

## Q1 2020

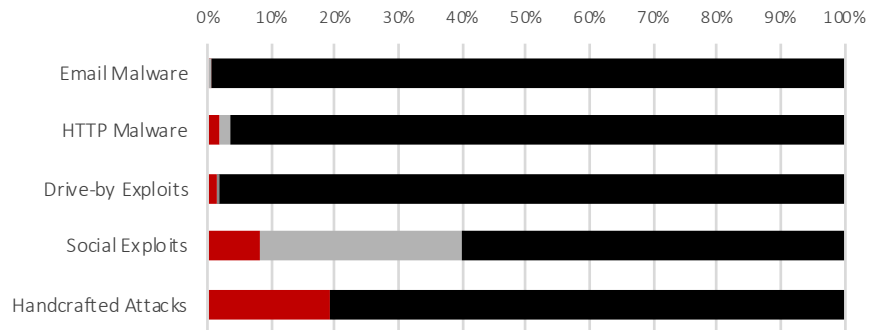
## PRODUCT RATING

AA

### Overview & Outlook

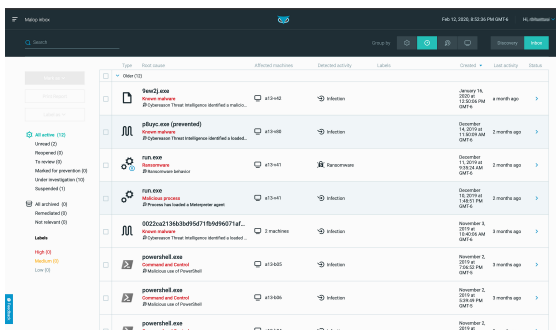
During Q1, 2020, NSS Labs performed an independent test of the Cybereason Professional v19.1.86.0.

Comprehensive, robust management. Overall protection impressive; low false positive rate; excellent resistance to evasion. Excellent malware protection; strong exploit protection. Minor room for improvement defending against handcrafted (targeted) attacks.



### MANAGEMENT

AA



Central management is available with a thin client (web browser), which we used during testing. Cybereason also offers an API and service offering to augment standard UI features. Installation and configuration of Cybereason Professional occurred without a hitch and ongoing operational tasks were easy to perform.

The management console supports role-based access control (RBAC) and third-party authentication using TFA via TOTP-compatible one-time password generators. We found it to be straightforward to define and save multiple security policies, which we then applied to specific users and groups. Logging was robust and the use of standardized logging and reporting formats facilitated fast and accurate consumption of data. The system provided built-in reports, including industry-standard reports for compliance, as well as the ability to generate custom reports. Change control is solid, with built-in audit logs as well as (optional) revision history and rollback capabilities available as a service.

**FALSE POSITIVE RATE** 6/645 (0.9%) AA

With a false positive rate of 0.9%, the Cybereason Professional is unlikely to introduce much additional work for administrators.

### RESISTANCE TO EVASION

49/49 (100%) AAA

The endpoint protection was capable of detecting and blocking malware and exploits when subjected to numerous evasion techniques.

### BLOCK RATE

2,260/2,282 (99.04%) AA

ATTACKS	RATING	BLOCKED ON DOWNLOAD	BLOCKED ON EXECUTION	TOTAL BLOCKED	DETECTED	UNBLOCKED & UNDETECTED
Email Malware	AA	1,525	4	1,529	-	2
HTTP Malware	AA	410	7	417	-	7
Drive-by Exploits	AA	251	-	251	1	4
Social Exploits	AA	30	16	46	-	4
Handcrafted Attacks	A	17	-	17	-	4
<b>TOTAL</b>	<b>AA</b>	<b>2,233</b>	<b>27</b>	<b>2,260</b>	<b>1</b>	<b>21</b>
		99.04%	0.04%	0.92%		

Results indicate that the product is highly capable. We found the protection against the vast majority of classic malware attacks to be excellent, as was the protection against more advanced attacks, including exploits of all types. Only when the product was asked to protect against handcrafted (targeted) attacks did we find its protection could improve a bit, albeit slightly, with 17 of 21 attacks blocked.

### TOTAL COST OF OWNERSHIP

\$172,500

#### Expected Costs (2,500 Agents)

Initial Purchase Price	\$57,500
Annual Cost of Support/Maintenance	\$0
Other Annual Cost (AV, IPS, Cloud, etc.)	\$0
<b>3-Year Total Cost of Ownership</b>	<b>\$172,500</b>
Total Cost Year 1	\$57,500
Total Cost Year 2	\$57,500
Total Cost Year 3	\$57,500

### Summary of Results

## Table of Contents

<b>Security.....</b>	<b>3</b>
Tuning and False Positives.....	3
Resistance to Evasions.....	3
Malware Delivered over Email .....	4
Malware Delivered over HTTP .....	4
Drive-by Exploits.....	5
Social Exploits .....	6
Handcrafted (Targeted) Attacks.....	6
<b>Management &amp; Reporting Capabilities.....</b>	<b>7</b>
Authentication .....	7
Policy.....	7
Logging.....	7
Change Control.....	8
Reporting .....	8
Alert Handling .....	8
<b>Total Cost of Ownership (TCO) .....</b>	<b>9</b>
3-Year Total Cost of Ownership .....	9
<b>Test Environment.....</b>	<b>10</b>
<b>Appendix .....</b>	<b>11</b>
<b>Authors.....</b>	<b>12</b>
<b>Test Methodology .....</b>	<b>12</b>
<b>Contact Information.....</b>	<b>12</b>

## Table of Figures

Figure 1 – False Positives.....	3
Figure 2 – Resistance to Evasions .....	3
Figure 3 – Malware Delivered over Email .....	4
Figure 4 – Malware Delivered over HTTP .....	4
Figure 5 – Drive-by Exploits.....	5
Figure 6 – Social Exploits .....	6
Figure 7 – Handcrafted (Targeted) Attacks.....	6
Figure 8 – 3-Year TCO (US\$).....	9

# Security

The threat landscape is evolving constantly; attackers are refining their strategies and increasing both the volume and complexity of their attacks. Enterprises now are having to defend against everyday cybercriminal attacks as well as targeted attacks and even the rare advanced persistent threats (APTs). For this reason, we tested using multiple commercial, open-source, and proprietary tools to employ attack methods that are currently being used by cybercriminals and other threat actors. We increased the levels of difficulty as we tested, beginning with common attacks, escalating to targeted attacks, and then applying obfuscation techniques to see if we could evade defenses. We then recorded whether the endpoint protection blocked and logged threats accurately and how frequently it triggered false positives.

## Tuning and False Positives

This test includes a varied sample of legitimate application traffic that may be falsely identified as malicious (also known as false positives). As part of the initial setup, we tuned the endpoint protection as it would be by a customer. Every effort was made to eliminate false positives while achieving optimal security effectiveness and performance, as would be the aim of a typical customer deploying the device in a live network environment. To ensure that the vendor did not deploy unrealistic (overly aggressive) security policies that blocked access to legitimate software and websites, we tested the endpoint protection against 645 false positive samples, including but not limited to the following file formats: .exe, .jar, .xls, .xslm, .accdb, .css, .pdf, .doc, .docx, .zip, .DLL, .js, .xls, .chm, .rar, .lnk, .cur, .xrc, .slk, .ppt, pptx, .iqy, .htm.

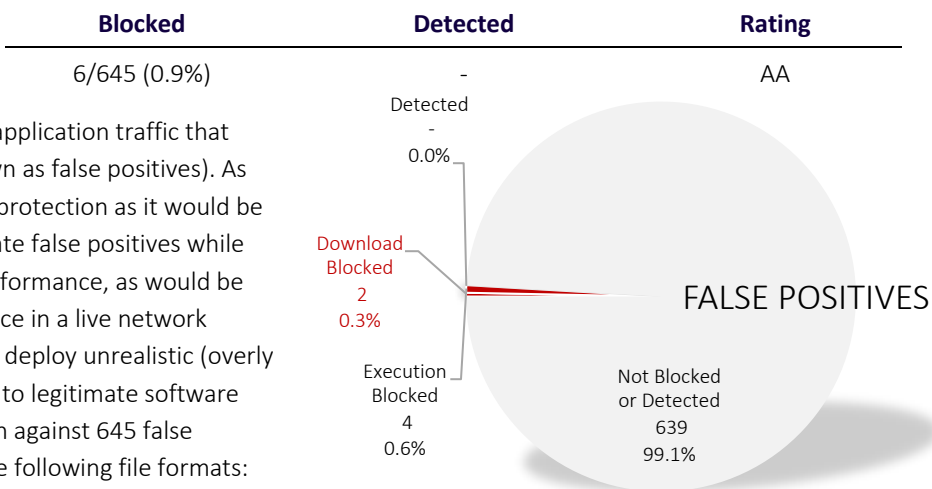


Figure 1 – False Positives

## Resistance to Evasions

Threat actors apply evasion techniques to disguise and modify attacks at the point of delivery in order to avoid detection by security products. Therefore, it is imperative that endpoint protection correctly handles evasions. If an endpoint protection platform fails to detect a single form of evasion, an attack can bypass protection.

Our engineers verified that the endpoint protection was capable of detecting and blocking malware when subjected to numerous evasion techniques. To develop a baseline, we took several attacks that had previously been detected and blocked. We then applied evasion techniques to those baseline samples and tested. This ensured that any misses were due to the evasions and not the underlying (baseline) attacks.

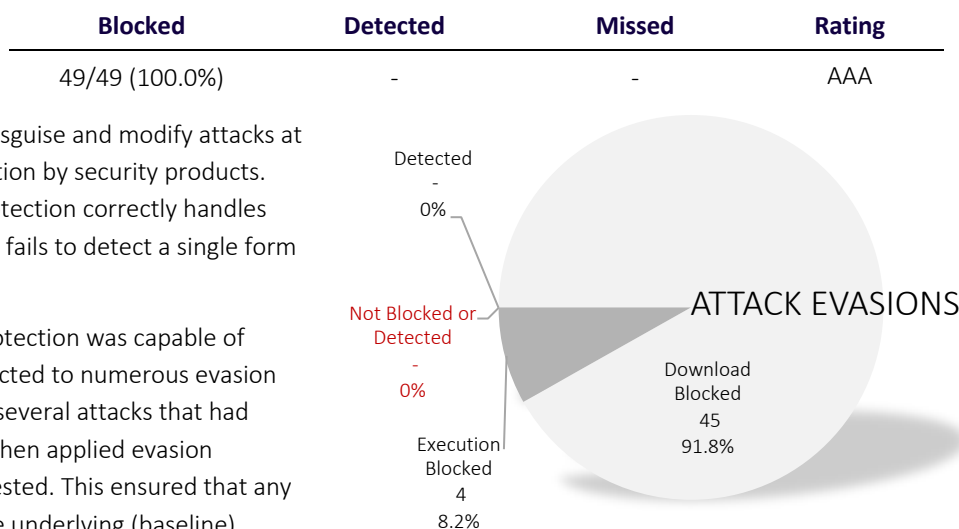


Figure 2 – Resistance to Evasions

For example, we applied an evasion technique called *process injection* where the original file is extracted from the binary and code is injected into a legitimate/trusted target process (i.e., Google Chrome). The malicious execution then occurs under the context of the target process (Chrome). Once these process injections techniques ran, we tried to further elude the detection by introducing anti-sandbox/anti-discovery evasions that employed techniques to determine whether or not the malware was on a user's machine; whether or not a security product was present; whether or not debugging or sandboxing was occurring; etc.

	Blocked	Detected	Missed	Rating
<b>Malware Delivered over Email</b>	1,529/1,531 (99.9%)	-	2/1,1531(0.1%)	AA

One of the most common ways in which users are compromised is through malware delivered over email. For several years, the use of social engineering has accounted for the bulk of cyberattacks against consumers and enterprises. Socially engineered malware attacks often use a dynamic combination of social media, hijacked email accounts, false notification of computer problems, and other deceptions to encourage users to download malware. One well-known social engineering attack method is spear phishing. Cybercriminals use hijacked email accounts to take advantage of the implicit trust between contacts and deceive victims into believing that the sender is trustworthy. The victim is tricked into opening the email attachment, which then launches the malicious malware program.

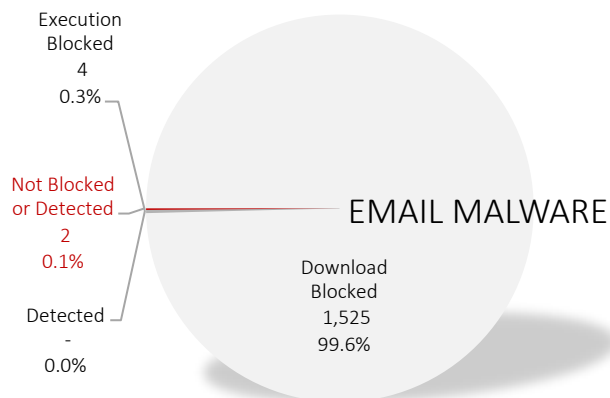


Figure 3 – Malware Delivered over Email

To test how well the endpoint protection is able to protect against this type of attack, malware was emailed to the user. The desktop client then retrieved the email and opened/executed the malware. If the malware was blocked, the corresponding time was recorded. We deployed a CentOS 7.7.1908 Linux mail store with kernel 3.10.0-957.5.1.el7.x86\_64 running Dovecot v2.2.36 for IMAP as the mail server. Victim machines consisted of a combination of 32-bit and 64-bit Windows 7 endpoints and 64-bit Windows 10 endpoints.

	Blocked	Detected	Missed	Rating
<b>Malware Delivered over HTTP</b>	417/424 (98.3%)	-	7/424 (1.7%)	AA

One of the more widespread threats to the enterprise involves attackers using websites to deliver malware. In these web-based attacks, the user is deceived into downloading and executing malware. For example, an employee may be tricked into downloading and installing a malicious application that claims it will “speed up your PC.”

In cases where an attacker is aiming for a large number of victims, the attacker may hijack widely used reputable websites to distribute the malware. However, in cases where an attacker plans to target specific individuals, the attacker typically would use an industry-specific “watering hole” plus one or more social engineering techniques to deceive a user into unknowingly installing malware.

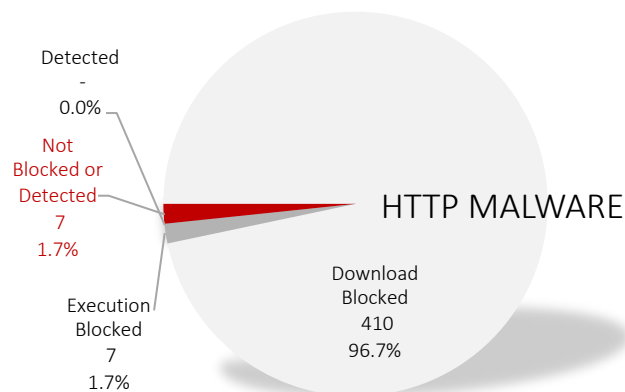


Figure 4 – Malware Delivered over HTTP

We tested the capability of the endpoint protection to protect against malware that was downloaded over HTTP and then executed (if the download was not blocked) using 424 malware samples against live victim machines running a combination of 32-bit and 64-bit Windows 7 endpoints and 64-bit Windows 10 endpoints, with various versions of Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, and Microsoft Edge. Browser reputation systems were disabled so that the endpoint protection was not inadvertently credited for protection offered by a web browser.

## Drive-by Exploits

Blocked	Detected	Missed	Rating
251/256 (98.0%)	1/256 (0.4%)	4/256 (1.6%)	AA

While there are millions (or hundreds of millions) of malware samples in circulation at any given point in time, they are frequently delivered by exploits that target consumer desktops known as drive-by exploits.

In a drive-by exploit, an employee visits a website containing malicious code that exploits the user's computer and installs malware without the knowledge or permission of the user. An example of this would be where an employee visits WSJ.com (Wall Street Journal), which is inadvertently hosting an advertisement that contains an exploit. Another example (that we frequently observe in the wild) is where a user navigates to a URL and then is re-directed without interaction to a web page serving malicious content. Using this technique, a single exploit can silently deliver and install millions of malware samples to unsuspecting victims' computers.

To test how well the solution was able to protect against drive-by exploits, victim machines were deployed running 32-bit Windows 7 (version 6.1 (Build 7601: SP1) and 64-bit Microsoft Windows 10 (version 1709 (Build: 16299.15) with Microsoft Office (Office 16.0.7341.2032) and various versions of Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, and Microsoft Edge. Depending on the victim machine, one or more of the following applications was installed: Java 8 Update 231, Microsoft Silverlight 5.1.20125, Adobe Flash Player 18.0.0.160, Adobe Reader DC 2017.012.20093, Adobe Reader 9.40, Java 6 Update 27, Adobe Flash Player 32.0.0.238, Java 8 Update 221, Microsoft Silverlight 5.1.50918, Adobe Flash Player 32.0.0.223, Java 8 Update 211, Adobe Flash Player 32.0.0.207, Internet Explorer 11, Internet Explorer 10, and Internet Explorer 9. Browser reputation systems were disabled so that the endpoint protection was not inadvertently credited for protection offered by a web browser.

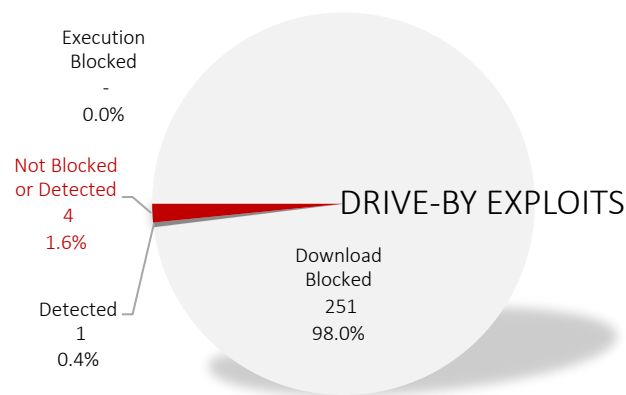


Figure 5 – Drive-by Exploits

While vulnerabilities are patched and defenses against exploits incorporated into new versions of operating systems (i.e., Windows), many organizations cannot easily upgrade due to financial, technical, or other constraints. As of January 2020, NetMarketShare<sup>1</sup> reports OS market share for Windows 7 (released 11 years ago in 2009) at 25.56% and for Windows 10 (released in 2015) at 57.08%.

Research has shown that oftentimes the most valuable assets have the most stringent change control to avoid business interruption. This creates a challenging dynamic whereby the most valuable assets tend to be the most difficult to defend (e.g., older OS, unpatched, etc.). Therefore, as vulnerabilities are patched and defenses against exploits are incorporated into new versions of operating systems (i.e., Windows)—which makes exploitation of computers more difficult—the value of endpoint protection is often associated with its ability to protect older, unpatched, and generally more vulnerable systems.

<sup>1</sup> <https://netmarketshare.com>

## Social Exploits

Blocked	Detected	Missed	Rating
46/50 (92.0%)	-	4/50 (8.0%)	AA

Social exploits combine social engineering (manipulating people into doing what you want them to do) and exploitation (malicious code designed to take advantage of existing deficiencies in hardware or software systems, such as vulnerabilities or bugs). An example of this would be an email with “Your Bonus” as a subject line and containing a malicious spreadsheet labeled “bonus.xlsx” (which the employee opens).

As with drive-by exploits, these attacks are limited to specific operating systems and/or applications. However, the exploits contained within Excel spreadsheets or Word documents may target kernel functions or common functions such as object handling, which provides attackers with a wide attack surface. As such, sending social exploits through mass email (phishing), could yield profit as the number of victims would be large, albeit smaller than in the case of malware since exploits would have technical dependencies.

To test how well the product was able to protect against social exploits, we deployed 19 victim machines. All of the machines were running Windows 10 version 1709 (OS Build 16299.15). Machines were configured with Internet Explorer 11 (version 11.15.16299.0 – Update Version 11.0.47) and Microsoft Office 2016 (version 16.0.7431.2032).

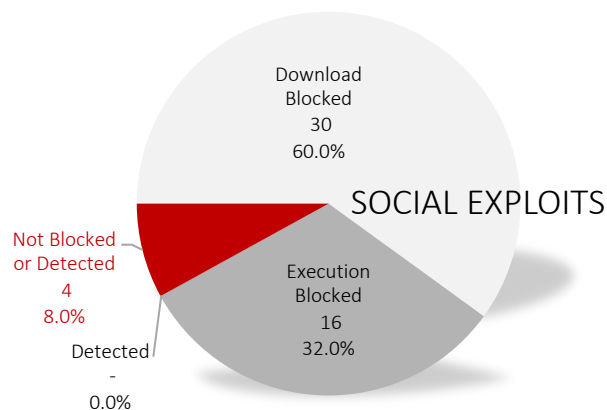


Figure 6 – Social Exploits

## Handcrafted (Targeted) Attacks

Blocked	Detected	Missed	Rating
17/21 (81.0%)	-	4/21 (19.0%)	A

The aim of this test was to see which endpoint products were able to protect customers while under adverse conditions dictated by the attacker. In this case, we wanted to find out which products could block new handcrafted (unknown) malware while being prevented from accessing cloud services.

What happens, for example, if an employee goes on a business trip to China where Internet traffic is tightly controlled? In such a scenario, access to the corporate VPN is likely blocked and the security software on the employee’s laptop may not be able to receive updates or communicate in general. What happens if the employee’s laptop is attacked with targeted malware?

For the purposes of this test, handcrafted (targeted) malware was created by modifying the source code of keyloggers, ransomware, and destructware, and then recompiling the binary so that it was new to the products being tested. We then attempted to infect a host (e.g., a laptop) with the malware and recorded whether or not the endpoint protection blocked the attack.

Because creating samples in this manner is a painstaking and time-consuming exercise, we tested only a handful of targeted samples; results should be viewed with this in mind.

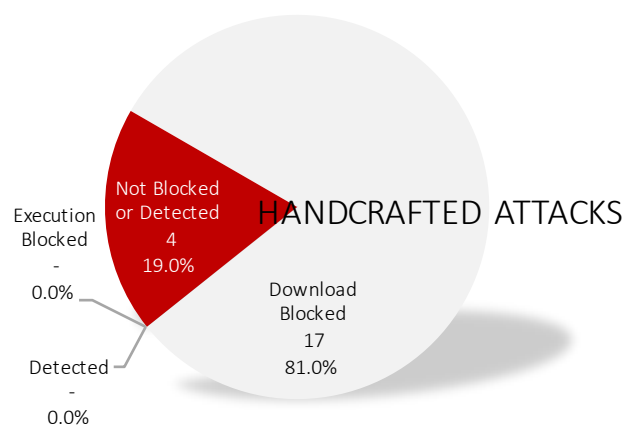


Figure 7 – Handcrafted (Targeted) Attacks

Central management is available with a thin client (web browser), which we used during testing.

# Management & Reporting Capabilities

Rating

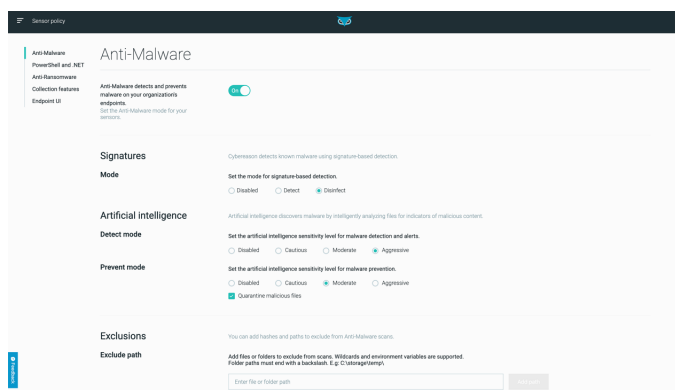
AA

## Authentication

Cybereason management supports role-based access control (RBAC). Roles include: L1 Analyst, L2 Analyst, L3 Analyst, Executive, Responder, API User, User Administrator, System Administrator. These roles allow granular assignment of permissions to perform specific tasks such as examining alerts, investigating alerts, threat hunting, responding to threats, and managing different aspects of the system (users, policies etc.). Third-party authentication is supported using TFA via TOTP-compatible one-time password generators.

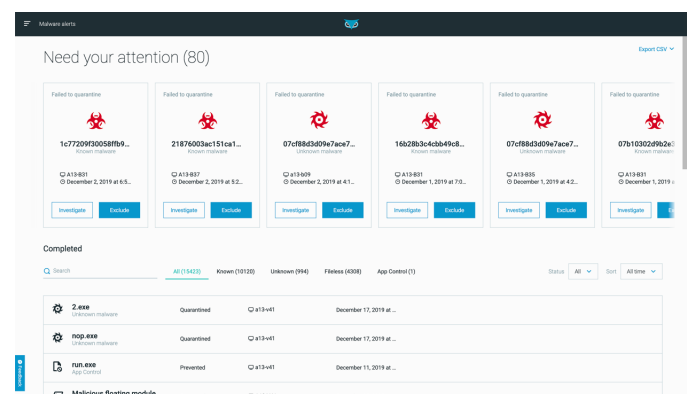
## Policy

Cybereason supports 50 policies by default, and this can be extended by customer request to an unlimited number. Cybereason policies enable the user to custom define prevention and detection settings, including active/inactive prevention and detection engines, sensitivity levels, custom rules, and whitelists and blacklists, and the user can also define custom endpoint control policies including personal firewall and device control policies. Configuration granularity is also per engine.



Once policies have been defined, it is possible to assign them to specific endpoints based on multiple possible endpoint tags, including endpoint users, network location/site, endpoint function (e.g., web server, domain controller, developer endpoint, etc.) Policies may be inherited such that endpoints can be grouped to receive a different setting from the assigned policy that has been applied to all endpoints. Bulk operations enable changing a policy item across an entire group via the policy management user interface, or as automated via the API.

The applicable policy on each endpoint is displayed in the endpoint management screen alongside the policy identifier. The endpoint agent validates that the policy is properly digitally signed with the relevant Cybereason server certificate and is compared via checksum to verify that the configuration has not been tampered with and that it matches the server configuration. Furthermore, it is possible to perform a diff of policies to highlight changes between versions via the API.



## Logging

Routine tasks such as log file maintenance and power cycling as well as any hardware failures or service interruptions are managed by Cybereason as part of its SaaS solution; customers are notified as part of the service should there be impact to users. The logs of the CMS contain policy changes and who made them, as well as any administrative actions such as session login/logout, user login/logout, successful authentication, and unsuccessful authentication attempts. The management system provides notifications for sensors that are not operating normally and informs the administrator when an endpoint is rebooted.

All logs are recorded using Greenwich Mean Time (GMT), but time in the user interface can be displayed in either GMT or the administrator's local time zone. To aid forensic analysis, malicious traffic information from endpoints and the corresponding reason an alert was triggered is logged and displayed for analysts.

## Change Control

Cybereason logs include full change control tracking; each logged activity includes the username and time of change as well as details of the change. Revision control and rollback are optional services that automatically back up policies whenever there is a change and can generate a differential report between any two revisions. Revisions may be automatically saved so that any prior rule/policy can be restored.

## Reporting

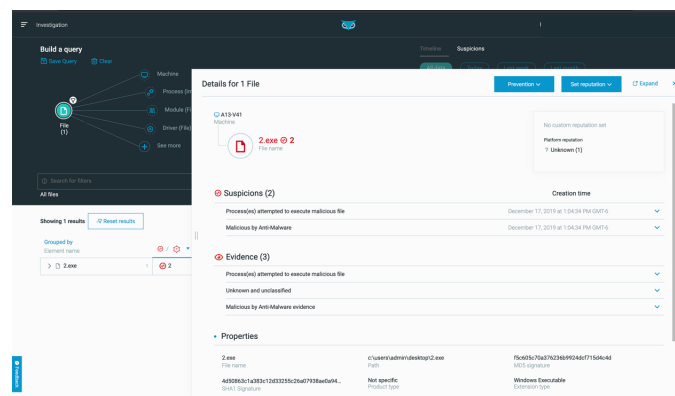
Cybereason provides summary reporting on all alerts from a single central management console. The product includes a report generator that enables administrators to construct complex data filters and summarize alerts on the specified search criteria. Reports are exportable in PDF format.

Built-in reports covering typical requirements such as a list of top attacks, top source/destination IP addresses, top targets, etc. are available via API and as a service. Report scheduling and automated delivery is also available via API and as a service. A custom report filter is available via API; custom report filters and data queries may be saved for subsequent use.

## Alert Handling

Cybereason captures all events and changes made during an attack and automatically correlates separate activities into a single alert, with a unified incident timeline, even when these activities are performed on different machines at different times, based on similarity in attack techniques used, i.e., tactics, techniques, and procedures (TTP), lateral movement indicators, and similarity in indicators of compromise (IOCs).

Complete telemetry into both incriminated and non-incriminated activities is also available to the administrator for guided and manual investigation, incident response, and threat hunting. All alerts are delivered to and handled by a single management console. Storage and overall capacity are managed by Cybereason as part of its SaaS offering.



Each alert contains an explicit reference to the rules and engines that triggered it. All data fields associated with an alert (process information, computer information, user information, network communication information) plus additional contextual information (other machines or users involved in the incidents, other machines communicating with the same network addresses, root causes of the incident, timeline of the incident, etc.) can be selected, searched on, and summarized. Incidents can be created based on the identifiers of the root cause (e.g., file hash, IP address, etc.) as well as by a behavior (TTP). Incidents can be annotated with status indicators as well as custom analyst notes. Exceptions can be created for benign activity (e.g., PowerShell scripts that are run by specific users on specific machines).



## Total Cost of Ownership (TCO)

Implementation of security solutions can be complex, with several factors affecting the overall cost of deployment, maintenance, and upkeep. All of the following should be considered over the course of the useful life of a product:

- **Initial Purchase** – The cost of acquisition
- **Maintenance/Subscription** – Fees paid to the vendor for ongoing use of software and access to updates
- **Technical Support** – Fees paid to the vendor for 24/7 support

### 3-Year Total Cost of Ownership

Calculations are based on vendor-provided pricing information. Where possible, the 24/7 maintenance and support option with 24-hour replacement is used, since this is the option typically selected by enterprise customers. Prices include the purchase and maintenance costs for 2,500 software agents

- **Year 1 Cost** is calculated by adding purchase price + first-year maintenance/support fees.
- **Year 2 Cost** consists only of maintenance/support fees.
- **Year 3 Cost** consists only of maintenance/support fees.

Expected Costs for Cybereason Professional – 2,500 Agents	
Initial Purchase Price	\$57,500
Annual Cost of Support/Maintenance	\$0
Other Annual Cost (AV, IPS, Cloud etc.)	\$0
3-Year Total Cost of Ownership	\$172,500
Total Cost Year 1	\$57,500
Total Cost Year 2	\$57,500
Total Cost Year 3	\$57,500

Figure 8 – 3-Year TCO (US\$)

# Test Environment

- BaitNET™ (NSS Labs Proprietary)
- 32-bit Microsoft Windows 7 (Version 6.1 (Build 7601: SP1)
- 64-bit Microsoft Windows 7 (Version 6.1 (Build 7601: SP1)
- 64-bit Microsoft Windows 10 (version 1607 (Build: 14393.0)
- 64-bit Microsoft Windows 10 (version 1709 (Build: 16299.15)
- Adobe Acrobat Reader 19.021.20061
- Adobe Flash Player 18.0.0.160
- Adobe Flash Player 32.0.0.207
- Adobe Flash Player 32.0.0.223
- Adobe Flash Player 32.0.0.238
- Adobe Reader 9.40
- Adobe Reader DC 2017.012.20093
- Google Chrome 78.0.3904.70
- Kali (Kernel release 4.19.0-kali1-amd64)
- Microsoft Internet Explorer 9.0.8112.16421
- Microsoft Internet Explorer 10.0.9200.16438
- Microsoft Internet Explorer 11.0.14393.0
- Microsoft Office Professional 2013 version 15.0.5119.1000 (Microsoft Word, Excel, PowerPoint, Access, etc.)
- Microsoft Office Professional 2016 version 16.0.7341.2032 (Microsoft Word, Excel, PowerPoint, Access, etc.)
- Microsoft Silverlight 5.1.20125
- Microsoft Silverlight 5.1.50918
- Oracle Java 6 Update 27
- Oracle Java 8 Update 181
- Oracle Java 8 Update 211
- Oracle Java 8 Update 221
- Oracle Java 8 Update 231
- Rapid7 Metasploit (v5.0.46-dev)
- VMware vCenter (Version 6.7u2 Build 6.7.0.30000)
- VMware vSphere (Version 6.7.0.30000)
- VMware ESXi (Version 6.7u3 Build 14320388)
- Wireshark version 3.0.3

## Appendix

NSS LABS RATINGS	
RATING	DEFINITION
AAA	A product rated 'AAA' has the highest rating assigned by NSS Labs. The product's capacity to meet its commitments to consumers is extremely strong.
AA	A product rated 'AA' differs from the highest-rated products only to a small degree. The product's capacity to meet its commitments to consumers is very strong.
A	A product rated 'A' is <b>somewhat</b> more susceptible to sophisticated attacks than higher-rated categories. However, the product's capacity to meet its commitments to consumers is still strong.
BBB	A product rated 'BBB' exhibits adequate protection parameters. However, sophisticated or previously unseen attacks are more likely to negatively impact the product's capacity to meet its commitments to consumers.
	A product rated 'BB,' 'B,' 'CCC,' 'CC,' and 'C' is regarded as having significant risk characteristics. 'BB' indicates the least degree of risk and 'C' the highest. While such products will likely have some specialized capability and protective characteristics, these may be outweighed by large uncertainties or major exposure to adverse conditions.
BB	A product rated 'BB' is less susceptible to allowing a compromise than products that have received higher-risk ratings. However, the product faces major technical limitations, which could be exposed by threats that would lead to its inability to meet its commitments to consumers.
B	A product rated 'B' is more susceptible to allowing a compromise than products rated 'BB'; however, it currently has the capacity to meet its commitments to consumers. Adverse threat conditions will likely expose the product's technical limitations and expose its inability to meet its commitments to consumers.
CCC	A product rated 'CCC' is currently susceptible to allowing a compromise and is dependent upon favorable threat conditions for it to meet its commitments to consumers. In the event of adverse threat conditions, the product is not likely to have the capacity to meet its commitments to consumers.
CC	A product rated 'CC' is currently highly susceptible to allowing a compromise. The 'CC' rating is used when a failure has not yet occurred but NSS Labs considers a breach a virtual certainty, regardless of the anticipated time to breach.
C	A product rated 'C' is currently highly susceptible to allowing a compromise. The product is expected to fail to prevent a breach and to not have useful forensic information compared with products that are rated higher.
D	A product rated 'D' is actively being breached by known threats and is unable to protect consumers. For non-specialized products, the 'D' rating category is used when protecting a consumer is unattainable without a major technical overhaul. Unless NSS Labs believes that such technical fixes will be made within a stated grace period (often 30-90 calendar days), the 'D' rating also is an indicator that it is a virtual certainty that existing customers using the product have already experienced a breach—whether they know it or not—and should take immediate action.

## Authors

Rabin Bhattarai, Thomas Skybakmoen, Vikram Phatak

## Test Methodology

NSS Labs Advanced Endpoint Protection (AEP) Test Methodology v4.0 is available at [www.nsslabs.com](http://www.nsslabs.com).

## Contact Information

NSS Labs, Inc.

3711 South Mopac Expressway  
Building 1, Suite 400  
Austin, TX 78746

[info@nsslabs.com](mailto:info@nsslabs.com)

[www.nsslabs.com](http://www.nsslabs.com)

**This and other related documents are available at: [www.nsslabs.com](http://www.nsslabs.com). To receive a licensed copy or report misuse, please contact NSS Labs.**

© 2020 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, e-mailed or otherwise disseminated or transmitted without the express written consent of NSS Labs, Inc. ("us" or "we").

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. "You" or "your" means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.
2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.
3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.
5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.
6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.