cybereason

9 LAYERS OF
UNPARALLELED
ATTACK PROTECTION

# NGAV Redefined

# Introduction

## Welcome to Cybereason's Next Generation Anti-Virus Redefined online ebook.

Traditional antivirus tools from legacy vendors often spot the easy stuff but struggle to prevent novel threats from causing damage. That is why Cybereason has dramatically redefined the latest NGAV prevention technologies to identify and stop threats, from the simplest to novel threats never seen before.

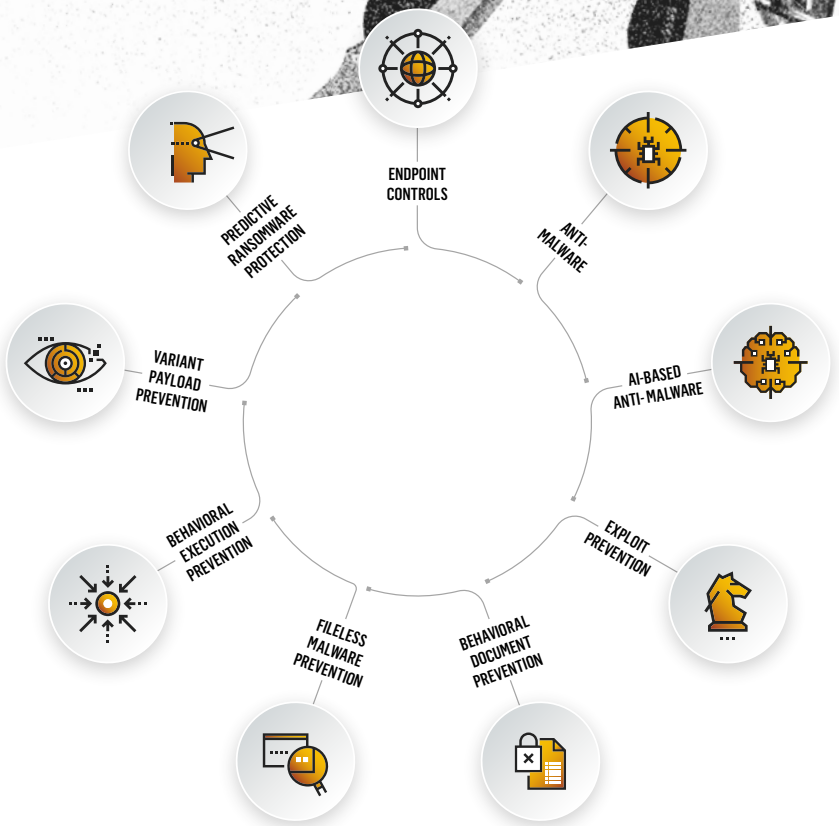
Cybereason is the only security vendor that delivers multi-layered NGAV prevention, where each layer is purpose-built to prevent unique attacker techniques. Cybereason provides unparalleled attack protection by combining **9 independent yet complimentary prevention layers** ensuring that your business achieves its goals and bad actors don't.

Explore how Cybereason uses each of the 9 layers of uniquely designed technologies to block malicious activity in the earliest stages of an attack.

Cybereason is the only security vendor that delivers multi-layered NGAV prevention, where each layer is purpose-built to prevent unique attacker techniques.

# Contents





# Endpoint Controls

Decrease the attack surface by blocking unauthorized USBs and network connections and ensure full disk encryption to keep your assets secure

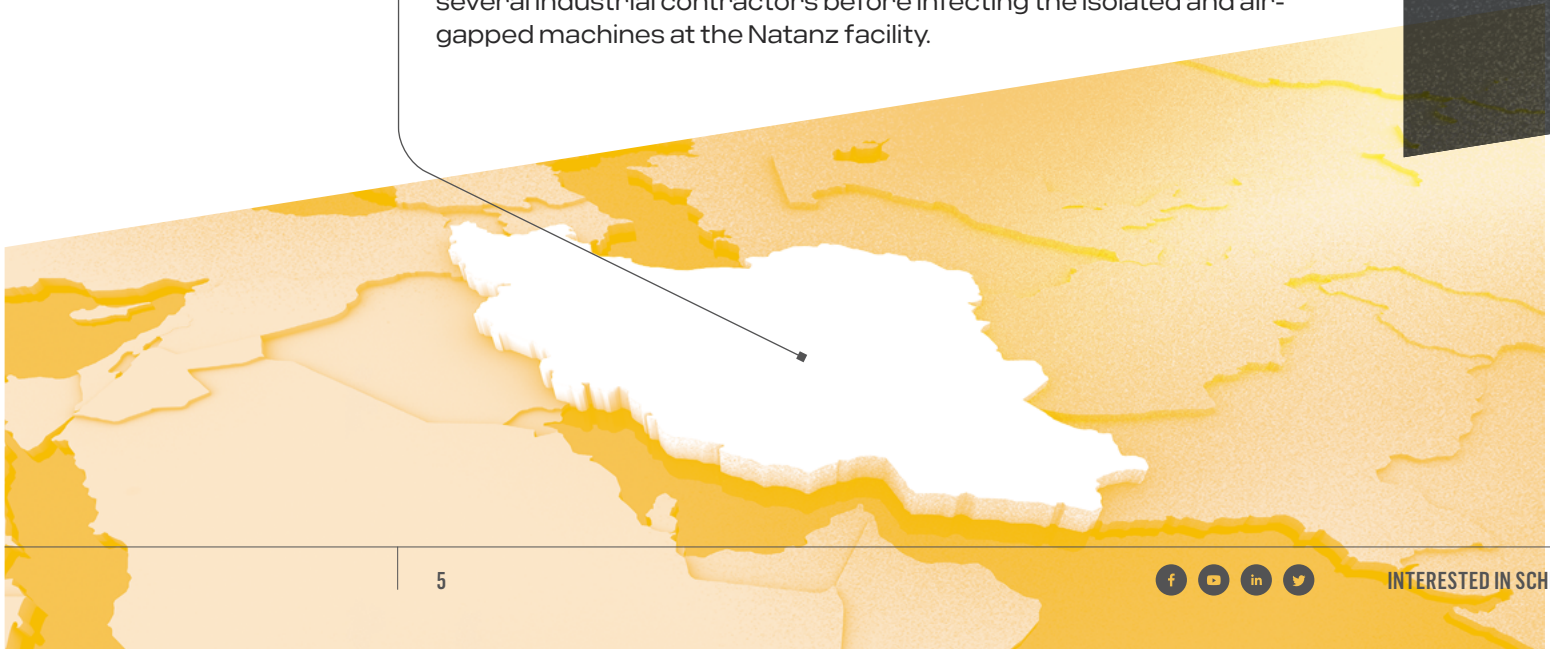
# ENDPOINT CONTROLS IN THE REAL WORLD

USB devices and externally connected devices can pose a significant risk to organizations. Stuxnet - an attack on Iranian nuclear facilities in 2010 - is one of the most famous USB-based attacks in history.

In 2009 the Iranian government built a highly protected and secretive nuclear fuel enrichment facility in Natanz, Iran, more than 165ft underground. Designed to be protected from bunker-busting bombs and cyber attacks, it was a highly secure facility. Over the course of 2009-10, many centrifuges at this facility used to enrich uranium (part of the process to create fuel required to generate nuclear power or nuclear weaponry) began failing at an unusually high rate.

Enter Stuxnet, the world's first digital weapon. The virus was transferred via a USB drive from one device to another across several industrial contractors before infecting the isolated and air-gapped machines at the Natanz facility.

Stuxnet - an attack on Iranian nuclear facilities in 2010 - is one of the most famous USB-based attacks in history.



Unlike previous malware, this one didn't simply impact the device it was on, but it affected electronics on other machines and physical equipment in the facility. The targets were German-built Siemens computer systems that regulated the speed of nuclear centrifuges, which were used to enrich and create nuclear fuel. While many details about the attack remain elusive, the impact was clear. The Stuxnet attack damaged more than 2,000 centrifuges and greatly slowed the ability to produce enriched uranium, setting back the Iranian nuclear program by up to 2 years.

Prevention technology like endpoint controls would have negated the impact of Stuxnet by blocking the use of unauthorized USB devices, stopping the spread of the virus. This case may seem unique, but it is a prime example of a vulnerability like poor device control protection that increases the risks posed by malicious actors who are persistent and willing to conduct unique and innovative attacks. Let's explore how it works.

Endpoint Controls allow a security practitioner to set policies and configurations to restrict the use of external storage devices

## HOW DO ENDPOINT CONTROLS WORK?

Endpoint Controls allow a security practitioner to set policies and configurations to restrict the use of external storage devices that might be used to infect endpoint machines with malicious files or to exfiltrate sensitive data. It also provides for personal firewall control, meaning the ability to reduce network communication risks by restricting incoming and outgoing connections.

Finally, it audits full disk encryption identifying endpoints that have not implemented full disk encryption and are vulnerable to data compromise. Combining each capability limits your attack surface from attackers leveraging storage devices, network vectors, and data theft.

NOW THAT WE'VE DISCUSSED HOW ENDPOINT SECURITY IS THE STARTING POINT IN IDEAL PREVENTION, LET'S LOOK AT THE NEXT LOGICAL STEP IN DEFENDING FORWARD, SIGNATURE-BASED ANTI-MALWARE.

# Anti-Malware

Comparing a file's signature with an updated list of known malware signatures is the basis of standard antivirus protection and the Cybereason NGAV Anti-Malware service. The Cybereason Defense Platform uses signature-based analysis to scan files on access and to prevent access and execution if a file is malicious.

# ANTI-MALWARE IN THE REAL WORLD

On May 1, 2004, malware variants known as Sasser and Sasser.B began infecting hundreds of thousands of systems worldwide. It specifically targeted Windows XP and Windows 2000 operating systems by leveraging shellcode that exploited a buffer overflow vulnerability in the Local Security Authority Subsystem Service (LSASS), which controls all aspects of security for Windows machines.

The remote shell launched on port 9996, and the malware checked various IP addresses before connecting to victims' computers via TCP port 445. It then created and ran a script file titled cmd.FTP on the target computer, causing the target machine to download Sasser from the infecting computer's malware-created FTP server. The malware was saved in the system directory as AVSERVE.EXE and AVSERVE2.EXE. The downloaded program was named _up.exe, followed by four or five random integers.

Within 24 hours, Sasser probed 200,000 computers per hour. Microsoft decided to launch a broad outreach campaign that lasted the entire week, including conducting a Webcast, posting information on the company's Web site, creating retail flyers and content for PC makers and key partners, and even paying Google to ensure that anyone who searched for information about the worm would see an ad that pointed to Microsoft.com for the patch and other downloads.

Within 24 hours, Sasser probed **200,000 computers** per hour

Cybereason NGAV Anti-Malware signatures analysis service scans files using advanced detection logic

Despite all of these efforts, Microsoft struggled to contain Sasser. Reports of the malware's impact spread quickly: Operations were disrupted at companies like Goldman Sachs and British Airways. Computers in half of Taiwan's post offices were infected. Sasser plagued PCs at government agencies in Hong Kong and on oil platforms off the coast of Mexico.

It took Microsoft 188 days from the time of the malware's discovery to issue a patch for the LSASS vulnerability. The magnitude of Sasser's disruption is staggering: 5,000 computer systems and associated X-ray equipment at a hospital in Lund, Sweden, stop responding; 1,200 PCs at the European Commission headquarters in Brussels cannot get online, and Sun Trust bank and American Express in the United States lose Internet connectivity for several hours.

# HOW DOES ANTI-MALWARE WORK?

By default, Cybereason NGAV scans files with extension types that can be executed, loaded, or run because these files could contain malware or malicious content. For example, scanned files include files that have **.exe**, **.dll**, and **.docx** extensions.

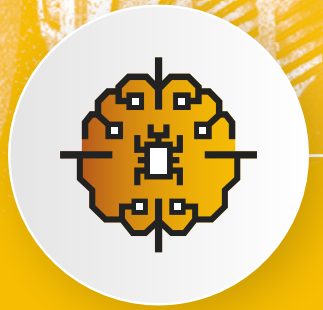
Cybereason NGAV Anti-Malware signatures analysis service scans files using advanced detection logic. The service also inspects the file to determine the file's reputation and to search for malicious content embedded in the file, such as a module or script.

Cybereason NGAV treats removable media such as USB and external hard drives as local drives and includes these removable media as part of scans. During scheduled scans, Cybereason scans any files inside the USB drive. During an on-access scan, files inside the USB drive are scanned once a user attempts to open a file or directory.

If you enable **Anti-Malware > Signatures mode**, sensors receive signature database updates every 15 minutes from the NGAV Global update server, ensuring that the database remains current and helping the sensors detect and prevent known malware with very high accuracy. The sensor downloads 1.5 MB of Signature database updates per day.

NOW THAT WE'VE DISCUSSED SIGNATURE-BASED ANTI-MALWARE PREVENTION LET'S LOOK AT THE NEXT LOGICAL STEP IN DEFENDING FORWARD:

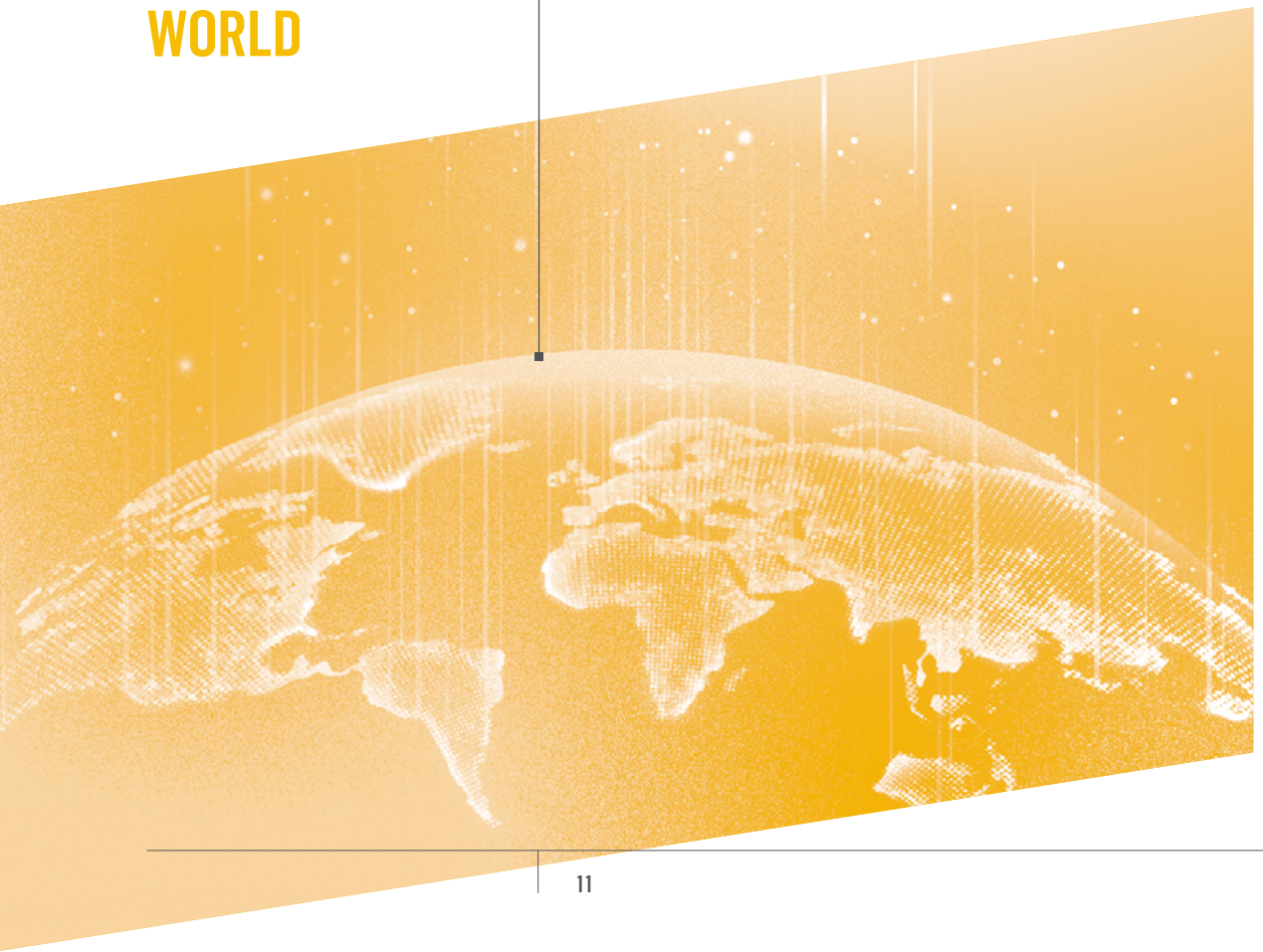
# AI-Based Anti-Malware



Decrease the attack surface by blocking unauthorized USBs and network connections and ensuring full disk encryption to keep your assets secure.

# AI-BASED ANTI-MALWARE IN THE REAL WORLD

Malware continues to become more complex and requires advanced AI-based Anti-Malware prevention. A case in point is Operation CuckooBees, a multi-year cyber espionage campaign waged by the Chinese state-sponsored APT group Winnti.

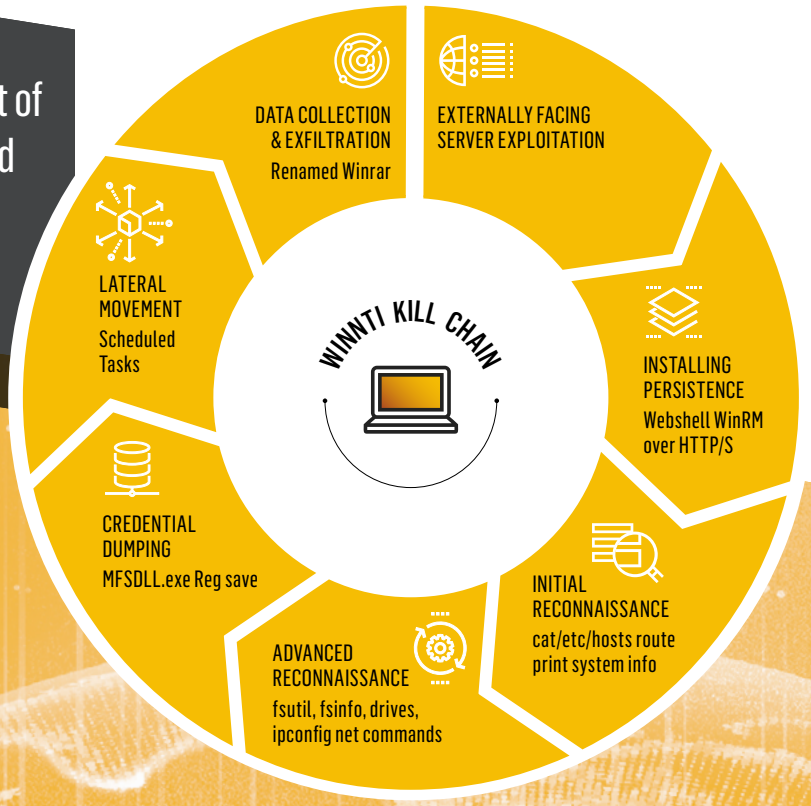


In 2021, the Cybereason Nocturnus Incident Response Team investigated multiple intrusions targeting manufacturing and technology companies across North America, Europe, and Asia. They found a sophisticated and elusive cyber espionage campaign operating undetected for more than two years. Operation CuckooBees, as it became known, conducted reconnaissance and identified valuable data to steal from its victims. The Winnti APT group sought sensitive documents, blueprints, diagrams, formulas, and manufacturing data, all designed to give the Chinese government and industries an unfair technological advantage rather than spending time and resources on traditional R&D. In addition, the attackers collected information that could be used for future cyberattacks, targeting a company's business units, network architecture, user accounts and credentials, employee emails, and customer data. The impact was significant, as they made off with hundreds of gigabytes of sensitive data.

Operation CuckooBees was successful because several layers of sophisticated and hard-to-detect malware led to deploying the WINNKIT rootkit composed of multiple interdependent components. This "house of cards" approach meant that every stage of the attack depended on the other layers to function properly to be successful, thus making it harder to analyze and identify each component separately.

Here is a quick highlight of the malware arsenal and methods employed:

Unlike signature-based analysis, prevention technology like AI-Based Anti-Malware is designed to detect malware like those used in Operation CuckooBees. The catch is malicious files have common characteristics, and Cybereason's advanced machine-learning models can map and detect these characteristics.




## HOW DOES AI-BASED ANTI-MALWARE WORK?

AI-Based Anti-Malware can compare a file's contents and metadata with existing models of malicious actions. Based on the analysis of the files, the Cybereason Defense Platform determines the likelihood that the file is malicious across the entire enterprise. This means Cybereason NGAV customers have broad protection against complex attacks like .NET-based malware attacks and Windows Management Instrumentation (WMI) attacks.

NOW THAT WE'VE DISCUSSED HOW AI-BASED ANTI-MALWARE PREVENTION BLOCKS UNKNOWN THREATS LET'S LOOK AT THE NEXT LOGICAL STEP IN DEFENDING FORWARD:

# Exploit Prevention

A computer exploit is a piece of software code that takes advantage of a vulnerability or bug for malicious use. For example, in a drive-by download, a user clicks a link in an email and is redirected to a malicious website, which takes advantage of browser vulnerabilities to load malware onto the user's computer.

Exploit Prevention uses known attack patterns and techniques to block exploits before the exploit can be carried out

Software such as operating systems, browsers, Microsoft Office, and third-party applications are vulnerable and often exposed to potential attacks.

Security teams and IT professionals can use the Cybereason NGAV Exploit Prevention feature to block exploit attempts on the organization's endpoints. Cybereason NGAV uses various security mitigation techniques to prevent attackers from successfully exploiting software vulnerabilities. Although it is impossible to patch an unknown or zero-day vulnerability, Exploit Prevention uses known attack patterns and techniques to block exploits before the exploit can be carried out, even when it originates from a zero-day vulnerability.

Exploit Prevention ensures that your organization is protected against vulnerabilities without waiting for additional detection rules or signature updates.

## EXPLOIT PREVENTION IN THE REAL WORLD

In January 2020, a security researcher reported the existence of a zero-day exploit nicknamed DogWalk, which arrived via a phishing email and downloaded malicious executables to the Windows Startup folder. At the time, Microsoft refused to issue an advisory or patch because it had determined it was not a security issue.

Dogwalk leveraged a path traversal weakness in the Windows Support Diagnostic Tool (MSDT) that attackers could exploit to conduct remote code execution on compromised systems. Once a target clicked on a link in a phishing email or on a web site controlled by the attackers, a malicious executable (.diagcab file) was added to the Windows Startup folder. The planted executables would then automatically run the next time the Windows machine was restarted and would begin downloading additional malware payloads.

Although all files downloaded and received via email include a Mark-of-the-Web (MOTW) tag used to determine their origin and trigger an appropriate security response, researchers noted that the MSDT application is not designed to check this flag, allowing the .diagcab file to be opened without warning.

Dogwalk remained in the wild for the next two years until Microsoft was forced to acknowledge the security vulnerabilities and issue a patch. By August 2022, Dogwalk was being tracked as CVE-2022-34713.

Cybereason NGAV Exploit Prevention includes several mitigation technologies that disrupt common exploit techniques

## HOW DOES EXPLOIT PREVENTION WORK?

Cybereason NGAV Exploit Prevention includes several mitigation technologies that disrupt common exploit techniques. These mitigations apply on the system level and the program level:

- System-level mitigations refer to security settings that apply to all applications or processes on the operating system.
- Program-level mitigations refer to security settings that apply to specific processes or programs and override the system mitigation for that program if one exists. For example, the system-level "Force randomization for images (Mandatory ASLR)" mitigation might be set to **OFF** for all programs, but the program mitigation might be set to **ON** specifically for Adobe Acrobat.

Cybereason identifies the combination of techniques to apply to different operating system features and processes to prevent exploit attacks efficiently. You can choose between the default configuration that uses standard security baselines or a more aggressive protection option that uses the Cybereason security baselines.

# Behavioral Document Protection



Identifying and preventing malicious macros is critical to stopping attackers from abusing legitimate documents and files to harm victims.

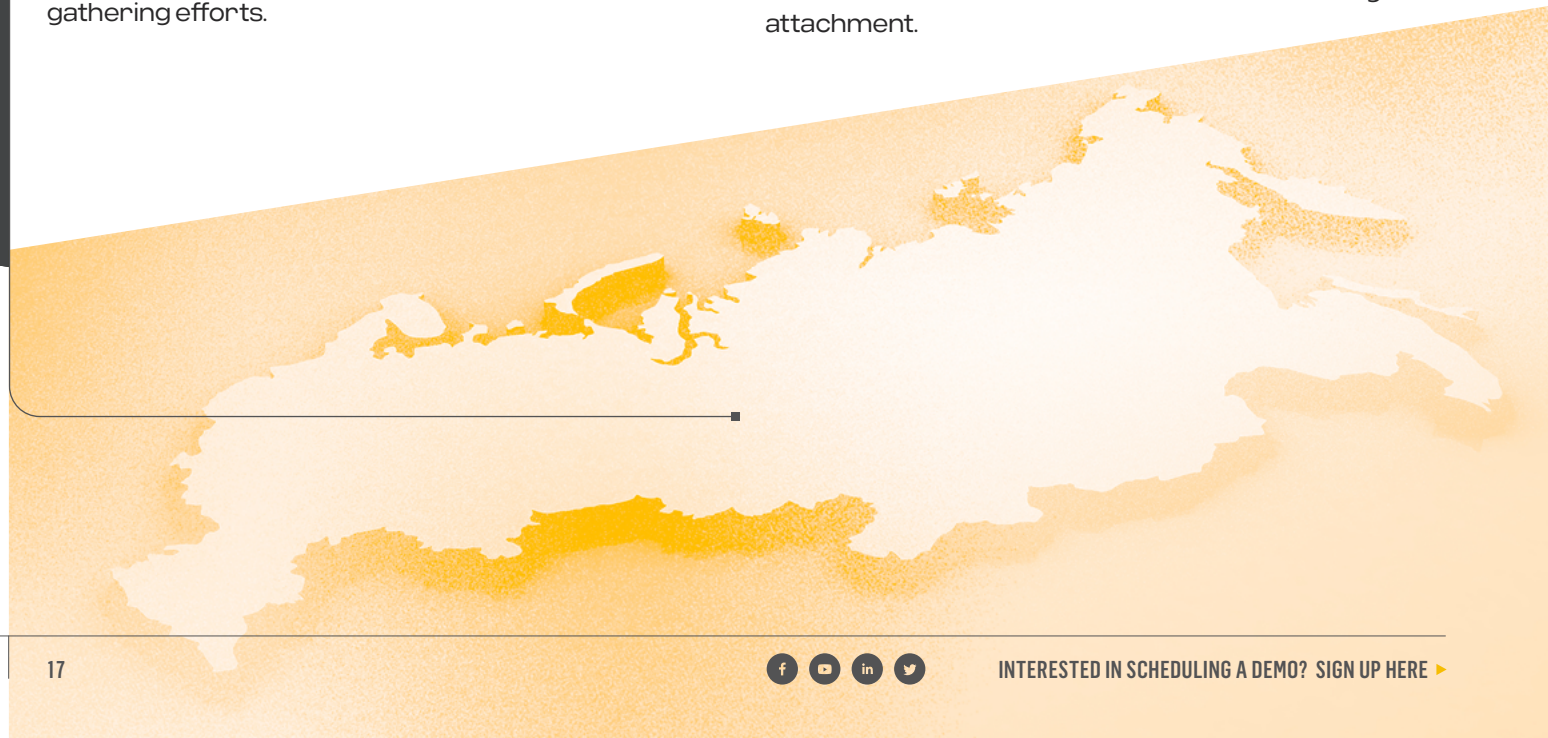
Trusted files, most notably documents (Word Files & Excel Documents), **can easily be overlooked** as a potential threat

# BEHAVIORAL DOCUMENT PROTECTION IN THE REAL WORLD

Trusted files, most notably documents (Word Files & Excel Documents), can easily be overlooked as a potential threat. Malicious actors know this and embed and obfuscate harmful code inside.

In February 2018, attackers used Sofacy Malware to target foreign affairs and defense-related ministries across Europe and North America. All of the targets were members of NATO and western aligned countries that were targets of Russian intelligence-gathering efforts.

The Sofacy attacks took place in two staqes. The first leveraged a phishing email that used a common subject line about an upcoming defense-related event, and the sender claimed to be from a trusted source in the defense industry known for research data (Jane's). A deeper look at the email header would have shown the address as a spoof. However, many people neglected to see this discrepancy. Instead, they noticed an attachment for a calendar of events and instructions if the reader had trouble reading the attachment.



Next, when the user opened the attachment, a malicious macro hid the text until the victim enabled macros. The attackers tricked victims by making the document's font the color white, leading the victim to think they needed to enable macros to solve the readability issue. Next, a malicious executable was run, and a trojan responsible for installing and running the payload allowed Sofacy to effectively infiltrate the victim's machine and environment, compromising their data.

Cybereason's Behavioral Document Protection identifies the threat posed in this excel attachment and stops the user from being harmed by recognizing the unusual nature of the file contents, all the way down to inconsistencies with file naming. That is why Cybereason takes a layered approach to defend against adversaries like APT 28 or Fancy Bear.

Cybereason can detect and quarantine Word, Excel, PowerPoint, and Rich Text (RTF) documents and allows customers to vary the level of sensitivity

## HOW DOES BEHAVIORAL DOCUMENT PROTECTION WORK?

Behavioral Document Protection identifies documents containing code, such as macros, analyzes them for signs of maliciousness using AI-based algorithms and quarantines those deemed malicious. Behavioral Document Protection analyzes documents when accessed, such as written to disk, thus ensuring that all documents are analyzed before any application can load them. That is why Cybereason can detect and quarantine Word, Excel, PowerPoint, and Rich Text (RTF) documents and allows customers to vary the level of sensitivity.

NOW THAT WE'VE DISCUSSED HOW BEHAVIORAL DOCUMENT PROTECTION BLOCKS THE MALICIOUS USE OF MACROS IN DOCUMENTS, LET'S LOOK AT THE NEXT LOGICAL STEP IN DEFENDING FORWARD:



# Fileless Malware Prevention

Attackers use increasingly sophisticated attack techniques to infiltrate systems through various engines and products. Most successful attacks use fileless malware to infiltrate systems.

In many cases, fileless attacks never access the disk, meaning that these attacks can easily elude standard antivirus tools

Attackers use various modules, frameworks, and programs (Powershell engine, .Net, JScript, VBScript, and Office macros) to launch advanced, fileless attacks to take control of a module, framework, or program, often without using the relevant process. In many cases, fileless attacks never access the disk, meaning that these attacks can easily elude standard antivirus tools.

# FILELESS MALWARE PREVENTION IN THE REAL WORLD

The July 2021 ransomware attack on Kaseya VSA by the notorious Russia-linked ransomware group REvil leveraged a vulnerability in the company's remote computer management tool, ultimately impacting more than 2,000 organizations.

The attack involved a malicious hotfix released by the attackers, which encrypted thousands of endpoints at multiple companies. PowerShell was used to carry out the critical piece of the attack to disable the antivirus prevention capabilities of Windows Defender (i.e., real-time detection, script and file scanning, and a host-based intrusion prevention system).

By July 4, REvil operators boasted on the group's "Happy Blog" that more than 1 million individual devices were infected and that they would provide a universal decryption key to Kaseya for $70 million in Bitcoin.

Cybereason NGAV prevents malicious PowerShell commands before the commands can execute

# HOW DOES FILELESS MALWARE PREVENTION WORK?

Cybereason NGAV, specifically Fileless Malware Prevention, examines the behavior of the Powershell engine, .Net, JScript, and VBScript to ensure that attackers cannot slip by defenses by loading malicious code into memory.

- **Powershell:** Attackers use the legitimate PowerShell module to launch advanced, fileless attacks. Cybereason NGAV prevents malicious PowerShell commands before the commands can execute, even in cases where an attacker obfuscates the PowerShell command.
- **.NET:** Attackers increasingly exploit the powerful .NET framework. Cybereason can defend against malicious .NET techniques such as DotNetToJScript, .NET floating modules, and tools such as SharpSploit, SILENTTRINITY, and Internal Monologue.
- **JScript and VBScript:** Attackers use native Windows scripting languages to implement sophisticated, multiple-stage attacks. For example, malicious documents may launch an HTML page containing VBScript code that triggers malicious shellcode. NGAV Fileless Malware Prevention exposes these behaviors and identifies the stage where the script needs to supply the scripting engine with plain, unobfuscated code. It then scans and blocks this deobfuscated content.
- **Office Macros:** Attackers use malicious macros within the VBA framework to launch attacks from Office documents. If Cybereason NGAV detects specific Windows API calls that are considered high-risk, it analyzes the macro and prevents it from executing if the macro is deemed malicious.
- **Windows Management Instrumentation (WMI):** Attackers use WMI to interact with local and remote systems and assist discovery and lateral movements, such as gathering information or remote file execution. Cybereason NGAV integrates with Microsoft Antimalware Scan Interface (AMSI) on Windows systems to protect against attacks that exploit WMI.

NOW THAT WE'VE DISCUSSED FILELESS MALWARE PREVENTION, LET'S LOOK AT THE NEXT LOGICAL STEP IN DEFENDING FORWARD:

# Behavioral Execution Prevention

Protection to stop Living Off the Land Style Attacks where attackers use obfuscation techniques with trusted 3rd party software to hurt you.

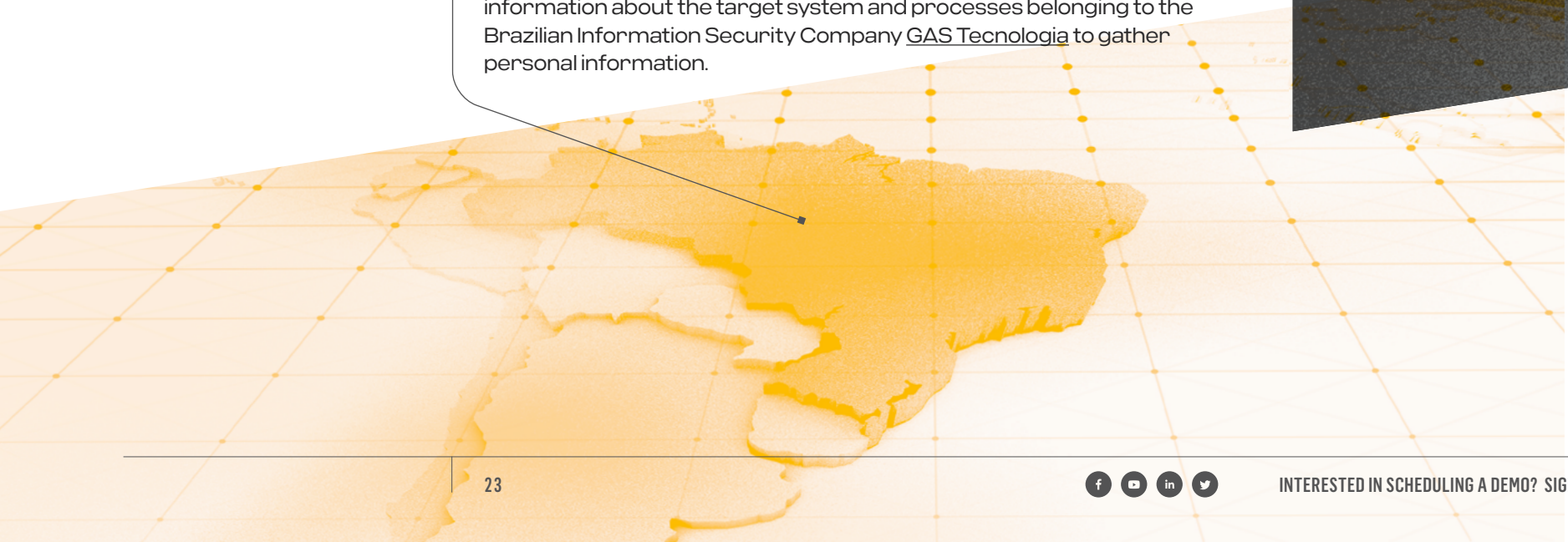
# BEHAVIORAL EXECUTION PREVENTION IN THE REAL WORLD

Astaroth Malware is a wolf in sheep's clothing, a Living Off the Land (LOL) type of attack, where trusted software programs (i.e. Operating Systems Mac OS & Windows) become dangerous to the victim.

Amid a dramatic rise in cyber crimes across Brazil in 2018 and abuse of legitimate native Windows OS processes for malicious purposes, the Cybereason Nocturnus Team discovered a nefarious campaign involving the Astaroth trojan targeting financial services organizations across Brazil and Latin America.

The Astaroth trojan exploited and abused native OS processes and trusted security solutions in its attack. In simple terms, Astaroth took advantage of legitimate tools like the Windows BITSAdmin utility and WMIC utility to interact with a C2 server and download a payload. Then it leveraged a component of antivirus software Avast to gain information about the target system and processes belonging to the Brazilian Information Security Company GAS Tecnologia to gather personal information.

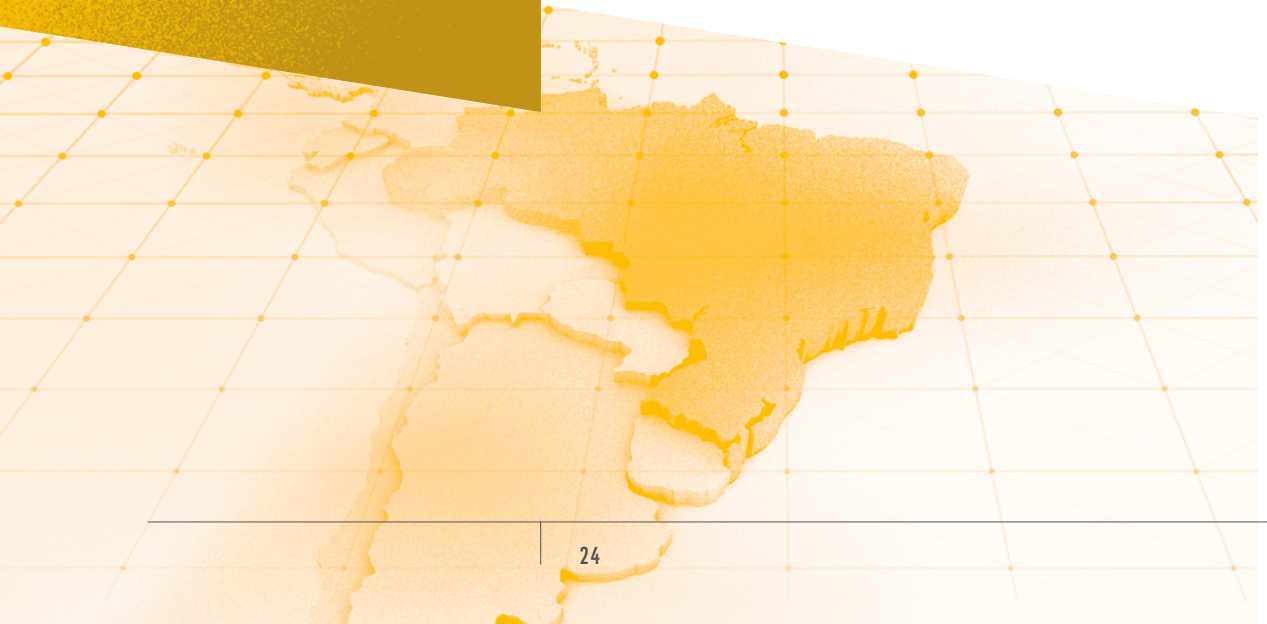
The Astaroth trojan exploited and abused native OS processes and trusted security solutions



Another powerful aspect of BEP is the ability to continue operating if the endpoint is disconnected from the platform

This particular version differed from previous versions of Astaroth. First, it used BITSAdmin, not Certutil. And while previous versions would quit when Avast was uncovered, this version injected malicious code into Avast's processes to evade detection. The attacks did have something in common: They all started with a phishing campaign and associated zip file attachments before following the attack sequence above. This was a sophisticated attack, and it involved thousands of victims.

Cybereason's Behavioral Execution Prevention using Binary Similarity Analysis technology would have been able to identify the subtle signatures of malicious code being executed in trusted processes like BITAdmin utility and stop them upon execution in real-time, thus rendering the attack harmless.



## HOW DOES BEHAVIORAL EXECUTION PREVENTION WORK?

Behavioral Execution Prevention (BEP) leverages Endpoint Detection and Response (EDR) detections to generate preventative heuristics for the Cybereason NGAV suite. BEP leverages data patterns and rules to detect abnormalities in image metadata and names, command line commands, and process hierarchies to stop attackers in their tracks. Another powerful aspect of BEP is the ability to continue operating if the endpoint is disconnected from the platform, such as working offline. Behavioral Execution Prevention is designed to reduce the attack surface and decrease the time needed for Cybereason's NGAV product to block malicious activity.

NOW THAT WE'VE DISCUSSED HOW BEHAVIORAL EXECUTION PREVENTION BLOCKS LIVING OFF THE LAND ATTACKS, LET'S LOOK AT THE NEXT LOGICAL STEP IN DEFENDING FORWARD:

# Variant Payload Prevention

Monitors the code being loaded into memory and uses Binary Similarity Analysis to identify previously unknown (obfuscated) malware based on its similarities to existing malware payloads such as a Cobalt Strike Beacon or Metasploit Meterpreter.

# VARIANT PAYLOAD PREVENTION IN THE REAL WORLD

With Cybereason's Anti-Ransomware mode enabled, the Ryuk execution is stopped before encrypting the hard drive

Emotet was first identified as early as 2014 as a trojan used to steal banking credentials. Shortly after Version 1 was released, it was updated to Version 2 with money transfer, malspam, and banking features. By January 2015, it had evolved yet again with evasive features.

Emotet's capabilities have continued to advance significantly into a type of modular malware. Because of its modular nature and the practicality of Emotet's distribution features, it is often used by attackers to gain a foothold in a target environment.

Emotet's main infection vector is through phishing attacks, which use emails with malicious links or Microsoft Word files with malicious macros embedded to spread. Once deployed, Emotet can launch different malware payloads based on the target machine and its goal.

Since its discovery, Emotet has evolved from a traditional banking Trojan to a malware loader. Over the last few years, before authorities disrupted the infrastructure of Emotet operators as part of a global operation in the first quarter of 2021, malicious actors have been using Emotet to deliver the Ryuk ransomware to compromised systems.

Cybereason detects the various execution phases of Ryuk in detail, including process injection, persistence creation, and shadow copy deletion. With Cybereason's Anti-Ransomware mode enabled, the Ryuk execution is stopped before encrypting the hard drive.

# HOW DOES VARIANT PAYLOAD PREVENTION WORK?

Cybereason NGAV includes Variant Payload Prevention, which performs real-time analysis of memory executions to detect every fracture of malicious code. It also identifies previously unknown malware based on its "genetic" similarities to existing malware, creating a powerful fingerprint immune to subtle code modifications.


WATCH VIDEO

NOW THAT WE'VE DISCUSSED VARIANT PAYLOAD PREVENTION LET'S LOOK AT THE NEXT LOGICAL STEP IN DEFENDING FORWARD:

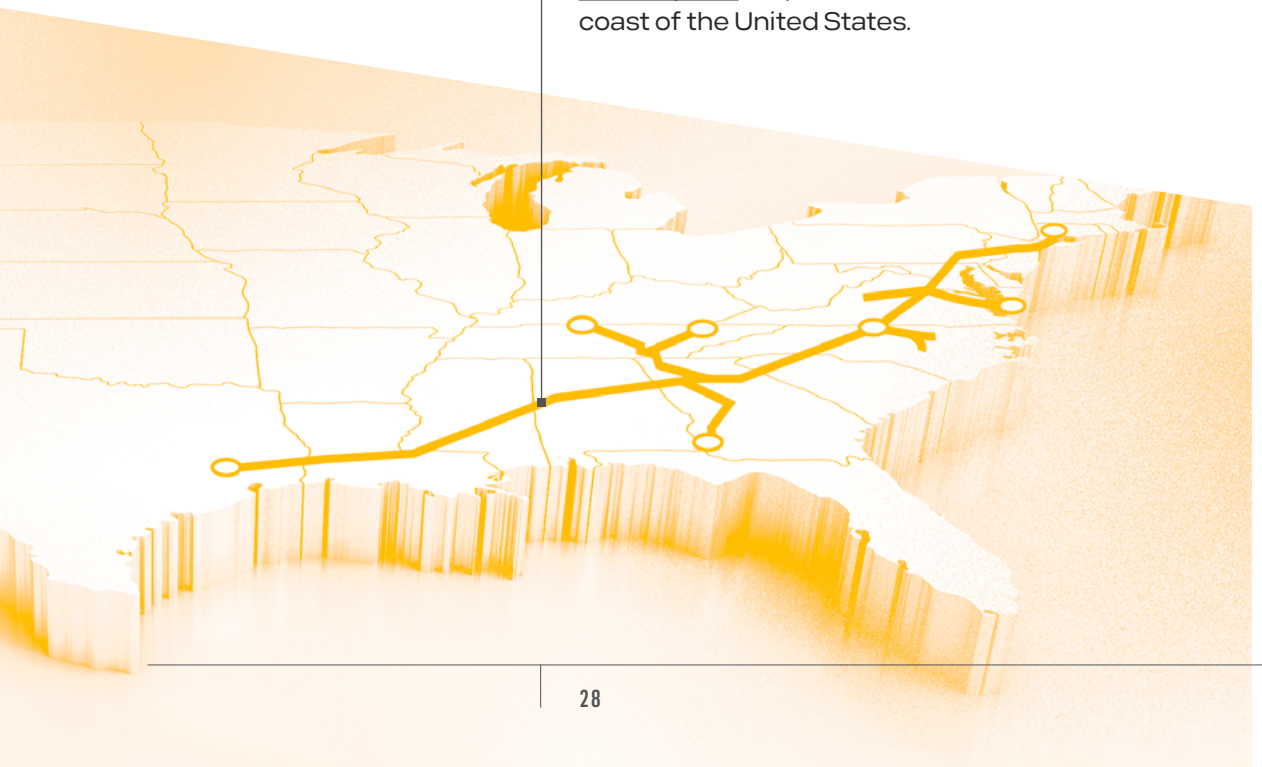
# Predictive Ransomware Protection

With multiple layers of behavioral-based prevention, Cybereason's Predictive Ransomware Protection stops any ransomware strain - even those never before seen - and restores impacted files.

# PREDICTIVE RANSOMWARE PROTECTION IN THE REAL WORLD

Ransomware is a pervasive and dangerous threat that is top of mind for security organizations around the globe. Attacks like the one launched in 2021 against the Colonial Pipeline demonstrate the need for organizations to deploy technologies capable of defeating sophisticated and targeted ransomware attacks.

On May 8th, 2021, a ransomware attack targeted the largest fuel pipeline in the United States, stopping the flow of nearly 100 million gallons of fuel across the entire eastern seaboard. The economic impact was significant as the pipeline provides close to 45% of the daily fuel required for the economies of the east coast of the United States.



The result was an immediate increase in gasoline prices (6 cents per gallon) and panic across the industry, government officials, and consumers. Over the next six days, as the pipeline remained shuttered, fuel shortages began to affect consumers across the country.

On May 10th, the FBI announced that the FIN7 ransomware group had targeted the Colonial Pipeline using their Darkside ransomware. The attackers had gained access to Colonial's network a month earlier using a VPN (Virtual Private Network) account that was no longer in use at the time of the attack. The password for the account was found on the dark web in a batch of leaked emails from a previous hack. The VPN did not have MFA (Multi-Factor Authentication), which may have stopped the attack and is a common security control measure used today by security practitioners. Furthermore, Colonial did not have robust anti-ransomware prevention in place, which would have provided a further safeguard to protect against attacks like this.

By the end of the shutdown, Colonial paid a $4.4 million ransom ($2.3 million of which was recovered by the FBI) to restore pipeline operations. Predictive Ransomware Protection from Cybereason is designed to stop attacks like the one launched against Colonial Pipeline by using sophisticated AI-driven tools that can identify and stop ransomware like Darkside from encrypting files and doing damage to organizations.

AI-powered, enterprise anti-ransomware solution designed to detect the most subtle of adversary behaviors

# HOW DOES PREDICTIVE RANSOMWARE PROTECTION WORK?

Cybereason's Predictive Ransomware Protection works to identify key indicators of behavior attributed to ransomware like Darkside, quarantines it, and prevents it from being executed. Predictive Ransomware Protection is an AI-powered, enterprise anti-ransomware solution designed to detect the most subtle of adversary behaviors at the earliest stages of an attack and automatically end the operation before data exfiltration or disruptive encryption can occur.

Using artificially intelligent endpoints, multilayer protection, and visibility from the kernel to the cloud, even the most sophisticated attackers can't evade it. In the rare event that an attacker encrypts data, Cybereason's rapid recovery feature can restore the targeted data to its original state and ensure organizations are up and running quickly with minimal downtime or impact.


WATCH VIDEO

Now that we've discussed how Predictive Ransomware Protection stops ransomware attackers in their tracks and talked about how Cybereason has redefined NGAV for our customers consider scheduling a personalized demo with us!

Interested in scheduling a Demo? Sign up now!