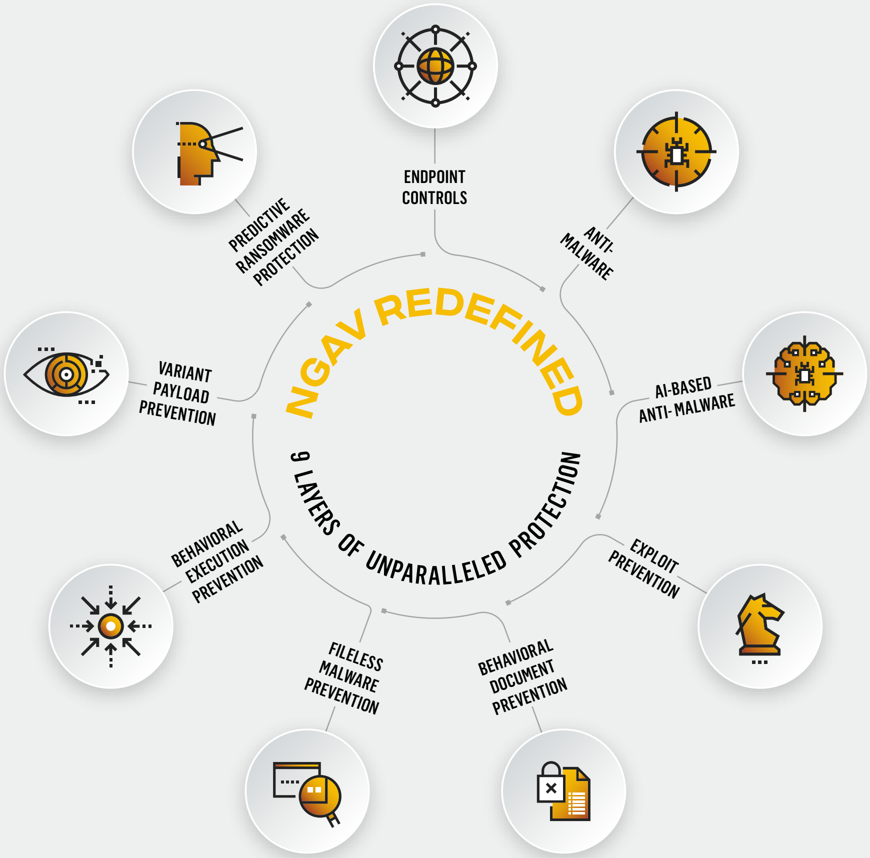
cybereason® | PRODUCT BRIEF

Next-Generation Antivirus (NGAV)

9 LAYERS OF UNPARALLELED ATTACK PROTECTION

NGAV Redefined

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.


ENDPOINT CONTROLS
ANTI-MALWARE
AI-BASED ANTI-MALWARE
EXPLOIT PREVENTION
BEHAVIORAL DOCUMENT PREVENTION
FILELESS MALWARE PREVENTION
BEHAVIORAL EXECUTION PREVENTION
VARIANT PAYLOAD PREVENTION
PREDICTIVE RANSOMWARE PROTECTION
NGAV REDEFINED
9 LAYERS OF UNPARALLELED PROTECTION

PROACTIVELY END ATTACKS EARLIER IN THE KILL CHAIN

Cyber criminals are leveraging novel and creative ways to exploit vulnerabilities in an organization's defenses. That is why Cybereason uses 9 layers of uniquely designed technologies to block malicious activity in the earliest stage of an attack. Cybereason's unique multi-layered AI-powered approach ends attacks pre-execution, on-execution, and post-execution ensuring that defenders always win. Robust forward defenses mean less malicious activity in the environment requiring later investigation and response, giving your team back precious time.

STOP ANY FORM OF RANSOMWARE, EVEN THOSE NEVER BEFORE SEEN

With ransomware attacks growing more sophisticated by the day, it can feel like it's only a matter of time before they come for you. With multi-layered protection, AI-powered endpoints, protection from the kernel to the cloud, and the only Predictive Ransomware Protection available, a ransomware attack won't feel inevitable. You'll feel invincible. Cybereason is the only vendor that can confidently say together with our customers we are undefeated in the fight against ransomware.

NATION-STATE LEVEL SECURITY DESIGNED FOR EVERYDAY USE

Historically, highly advanced tools have required legions of staff and bottomless IT budgets, while streamlined tools have been simplistic and ineffective. With a single agent, Cybereason NGAV provides nation-state level prevention that amplifies your existing teams and resources. Stopping more attacks before they start improves the efficiency of your SOC, leaving them fewer events to investigate. While ease of use and streamlined deployment drastically reduces management overhead.

9 LAYERS OF UNPARALLELED ATTACK PROTECTION

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.

PROVEN PROTECTION - CYBEREASON ACHIEVES THE BEST RESULTS IN MITRE HISTORY

In the 2022 Enterprise Evaluation MITRE tested the abilities of 30 vendors to stand up against the pervasive ransomware gangs Wizard Spider + Sandworm.

Cybereason's 9 layers of unparalleled attack protection produced the highest scores in the history of the MITRE ATT&CK® Evaluations, by achieving:
100% Prevention:
Cybereason detected and prevented 100% of the 9 attack sequences for both Windows and Linux

Cybereason also demonstrated 100% Visibility, 100% Real-Time Detections, and an industry best of 99% Analytic Coverage in the MITRE evaluation.

Experience NGAV Redefined:
Cybereason.com/platform/endpointprevention

ABOUT CYBEREASON

Cybereason is the champion for today's cyber defenders with future-ready attack protection that extends from the endpoint, to the enterprise, to everywhere. The Cybereason Defense Platform combines the industry's top rated detection and response (EDR and XDR), next-gen anti-virus (NGAV) and proactive threat hunting to deliver context-rich analysis of every element of a malicious operation (Malop). The result: defenders can end cyber attacks from endpoints to everywhere.