CHECK POINT

ZERO SECOND PROTECTION TEST REPORT

ONE MINUTE CAN CHANGE EVERYTHING FOR A BUSINESS

What can malware do in 60 seconds? One minute can change everything for a business. The speed of business is all about being responsive to customers and stakeholders. So what happens when the speed of business is overtaken by the speed of malware? Given the unprecedented growth in the number of security threats that focus on stealing data, sabotaging business continuity and damaging a company's reputation, what should organizations do to ensure the speed of malware doesn't disrupt the speed of business? The Check Point team devised a test to quantify that exact question.

BEATING THE SPEED OF MALWARE

Today, with the high speed connectivity that most organizations deploy, malware infection can spread in seconds. The response time to malware has resulted in the coining of popular names such as Zero Day response, meaning that developers have had zero days to fix the flaw. With the speed of malware however, this is not enough. A new response time is needed: Zero Second. Zero Second does not allow malware even one second on your network. In one second, an infected email can propagate to hundreds of hosts.

ZERO SECOND DOESN'T ALLOW MALWARE EVEN ONE SECOND ON YOUR NETWORK

Check Point analysts devised a test to assess how fast security solutions from Check Point, FireEye, Fortinet and Palo Alto Networks respond in stopping malware from entering the organization. They started with an unknown malware they confirmed would be recognized by each vendor's emulation software. They then tested how long it took each vendor's threat emulation to identify the unknown malware. Once identified and a signature defined, they measured how long it took each vendor to propagate the protection so that malware would be blocked in the future. The overall results timeline is shown in Figure 1 below and analyzed in the rest of this report.

WITH CHECK POINT, MALWARE SPENDS ZERO SECONDS ON THE NETWORK

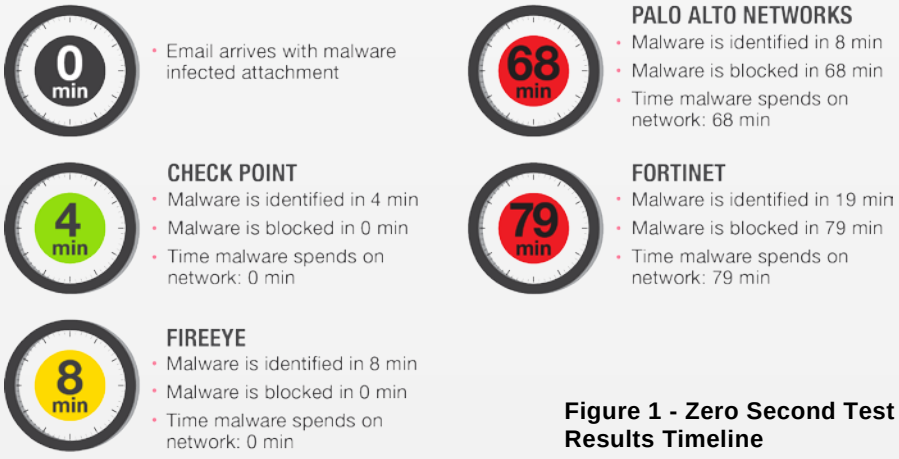


Figure 1 - Zero Second Test Results Timeline

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

ZERO SECOND: EVALUATION USE CASE

A typical situation was simulated to assess how security vendors respond to an infected email. Imagine a scenario where your Human Resources (HR) recruiter receives an email with an infected resume document attached. The test utilized a PDF file infected with a recognizable unknown malware. Once the HR recruiter opens the attachment, it infects their computer immediately. This makes their machine what is commonly referred to in the industry as "patient 0," or the first infected machine in a malware attack. From there the malware can propagate laterally in the network infecting additional computers, servers, storage or other connected devices.

TEST OVERVIEW

Check Point research analysts selected a sample unknown PDF malware that all vendors could detect in their sandbox solution. The objective of this test was not to evaluate catch rate. For that, we recommend you reference Check Point's 2014 Unknown 300 Test Report.

The sample malware was sent to a mailbox inside the network. As each vendor was conducting their threat emulation, the same malware was sent again every sixty seconds to the same mailbox. During the emulation and security gateway update, this repeated transmission approach would reveal how long it takes before the same infected email is blocked.

TESTED VENDORS AND LAB SETUP

Four vendor products were tested in our comparison. The test setup is shown in Figure 2 below.

- Check Point—ThreatCloud™ on 13500 gateway—R77.20
- FireEye—Email Threat Prevention Cloud
- Palo Alto Networks—WildFire Cloud on PA-5020 gateway—PAN-OS 6.0.5
- Fortinet—FortiSandbox Cloud on FG-1500D gateway—FortiOS 5.2.1

To ensure the test validity, platforms were updated and patched with the latest firmware and updates available from each vendor as of October 2014. The test configuration also matched the vendor's best practices. The test's only objective was to evaluate the detection and prevention time for malicious files. Catch rate and performance were not tested and did not influence the test results in any way.

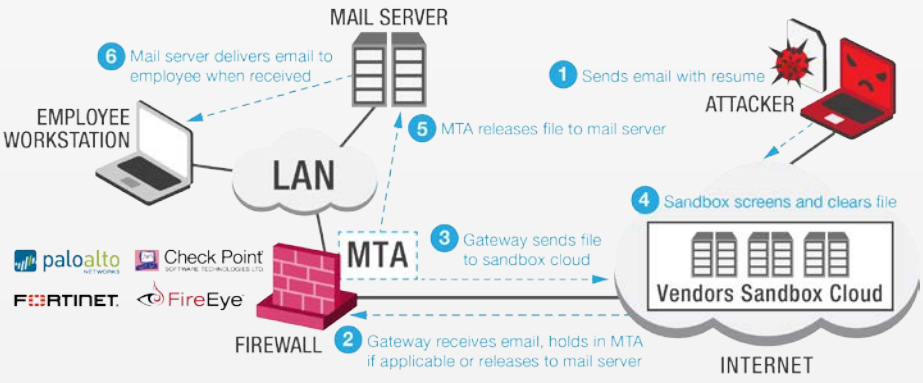


Figure 2 - Zero Second Test Structure

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

TEST RESULTS

The summary results, shown in Table 1, highlight the emulation time for each system and the update time, or time it takes each to emulate and update the gateway to block that malware. The combination is the total time shown in the center column. If the malware is allowed to enter the network during the emulation and update time, it is noted in the network infection risk time. For the sake of completeness, the catch rate results from the Unknown 300 Test are also shown to highlight how each of the tested solutions performed in catching true unknown malware.

PALO ALTO NETWORKS WILDFIRE AND FORTINET ALLOW MALICIOUS FILES TO ENTER THE ORGANIZATION'S NETWORK DURING THE EMULATION AND SIGNATURE UPDATING PROCESS

	Emulation time (minutes)	Signature Creation and Gateway Updating (min)	Total Time to Update Gateway (min)	Total Time Network is at Risk (min)	Unknown 300 Catch Rate
Check Point	4	0	4	0	100%
FireEye	8	0	8	0	70%
Palo Alto Networks	8	60	68	68	62%
Fortinet	19	60	79	79	27%

Table 1 - Zero Second Emulation and Update Time Results

To obtain the emulation time for each system, the Zero Second Test used five (5) recognizable unknown malware files. These files were tested on different days and different times of day to create an average emulation time. This effectively neutralized any influence network conditions might have on the results. The emulation time results of each trial are shown in Table 2 below along with the calculated average emulation time used in Table 1.

PALO ALTO NETWORKS WILDFIRE HAS A 30–60 MINUTES DELAY IN UPDATING ITS GATEWAY SIGNATURES WITH NEWLY DISCOVERED UNKNOWN MALWRE

Emulation time (minutes)	Malware 1	Malware 2	Malware 3	Malware 4	Malware 5	Average
Check Point	4	4	5	3	4	4 minutes
FireEye	8	11	5	7	9	8 minutes
Palo Alto Networks	7	9	12	6	6	8 minutes
Fortinet	13	24	21	17	19	18.8 minutes

Table 2 - Zero Second Evaluation Emulation Times

Once the emulation is complete and the malware is successfully detected, each vendor's system has a time interval needed to create the threat signature for that malware and update the security gateway. Once the gateway is updated, it then begins blocking any new attacks of that same virus signature. As is seen in the Security Findings section, some of the vendor solutions have significant lag times in updating new signatures to their security gateways.

SECURITY FINDINGS

As the Check Point test team conducted the "Zero Second" test, they came across several security findings that are important to consider in the fight against malware. There are two main time intervals that were measured as part of the evaluation:

- Emulation Time—the time needed to identify an incoming file is infected
- Signature Creation and Update Time—the time needed to create a signature of the infected file and update the gateway with the new signature

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

Both of these times are critically important to an organization. For all of the tested systems, the emulation time represents the time it takes to identify a malicious file. The signature creation and update time represents the time it takes to prevent these same threats in the future. The update time interval is especially important to those systems that allow potentially infected files into the network during initial emulation.

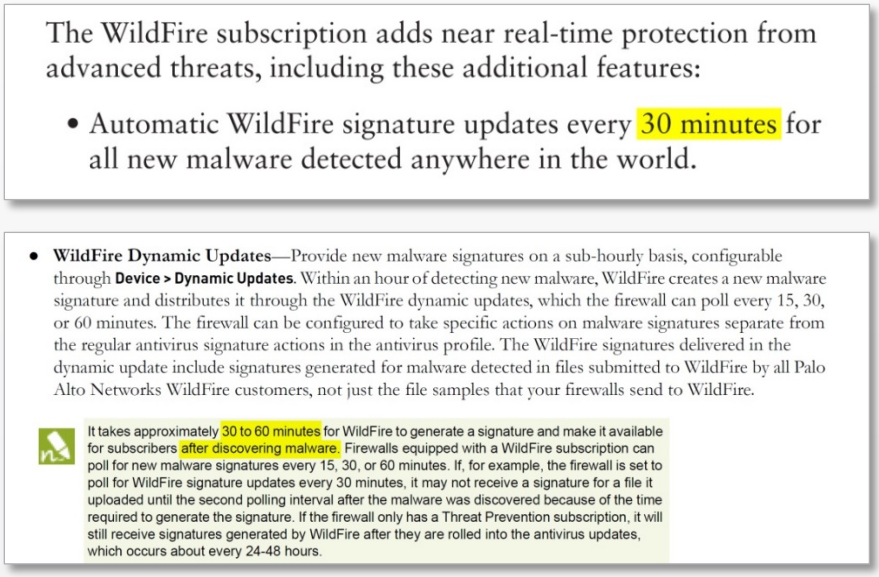
DETECTION VS. PREVENTION

All of the tested systems have a sandboxing or threat emulation capability used to detect the malware. For some, the infected file is passed through to the end recipient while the threat emulation takes place. These vendors assert any delay is unacceptable in business. For others, the file is held until the emulation test is complete before deciding whether or not the file is safe to pass on to the recipient. These vendors would assert that it is much better to invest a few minutes to scan for viruses and prevent them from entering your network than invest hundreds or thousands of labor hours to clean up an infection.

FORTINET'S FORTIGUARD TAKES 78 MINUTES TO START BLOCKING NEWLY DISCOVERED UNKNOWN MALWARE

Of the four tested vendors, Check Point and FireEye both detect and prevent incoming malware before it passes into the network. The Palo Alto Networks WildFire and Fortinet's FortiGuard solutions allow files to enter the organization's network during the emulation and signature updating process, exposing those networks to further damage if the virus is inadvertently launched during that time.

Based on Palo Alto Network's Wildfire product documentation shown in Figure 3 there is a delay of 30–60 minutes needed to update its gateway signatures with recently discovered unknown malware. Based on findings shown later in this report, their tested average for emulation was 8 minutes and the time interval to check for updated signatures is every 15 minutes. This translates into a range of
38–83 minutes before future attacks with that same malware are prevented.



The WildFire subscription adds near real-time protection from advanced threats, including these additional features:

- Automatic WildFire signature updates every 30 minutes for all new malware detected anywhere in the world.

- **WildFire Dynamic Updates**—Provide new malware signatures on a sub-hourly basis, configurable through **Device > Dynamic Updates**. Within an hour of detecting new malware, WildFire creates a new malware signature and distributes it through the WildFire dynamic updates, which the firewall can poll every 15, 30, or 60 minutes. The firewall can be configured to take specific actions on malware signatures separate from the regular antivirus signature actions in the antivirus profile. The WildFire signatures delivered in the dynamic update include signatures generated for malware detected in files submitted to WildFire by all Palo Alto Networks WildFire customers, not just the file samples that your firewalls send to WildFire.

It takes approximately 30 to 60 minutes for WildFire to generate a signature and make it available for subscribers after discovering malware. Firewalls equipped with a WildFire subscription can poll for new malware signatures every 15, 30, or 60 minutes. If, for example, the firewall is set to poll for WildFire signature updates every 30 minutes, it may not receive a signature for a file it uploaded until the second polling interval after the malware was discovered because of the time required to generate the signature. If the firewall only has a Threat Prevention subscription, it will still receive signatures generated by WildFire after they are rolled into the antivirus updates, which occurs about every 24-48 hours.

Figure 3 - Palo Alto Networks WildFire Data Sheet and Admin Guide References

PALO ALTO NETWORKS NEEDS DIFFERENT SUBSCRIPTIONS TO DETECT AND THEN PREVENT MALWARE—SIGNIFICANTLY INCREASING ANNUAL SUBSCRIPTION FEES

In the case of Palo Alto Network's Wildfire, one significant security finding is that one subscription is needed to detect and an additional subscription is needed to prevent. The baseline Wildfire subscription simply emulates and creates the signature of the malware. A second, Threat Prevention subscription, blocks those malware from entering the network. The combination costs an extra 40% of the appliance price for each year of subscription.

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

THE TEST RESULTS SHOWED THAT CHECK POINT WAS ABLE TO IDENTIFY AND UPDATE SIGNATURES IN LESS THAN 4 MINUTES

A security finding on Fortinet is that their solution utilizes an antivirus signature update process to block recently detected unknown malware. The time interval to update new detected signatures on their system is a minimum of 60 minutes after emulation is complete. As seen in the results section, the emulation time in the FortiGuard cloud was the longest, more than 18 minutes on average. The combined total of 78 minutes is a significant amount of time to allow infected files to exist in a network as well as allowing additional receptions of the same infected file to enter.

The Importance of MTA Support

A mail transfer agent (MTA), also called a mail relay, is the ability to proxy email to and from an organization. The MTA is an important security feature because (1) it separates the direct connection to the organization's internal mail server and (2) it offers a location to 'hold' emails—including those with suspected attachments—until they are scanned thoroughly.

FIREEYE AND PALO ALTO NETWORKS TAKE 2X LONGER THAN CHECK POINT TO EMULATE A FILE

A security finding showed that Palo Alto Networks does not support a MTA effectively allowing all unknown malware to traverse the gateway. It also showed that Fortinet requires an added appliance, called FortiMail, to support that security feature. Even with FortiMail, the Fortinet solution lets that first infected email to pass during emulation so it would not prevent 'patient 0' infection.

Archived Files

Many organizations use archived files such as .rar extensions. These files can also be used to mask malware. A security solution must support the inspection of archived files in order to provide full protection. A security finding indicates that Palo Alto Networks could not emulate any archive file extension except zip.

SUMMARY

Every minute counts when it comes to protecting your organization from email attached viruses. The Zero Second Test showed that Check Point leads in detecting and preventing unknown malware at 2x the speed of FireEye, the second place system. Leaving your network exposed for over an hour, the case for Palo Alto Networks and Fortinet is incredibly dangerous.

In the same way that malware can move quickly, so can business. While one approach is to optimize for the speed of business at the expense of security, Check Point provides both speed and security. Waiting twice as long for an email to arrive can mean lots of potential revenue lost. Imagine someone trying to close on a real estate deal, or responding to a tender with a strict deadline, or the announcement from your security vendor that a new threat has been identified with instructions on how to safeguard your network. In all of these situations, minutes count.

What can happen in a minute? Forget Zero Day, hello Zero Second. When it comes to protecting your network, why would you wait one minute longer than you needed to or choose anything other than the best? Check Point is the leader with the industry's fastest threat emulation as well as the industry's best catch rate of unknown malware. If you would like to replicate this test, please contact us at threatprevention@checkpoint.com.

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content