cybereason® | DATASHEET

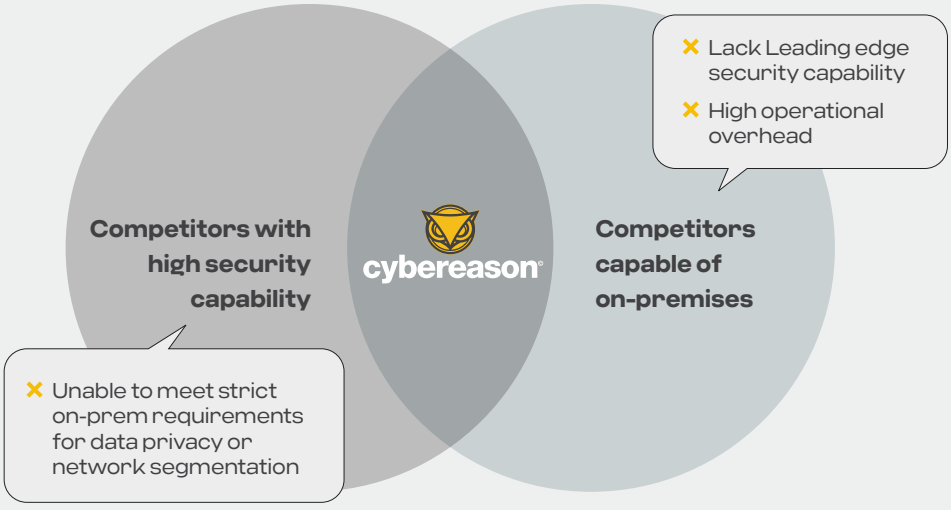
Cybereason On-Prem

STATE OF THE ART SECURITY FOR OFF-LINE ENVIRONMENTS

Leading Edge Organizations at Risk from Legacy Security

If your organization is restricted by regulations and industry standards in the use of public cloud infrastructure, then it's almost certain that your security team will be left using legacy endpoint security technologies. These technologies were created in a different age to the current advanced threat landscape, and they simply don't meet the minimum requirements of security efficacy today. Sadly, the security your organization needs to detect and respond to complex, and emerging threats typically requires public cloud infrastructure to maintain effectiveness, putting this out of reach to organizations like yours.

Cybereason's unique position in the market



- Cybereason delivers more security value than the competition
- All the benefits of EPP and EDR deployed in any configuration

Until now, the industry believed the only endpoint security technology available that worked in off-line environments was old software that was designed before public cloud and software as a service was mainstream! Worse, your current vendor rarely provides updates to their on-premises software, instead seeing this as an inconvenience to their cloud-first strategy, and so, customers are left with a technology that is essentially in 'maintenance mode'.

KEY CAPABILITIES

State of the Art Endpoint Security - For private & air-gapped environments

Don't Chase Alerts, Intercept MalOps - Fully contextualized and correlated attack stories

Identify and End Attacks Faster - Improve detection and response times by 93%.

Remediate in Minutes, Not Hours - Save time on every investigation with guided remediation

State of the Art and On-Premises!

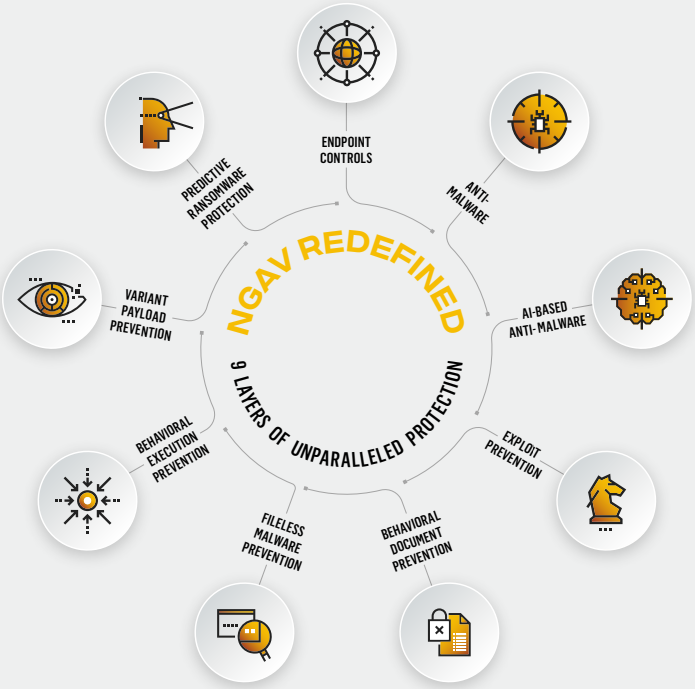
At Cybereason, we hear you! - Ironically, the reason your security team is still using legacy endpoint security is because they are protecting critical and sensitive networks, which in turn, require clear data boundaries, and segmentation. Cybereason believes all Defenders are equal, and no-one should be left behind! That is why at Cybereason we provide high assurance customers with Cybereason On-Prem that includes Endpoint NGAV & EDR solutions. Our customers choose us not only because they can get the latest technologies to fight against the latest and most dangerous threats for their on-premises and air-gapped environments, but that it is market leading too!

Business Value

- Significantly reduce the risk of business disruption in critical off-line and private networks from ransomware and other targeted attacks through more effective, state of the art prevention, detection and response security capabilities with fewer false positives.
- Improve security operations efficiency and reduce triage, investigation and remediation times through process automation and AI-driven analytics.
- Bridge the security skills gap and empower analysts of all skill levels to quickly dig into the details of an attack without crafting complicated queries, then easily pivot directly from investigating to remediating affected devices with a single click.
- Simplified data and critical infrastructure compliance through 100% off-line deployment support, meaning all data remains on site, with no external access required that would otherwise open critical networks up to vulnerabilities.
- Reduced deployment risk and faster time to value and visibility, through a simplified deployment process.
- Integration with existing tools in your infrastructure to centralize monitoring, investigation and triage

Redefined Next Gen Antivirus (NGAV) with 9 Layers of Unparalleled Attack Protection

Cybereason is the only security vendor that brings a unique approach of multi-layered NGAV defense where each layer is purpose-built to prevent unique attacker techniques. When these 9 independent, yet complimentary, layers are combined, unparalleled attack protection is achieved, ensuring that your business achieves your goals, and bad actors don't.



1. **Endpoint Controls** - Block unauthorized USBs, network connections, and ensure full disk encryption - Decrease the attack surface by limiting the use of USB storage devices & mobile phones, configure firewall policies, and ensure full disk encryption.

2. **Anti-Malware** - Block commoditized malware - Threat intelligence and heuristics-based anti-malware ensure fundamental protection against known malware.

3. **AI-Based Anti-Malware** - Block novel malware - Artificial Intelligence evaluates behavior occurring across the enterprise as a whole to stop actors in their tracks, even when they're using never before seen malware.

4. **Exploit Prevention** - Virtual Patching for Windows Vulnerabilities - Block exploit attempts on the endpoint, using mitigation techniques to block exploits before they can be carried out, even when it originates from zero-day vulnerabilities.

5. **Behavioral Document Prevention** - Block malicious Macros - Analyzes documents when they are accessed to ensure no malicious code, such as macros, embedded in documents can load.

6. **Fileless Malware Prevention** - Block in-memory command line and script-based attacks - Examining the behavior of the Powershell engine, .Net, JScript, and VBScript ensures that attackers are not able to slip by defenses by loading malicious code into memory.

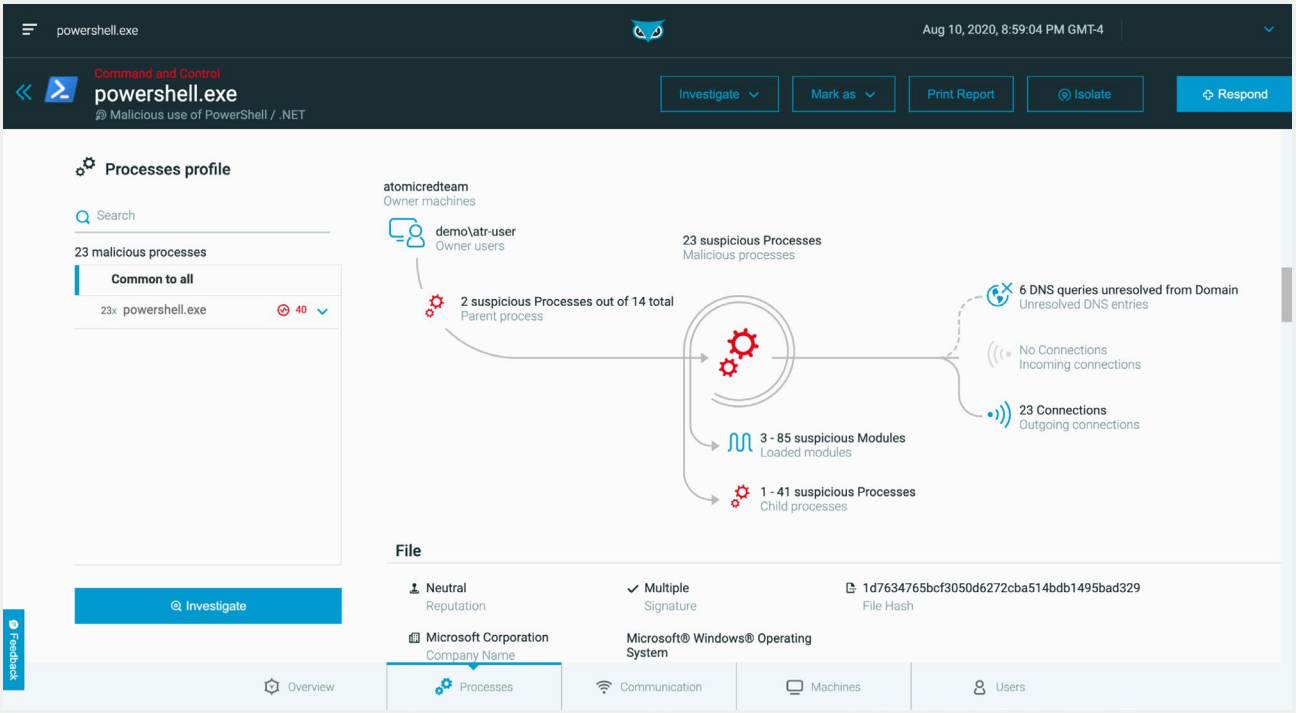
7. **Behavioral Execution Prevention** - Block living off-the-land techniques - Leveraging intelligence gathered from activity seen across Cybereason's EDR customer base, detections are moved forward in the kill chain to prevent LOLBins based attacks, where the attacker abuses legitimate systems services that are normally benign to perform malicious actions.

8. **Variant Payload Prevention** - Vaccinate against variations of malicious payloads, like Cobalt Strike, and Emotet - Monitors the code being loaded into memory and uses Binary Similarity Analysis (BSA) technology and near-match analysis to identify and block obfuscated code that exhibits characteristics of a known malicious payload such as a Cobalt Strike Beacon or Metasploit Meterpreter.

9. **Predictive Ransomware Protection** - Block encryption and restore files - Although the previous prevention layers block almost all ransomware activity, this final layer of protection ensures the most sophisticated ransomware behavior is identified and prevented from inflicting damage. In the unlikely event it's necessary, Rapid Restore rolls back specific encrypted files to their previously uncorrupted state. Cybereason PRP is leveraging Cybereason's proprietary and patented technology to identify, prevent, and recover from Ransomware behavior in real-time.

AI-Driven On-Prem Endpoint Detection & Response (EDR) to Predict, Understand, and End Malicious Operations

Cybereason On-Prem EDR moves beyond endless alerting to instead recognize, expose, and end malicious operations before they take hold. Using one agent, one console, and one team to defend all endpoints including air-gapped environments, AI-driven Cybereason On-Prem was designed to expose and intercept every MalOp (malicious operation).



A MalOp is not an alert, but a contextualized view of the full narrative of an attack. Only Cybereason provides the actionable intelligence to out-think the adversary, the remediation speed to outpace their operations, and the insights to end any attack.

The Visibility to Out-think - Track, visualize, and end malicious operations with the full attack story from root cause across every affected endpoint, device, user identity, application and cloud deployment.

The Speed to Outpace - Analyze, adapt, and move faster than attackers, eliminating emerging threats in minutes rather than days. Whether a commodity attack or targeted threat, you'll understand the attack and remediate with confidence.

The Precision to End Attacks - Leverage automated and single-click remediation across the entire ecosystem to end attacks and dramatically reduce the need for lengthy analyst investigations.

Deployment Requirements for Cybereason On-Prem

The Cybereason On-Prem server installation supports VMware vSphere ESXi version 6.5 or above, providing a more flexible choice of deployment options for either On-prem, private clouds and local data centers.
For support of other platforms including AHV Nutanix, please contact sales@cybereason.com

PREFERRED OPERATING SYSTEMS FOR VERSION 23.1 OF THE CYBEREASON ON-PREM ENDPOINT SENSOR

WINDOWS	MAC	LINUX
Windows XP*	Yosemite (10.10)*	Amazon Linux (All versions before 2017)*
Windows Vista*	El Capitan (10.11)*	CentOS 6, 7, 8
Windows 7 SP1	macOS Sierra (10.12)	RedHat Enterprise Linux 6, 7, 8
Windows 8	macOS High Sierra (10.13)	Oracle Linux 6, 7, 8
Windows 8.1	macOS Mojave (10.14)	Debian 8, 9, 10
Windows 10	macOS Catalina (10.15)	Amazon Linux AMI 2017.03
Windows 11, 21, H2	macOS BigSur 11	Amazon Linux 2
Windows Server 2003*	macOS Monterey 12	Ubuntu 14 LTS, 16 LTS, 18.04 LTS
Windows Server 2008*		Ubuntu 20.04 LTS, 20.10
Windows Server 2019		
Windows Server 2016		
Windows Server 2012 R2		
Windows Server 2012		
Windows Server 2008 R2 SP1		
Windows Server 2022		

*Correct at time of production (January 2024), please contact sales@cybereason.com for more information on support for legacy Operating Systems

ABOUT CYBEREASON

Cybereason is the leader in future-ready attack protection, partnering with Defenders to end attacks at the endpoint, in the cloud, and across the entire enterprise ecosystem. Only the AI-driven Cybereason Defense Platform provides predictive prevention, detection, and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 50 countries.