi-layered endpoint prevention is delivered using signature and signatureless techniques to prevent known and unknown threats, and behavioral and deception techniques to prevent ransomware and fileless attacks.

CYBEREASON.COM/DEMO

Learn more at Cybereason.com →

cybereason