cybereason | DATASHEET

Predictive Ransomware Protection

Undefeated in the fight against ransomware

Cybereason is undefeated in the fight against ransomware: With multiple layers of behavioral-based prevention, Cybereason stops any ransomware strain - even those never before seen.

Ransomware attacks have gone mainstream in recent years, and are clearly a preferred method of attack for cyber operators. Ransomware outbreaks are proving to be a profitable use of time for adversaries, with the potential ransom demand now reaching well into the millions of dollars - signifying a new and unwelcome risk to security and business leaders. Ransomware attacks will continue, making a ransomware defense strategy essential to success.

From large enterprises to small businesses, government organizations, and nonprofits, any organization with weakened or exposed defenses could find itself an enticing target. To end these ransomware attacks, cyber defenses must become just as pervasive as the attackers.

DOESN'T PAY TO PAY

50%

of those who paid a ransom experienced another attack

16 DAYS

Ransomware attacks on average result in 16 business days of system downtime

$70 MILLION

The largest ransomware payment demand recorded to date was $70

CYBEREASON DELIVERS PREDICTIVE PROTECTION IN THE FIGHT AGAINST RANSOMWARE

- **Artificially intelligent endpoints:** Only Cybereason predicts and blocks ransomware activity using artificial intelligence on every endpoint, unlike competitive solutions that assume defeat and rely only on unreliable "rollbacks."
- **Multi-layered Protection:** Cybereason protection leads with the industry's only predictive protection that ends ransomware based on even the most subtle behaviors and attacker activity - BEFORE encryption takes place. This combined with our award-winning NGAV, AV, script based, and file based protection ensures that both known and never before seen ransomware never gets through.
- **Visibility from the kernel to the cloud:** Sophisticated attackers know how to evade standard means of detection. Cybereason provides unobstructed access to the full array of data involved in a ransomware attack, and then contextualizes the operation for rapid decision-making. This enables Defenders to broaden the reach of investigations, clearly see the complete picture of the full attack surface, and root out ransomware operations.

Predictive protection means that Cybereason ends ransomware with a high degree of confidence based on subtle behaviors and attacker activity. We see what others miss and infer the adversaries next move without manual input from Defenders.

Predictive protection equates to more productivity for Defenders out of their solutions. They don't have to manually block, investigate or respond due to the high-level of automated protection delivered by Cybereason.

BENEFITS

Transition your security posture to a future-ready state that will prevent expensive ransomware attacks.

DEFEAT RANSOMWARE

Don't rely on vulnerable data backups to recover from a ransomware attack - simply stop it in the first place.

Independently validated technology that stands ahead of the rest in industry-standard testing, like MITRE ATT&CK, delivers tangible results that you can rely on.

Proven ransomware protection has stopped sophisticated adversaries and modern ransomware such as DarkSide and REvil.

COMPLEMENT YOUR EXISTING SECURITY STACK

Operate with and alongside existing products in your security stack for integration and automation.

Streamline operations with a simple UI and intuitive workflows.

Consolidate capabilities at the endpoint with a single lightweight sensor that uses less than 5% CPU.

ACHIEVE IMMEDIATE TIME TO VALUE

Simple, rapid deployment delivers instant protection and near-immediate time to value.

With a less than 1% false positive rate, organizations gain full ransomware protection without additional work added for administrators.

CYBEREASON
PREDICTIVE PROTECTION CAPABILITIES

BINARY SIMILARITY ANALYSIS

Block obfuscated ransomware through near-match analysis and "fuzzy" matching.

NATURAL LANGUAGE FILE ANALYSIS

Prevent at the first sign of encryption by monitoring structural changes in files that indicate encryption. Rollback and restore encrypted files automatically and without manual input to their previously uncorrupted state.

SIGNATURE BASED ANALYSIS

Detect and prevent known variants of ransomware using static signatures enriched with threat intelligence via an infinitely expanding database of threat information. This cache of threat data contextualizes attacks without the need to research off-platform, providing clear details on what took place and how to respond and recover.

BEHAVIOR BASED EXECUTION PREVENTION

End ransomware operations before they begin with machine learning based blocking of both known and unknown strains of ransomware. Behavior-based protection goes beyond signatures to include blocking of malicious behaviors specific to never-before-seen ransomware.

FILELESS PROTECTION

Sophisticated attackers are likely to use advanced tactics to infiltrate an environment while attempting to hide their behavior. Fileless Protection discovers and blocks memory-based attacks or other fileless techniques based on the activity the systems exhibit.

BEHAVIORAL DOCUMENT PROTECTION

Detect malicious macros and corrupted files that are common hiding places for ransomware. Cybereason identifies and stops malicious behaviors resulting from nefarious macros in Excel sheets or other documents—regardless of if a signature exists for these malicious files.

RESEARCH-DRIVEN INSIGHTS: NOCTURNUS RESEARCH

As ransomware strains evolve, Cybereason's Nocturnus security research team exposes new malware and dives deep into the research for community information sharing. Insights are passed directly to customers through product updates that protect against the newest strains of malware.

Learn more **here**

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.