Q1 2022

Advanced Threat Defense

Certification Testing Report

RevBits
RevBits Endpoint Security

Tested against this standard

ICSA Labs Advanced Threat Defense Criteria v.1.0

April 19, 2022

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

ICSA Labs Advanced Threat Defense – Report-at-a-Glance

RevBits

RevBits Cyber Security Solutions

RevBits ENDPOINT SECURITY

www.revbits.com/

ICSA Labs CERTIFIED ADVANCED THREAT DEFENSE

ICSA Labs
Advanced Threat Defense

Certified

Test Period: Q1 2022
Certified Since: 04 / 2021

Executive Summary

During 29 days of testing during the first quarter of 2022, ICSA Labs tested the detection capabilities of RevBits Endpoint Security with a mix of 793 test runs. The mix was primarily composed of new and little-known malicious threats – i.e., recently harvested threats not detected by traditional security products.

Periodically, ICSA Labs launched innocuous applications and activities to additionally test RevBits Endpoint Security in terms of false positives. Throughout testing, ICSA Labs observed product logs to ensure not only that RevBits Endpoint Security indicated the existence of a malicious threat but also that logged threats were distinguishable from other logged traffic and events.

RevBits Endpoint Security passed, having met all criteria requirements. As seen in Figure 1 below, RevBits Endpoint Security did very well during this test cycle - detecting 99.6% of previously unknown threats while having zero false positives. Figures 2 and 3 below further highlight the RevBits solution's detection effectiveness and false positive (FP) test results.

Test Length	29 days	**Malicious Samples**	259	**Innocuous Apps**	534
Test Runs	793	**% Detected**	**99.6%**	**% False Positives**	**0%**

Fig. 1 – High Detection Effectiveness & Few False Positives

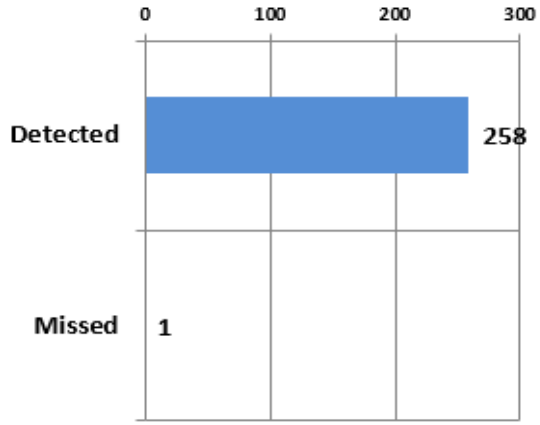


Fig. 2 – Detected 258 of 259 *New & Little-Known* Malicious Samples

Fig. 3 – 0 Alerts on 534 Innocuous Applications

Introduction

This is RevBits's 2nd consecutive ICSA Labs Advanced Threat Defense Certification testing report for RevBits Endpoint Security.

Standard ICSA Labs Advanced Threat Defense (ATD) testing is aimed at vendor solutions designed to detect new threats that other traditional security products miss. Thus, the focus is on how effectively vendor ATD solutions detect these unknown and little-known threats while minimizing false positives.

The remainder of the report presents a more detailed look at how the RevBits advanced threat defense solution performed during this cycle of standard ICSA Labs ATD Certification testing. To better understand how to interpret the results, this report documents not just the testing results themselves but the threat vectors, sample sources, and kinds of samples that ICSA Labs employed for this cycle of ATD testing against RevBits Endpoint Security.

Test Cycle Information

This report reflects the results of one test cycle at ICSA Labs. Standard ATD and ATD-Email test cycles are performed by ICSA Labs each calendar quarter and typically range from three to five weeks in duration. To be eligible for certification, security vendor solutions must be tested for at least 3 weeks. Because testing is performed quarterly, ICSA Labs tests ATD solutions four times during a calendar year.

During each test cycle ICSA Labs subjects advanced threat defense solutions to hundreds of test runs. The test set is comprised of a mix of new threats, little-known threats and innocuous applications and activities – delivered and launched one after another continuously for the length of testing. Below in Figure 4 is information about the test cycle from which this findings report is based.

Start Date	January 19, 2022	**Days of Continuous Testing**	29
End Date	February 19, 2022	**Test Runs**	793

Fig. 4 – This Test Cycle

ATD Solution Tested

During this testing cycle, ICSA Labs tested:

- RevBits Endpoint Security 1.9.0

  According to RevBits, RevBits Endpoint Security is intuitive, high-performance security software that blocks the most sophisticated attacks. RevBits Endpoint Security conducts a three-phase analysis of threats. The analysis is conducted first with signature comparisons, second with machine learning verification, and third using behavioral analysis. The feature-rich and comprehensive RevBits Endpoint Detection and Response (EDR) module provides complete control and access to the breached system from anywhere. For more information about RevBits Endpoint Security please visit:

  https://www.revbits.com/products/revbits-endpoint-security

Detection Effectiveness

To meet the criteria requirements and attain (or retain) certification through ICSA Labs testing, advanced threat defense solutions must be at least 75% effective at detecting new malicious threats. As shown in Figure 5 the RevBits Endpoint Security product detected 99.6% of the threats it encountered during testing, considerably better than the percentage required for certification.

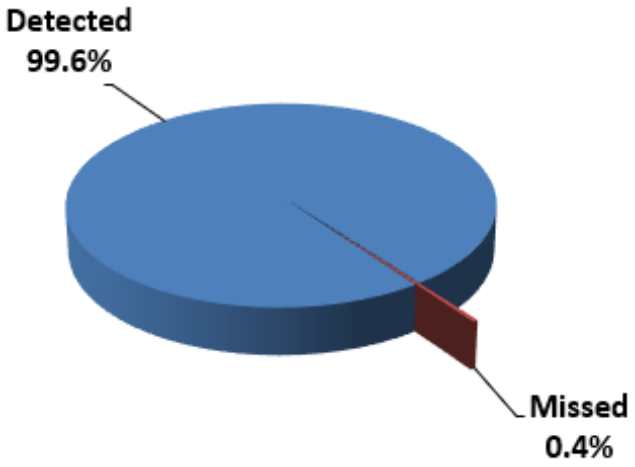


Fig. 5 – Detection Effectiveness of RevBits Endpoint Security

A second plot depicting the detection effectiveness of RevBits Endpoint Security appears in Figure 6. For the RevBits Endpoint Security product, the chart sheds light on whether or not RevBits did better or worse – the newer the malicious sample. RevBits Endpoint Security detected 97% of threats one hour old or less, which is excellent.

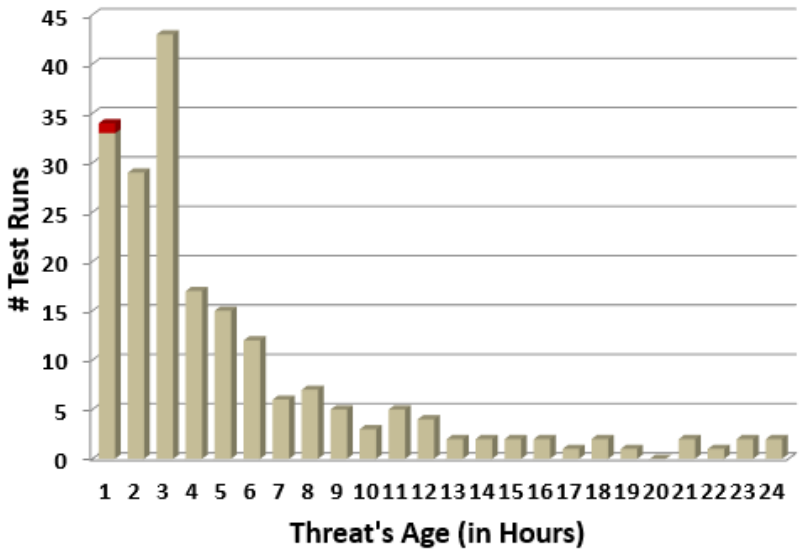


Fig. 6 – Detection Effectiveness by Age of Threat (Threats < 24 Hours Old)

A final effectiveness-related plot to consider for the RevBits Endpoint Security advanced threat defense solution during this test cycle is Figure 7 below. Plotted below is each of the 29 days during the test cycle along with how effective RevBits Endpoint Security was on each of those days. RevBits Endpoint Security was 100% effective on every day of the 29-day test cycle except for day 12, in which the solution missed just one malicious threat.

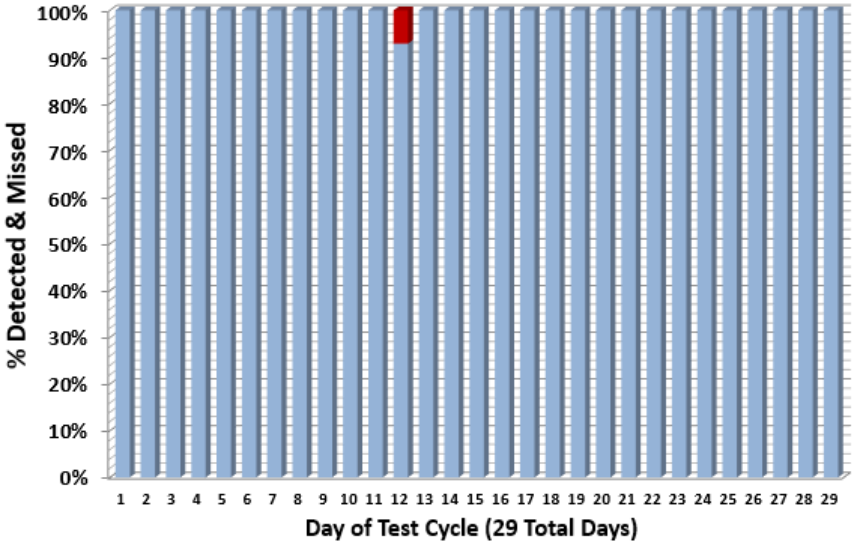


Fig. 7 – Detected & Missed Threats by Day of Test Cycle

Threat Vectors

In testing, ICSA Labs delivers new and little-known malicious threats to security vendor solutions using many of the top threat vectors that have led to enterprise cybersecurity incidents and breaches as reported in the latest Verizon Data Breach Investigation Report (DBIR).

DBIR data indicates that malware has been a key factor in thousands of security events where an information asset had its integrity, confidentiality, and/or availability compromised. Figure 9 on the following page depicts the threat vectors involved in these malware-related security incidents throughout the over fifteen-year history of Verizon's DBIR. Figure 8 below illustrates the most common malware-related threat vectors that lead to enterprise breaches during 2020 according to data from the 2021 DBIR.

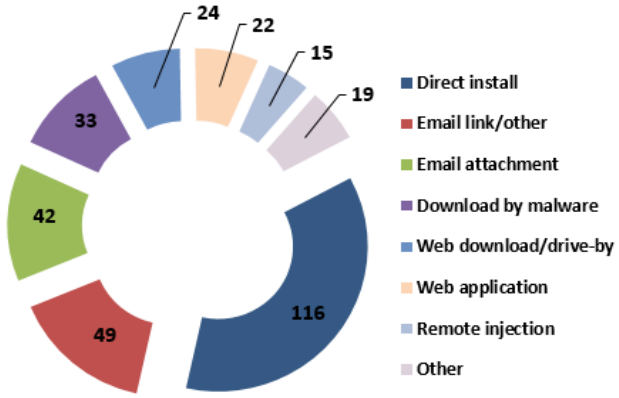


Fig. 8 – Top Threat Vectors Leading to Breaches in 2020 (per 2021 DBIR data)

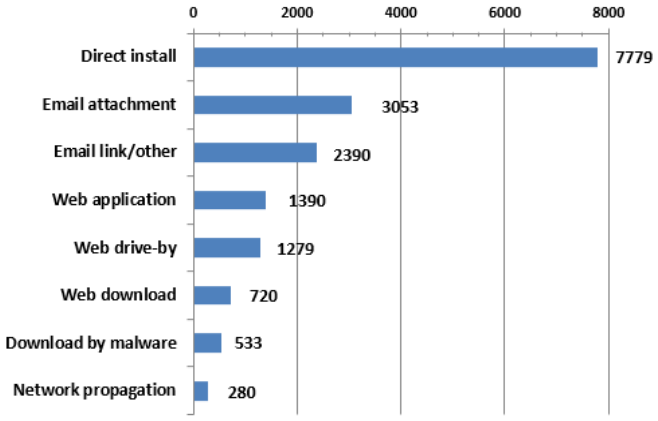


Fig. 9 – Malware-Related Threat Vectors Involved in Incidents (DBIR All-Time)

Standard ICSA Labs ATD testing includes the threat vector that is by far the most prevalent over time, "Direct Install". In addition, standard ATD testing includes the threat vectors labeled "Web download", "Web drive-by", and "Download by malware". In the separate but related, ICSA Labs ATD-Email testing, ICSA Labs delivers new and little-known malware in email attachments and emails with malicious URLs, corresponding to DBIR threat vectors "Email attachment" and "Email link/other", the latter being the second most common threat vector leading to enterprise breaches according to the 2021 DBIR (see Figure 8).

Source of Samples

A number of sample sources feed ICSA Labs' standard ATD and ATD-Email testing.

One source is the spam ICSA Labs collects. The labs' spam honeypots receive approximately 250,000-300,000 spam email messages/day. For ICSA Labs ATD testing, the team harvests attachments in that spam, making use of the ones that are malicious.

Samples may also come from malicious URLs. Some of these come from the spam mentioned above. From feeds like this ICSA Labs filters and checks the URLs to see if there is a malicious file on the other end of that URL -- either as a direct file link or a series of steps (e.g. a drive-by attack with a multi-stage download process) leading to it. If so, ICSA Labs collects the sample for potential use in testing.

ICSA Labs additionally uses other tools and techniques to create unique malicious files as an attacker or penetration tester might do. In some cases, these are trojanized versions of clean executables. In other cases, they may be original executables that are malicious.

Still another source of samples is the samples themselves. Any dropped files resulting from running another malicious sample are also evaluated and potentially used in testing.

Finally – and importantly to test for false positives – ICSA Labs also launches legitimate executables. Running innocuous applications helps ensure that vendor solutions aren't just identifying everything as malicious.

Regarding the Samples from this Test Cycle

Samples harvested for use in ATD testing are often unmodified and used as is. That is the case if ICSA Labs determines that the sample is new enough and/or not being detected by traditional security products. In many cases malicious samples require modification before they can avoid detection by traditional security products.

Of the 259 malicious samples, Figure 10 shows that there were more original samples used and fewer samples that required some kind of modification before use in testing. Of the 256 original samples, 0 were dropped, or left behind by other malware. Figure 11 reveals the source of the 256 malicious samples used in testing that were neither modified nor dropped.

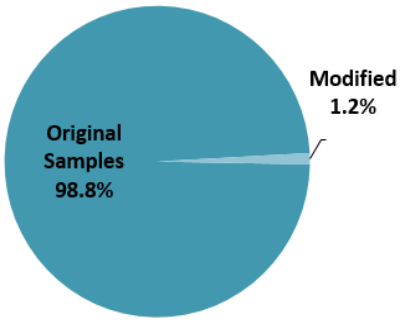


Fig. 10 –Malicious Samples – Original vs. Modified

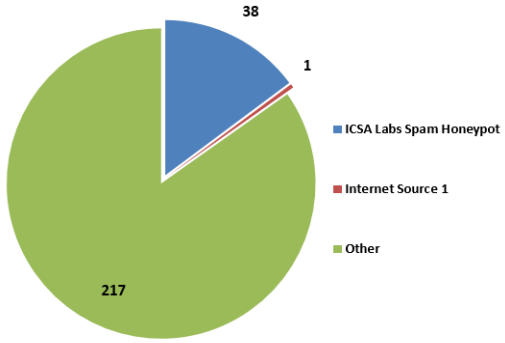


Fig. 11 – Unmodified/Non-Dropped Sample Sources

Following the test cycle, ICSA Labs analyzed the original malware samples used in testing, categorizing the malware into one of six malicious threat types: backdoor, ransomware, spyware, trojan, worm, or virus. Any malicious sample not falling into one of these six types, ICSA Labs categorized as “other”.

The six malware categories, and the number of original malicious samples used during the test cycle from each category are represented in Figure 12 on the next page. The figure indicates how many malicious threats RevBits endpoint Security detected and missed from each malware category during testing. In addition, the green line atop Figure 12 represents the effectiveness percentage of RevBits Endpoint Security against original malware belonging to each malware type.

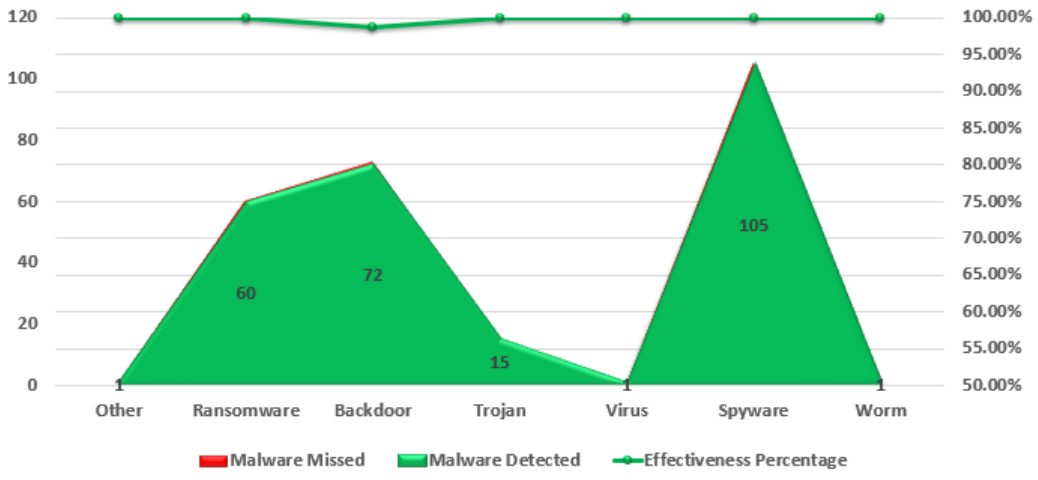


Fig. 12 – Effectiveness against original, unmodified malicious samples broken down by threat type

Figures 13 through 16 provide a deeper glimpse into four of the six malware types: ransomware, trojan, spyware, and backdoor. In its analysis of the original malicious samples used in testing, ICSA Labs further categorized malicious samples by malware family, where possible. The remaining figures, one for each of the four aforementioned malware types, are ordered by malware family. The figures show how many original malware samples Revbits Endpoint Security detected and missed across multiple malware families during the test cycle. In addition, the green line atop each figure indicates the effectiveness percentage of Revbits Endpoint Security against original malware from each malware family.

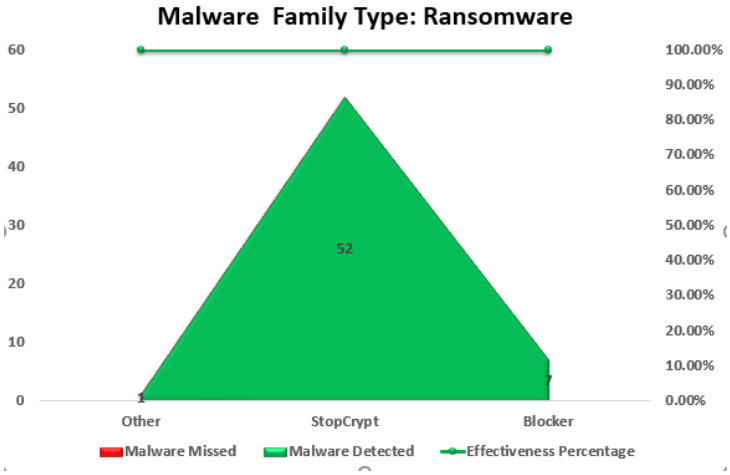


Fig. 13 – Effectiveness against Kinds of Ransomware Threats

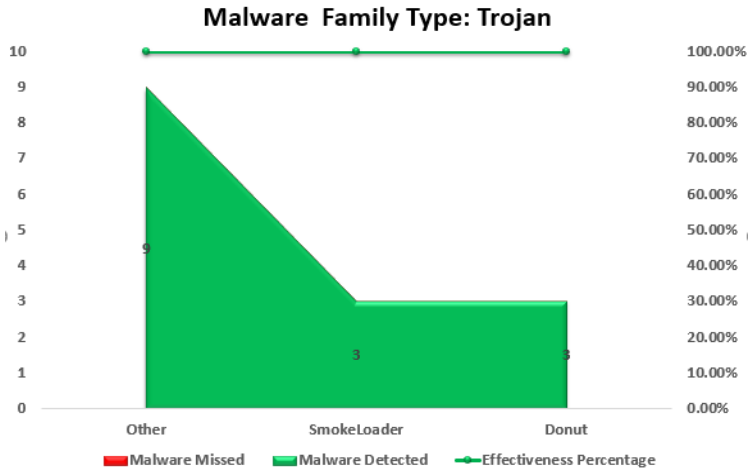


Fig. 14 – Effectiveness against Families of Trojans

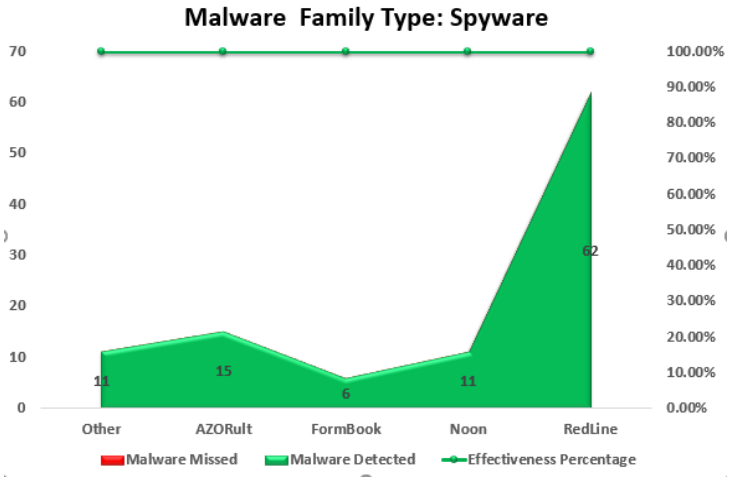


Fig. 15 – Effectiveness against Families of Spyware

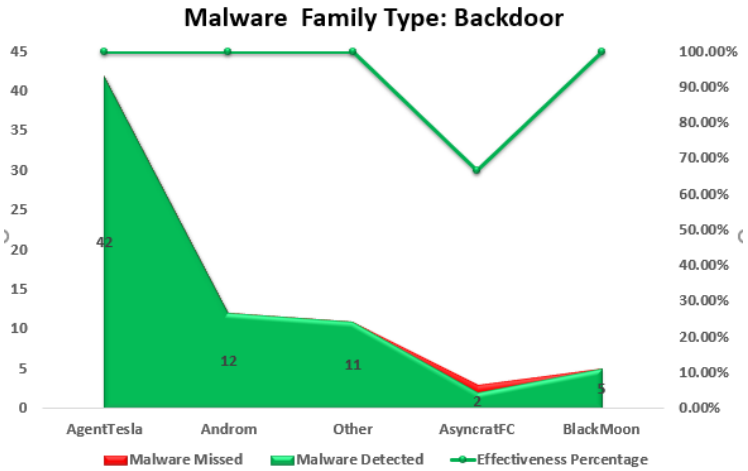


Fig. 16 – Effectiveness against Backdoors

As one would expect from a RevBits Endpoint Security solution that was 99.6% effective overall during the Q1 2022 test cycle, the solution was very effective at detecting malware across malware types and across malware families.

Prior ATD Reports

With this report, RevBits's Endpoint Security advanced threat defense solution passed all the test cases to retain ICSA Labs Advanced Threat Defense Certification. Successful completion of this test cycle marks RevBits Endpoint Security's 2nd consecutive quarter having met the ICSA Labs ATD certification testing criteria.

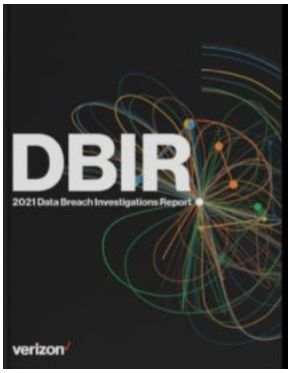
This and all earlier RevBits certification testing reports can be found on the ICSA Labs web site at:

https://www.icsalabs.com/product/revbits-endpoint-security

Significance of the Test & Results

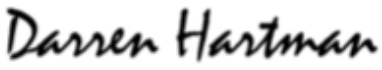
Readers of certification testing reports often wonder what the testing and results really mean. They ask, "In what way is this report significant?" The four statements below sum up what this ICSA Labs Advanced Threat Defense Certification Testing report should indicate to the reader:

1. ICSA Labs tested RevBits's Endpoint Security advanced threat defense solution using the primary threat vectors leading to enterprise breaches according to Verizon's Data Breach Investigations Report (DBIR).
2. ICSA Labs tests with malicious threats including new and little-known Ransomware that other security products typically miss.
3. RevBits Endpoint Security demonstrated superb threat detection effectiveness against over 255 *new and little-known* threats.
4. The RevBits Endpoint Security endpoint solution had 0 false positives during this test cycle which is excellent.



Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are performed under normal operating conditions.



Darren Hartman, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For over 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

www.icsalabs.com

RevBits IT Solutions

RevBits's AI- and ML-driven technologies ensure that companies are armed against all threats, known and unknown; and drive down the cost of ownership. A key tenet of our approach is enhanced visibility into the enterprise: you cannot secure what you cannot see. Improved visibility in the cloud means precise, actionable intelligence as well as more efficient and proactive management of resources - the best competitive edge enterprises require in today's marketplace.

RevBits.com