Q1 2020
Advanced Threat Defense
Certification Testing Report

Fortinet, Inc.
Advanced Threat Protection Solution

Tested against these standards
ICSA Labs Advanced Threat Defense Criteria v.1.0
ICSA Labs Advanced Threat Defense - Email Criteria v.1.0

April 13, 2020

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

ICSA Labs tested the Fortinet Advanced Threat Protection Solution (ATP) for 32 days during Q1 2020 to determine how well it detected new and little-known malicious threats. Throughout 4 weeks of near-continuous testing during this quarterly test period, Fortinet’s ATP faced 3,204 total test runs. The result was that the Fortinet ATP successfully met all requirements to maintain two ICSA Labs advanced threat defense (ATD) certifications:

- Standard ICSA Labs Advanced Threat Defense, and
- ICSA Labs Advanced Threat Defense – Email

Fortinet’s solution did well during the test cycle - detecting previously unknown threats and having very few false positives. In fact, during standard ATD testing, Fortinet ATP detected 99.3% of threats with a 0% false positive rate while in ATD-Email testing Fortinet ATP detected 99.8% of threats with only 1 false positive. Figure 1 shows the Fortinet ATP solution’s effectiveness and false positive rates in ICSA Labs’ standard ATD testing. Figure 2 shows the same characteristics in ICSA Labs’ ATD-Email testing.

The Q1 2020 test set was comprised of 821 unique new and little-known malicious threats as well as 806 non-malicious samples. The former was recently harvested malicious threats not detected by traditional security products. The latter were used to test the Fortinet ATP solution in terms of false positives. Security product solutions participating in both standard ATD and ATD-Email testing, like the Fortinet ATD, are tested in the leading ways in which enterprises are being compromised with malware according to data in Verizon’s Data Breach Investigations Report.
Introduction

This is Fortinet’s eighteenth consecutive ICSA Labs Advanced Threat Defense Certification testing report and fourteenth consecutive to include results from ICSA Labs Advanced Threat Defense E-Mail Certification.

All ICSA Labs advanced threat defense (ATD) testing focuses on determining how effectively ATD solutions detect the unknown and little-known threats that more traditional security products miss while minimizing false positives. The remainder of the report presents a more detailed look at how the Fortinet ATP performed during the Q1 2020 test cycle in both ICSA Labs:

- Standard Advanced Threat Defense Certification Testing, and
- Advanced Threat Defense – Email Certification Testing.

ICSA Labs additionally presents data concerning the combined effectiveness of Fortinet’s solution against a collection of malicious threats applicable to and separately seen by both the email security components and the other ATD components of the Fortinet ATP Solution. Finally, to better understand how to interpret the results, this report documents the threat vectors, sample sources, and kinds of samples that ICSA Labs employed for this cycle of ATD testing against the Fortinet ATP Solution.

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 during the test cycle. Below in Figure 3 is information about the test cycle from which this findings report is based.

<table>
<thead>
<tr>
<th>Start Date</th>
<th>January 22, 2020</th>
<th>Days Tested</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Date</td>
<td>February 22, 2020</td>
<td>Test Runs</td>
<td>3,204</td>
</tr>
</tbody>
</table>

Fig. 3 – This Test Cycle

ATD Solution Tested

During this testing cycle, ICSA Labs tested the Advanced Threat Protection (ATP) Solution from Fortinet Inc. The ATP is a multi-component solution. Three ATP components were tested in standard ATD testing while two ATP components were provided for ATD-Email testing. One of the components, the FortiSandbox, was common to both standard ATD and ATD-Email testing. AllFortinet ATP components in the lab along with the corresponding versions tested during this test cycle are listed and described below.

- Components used in ICSA Labs’ standard ATD testing
  - FortiGate 500D: v6.2.3 build 1066
    The FortiGate component’s role in the solution is to stop as many network-borne threats as possible with its threat prevention technologies before submitting remaining objects to FortiSandbox for further analysis. It also serves as a key element to quickly mitigate previously unknown threats that are identified by FortiSandbox.
FortiClient: v6.0 (latest version)

FortiClient runs on endpoint devices including PCs, Macs, smartphones and tablets. Its role is to ensure that all objects that reach the endpoint, on or off the network, are inspected with its threat prevention technologies to block as many identifiable threats as possible – with the option to send the remainder to FortiSandbox for additional analysis – while either holding them before install, or quarantining them as necessary afterwards, based on results. Note that during testing, FortiClient was run on a PC.

- Component used in ICSA Labs’ ATD Email testing
  - FortiMail VM04 – v6.2.2 build 263,191128
    FortiMail is an effective, high performance secure email gateway that applies the threat intelligence of FortiGuard Labs to block spam, malware and advanced threats. It also includes integrated DLP, encryption and archiving for a complete email security solution available as a physical or virtual appliance, SaaS, or managed security service. The FortiMail VM04 used in testing is a virtual appliance aimed at mid-to-large enterprises with up to 3000 users.

- Component in common for both standard ATD and ATD-Email testing
  - FortiSandbox-3000D: v3.1.2 build 0124
    The FortiSandbox uses instrumented VMs (as well as various pre- and post-filters) to run and analyze unknown objects, assign risk ratings and provide threat intelligence to speed response to previously unknown threats. It can obtain those objects directly off the wire, or from file share locations, manual submissions from security staff and other integrated Fortinet devices such as FortiGate, FortiMail, FortiWeb and FortiClient.

For more information about the Fortinet Advanced Threat Protection Solution, its component parts and related information please go to:


### 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 5 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 4 below illustrates the most common malware-related threat vectors that lead to enterprise breaches during 2017 alone (per 2018 DBIR).

![Fig. 4 – Top Threat Vectors Leading to Breaches in 2017 (per 2018 DBIR data)](image-url)
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”, the former being the second most common threat vector leading to enterprise breaches according to the 2018 DBIR.

Detection Effectiveness – Standard ATD

In this section, ICSA Labs presents the Fortinet ATP’s detection effectiveness against all non-email threat vectors mentioned in the “Threat Vectors” section, including web download, web drive-by, and download by malware.

To meet the standard ICSA Labs ATD testing criteria requirements and attain (or retain) certification, advanced threat defense solutions must be at least 75% effective at detecting new and little-known malicious threats. As shown in Figure 6, the Fortinet ATP Solution detected 99.3% of the threats it encountered during standard ATD testing, better than the percentage required for certification.
The next two plots take a deeper dive into the detection provided by Fortinet ATP in ICSA Labs’ standard ATD testing. The plot in Figure 7 sheds light on whether or not the ATP did better or worse – the newer the malicious sample. And as you can see the newness of the sample had little to do with the solution’s effectiveness. In fact, the Fortinet ATP Solution detected 100% of the 168 threats that were less than an hour old.

A final effectiveness-related plot to consider for the Fortinet ATP Solution during standard ATD testing this test cycle is Figure 8 below. Plotted below is each of the 32 days during the test cycle along with how effective the ATP was on each of those days. On all but 5 days during the Q1 2020 test cycle (27 of 32 days), Fortinet ATP detected 100% of the malicious threats it faced.
Detection Effectiveness – ATD Email

In this section, ICSA Labs presents the Fortinet ATP’s detection effectiveness against malicious email threats using the vectors mentioned in the “Threat Vectors” section. In this test cycle the primarily vector for delivering threats was via malicious attachments. The secondary threat vector was emails with malicious URLs.

As with the standard ATD testing, to meet the ICSA Labs ATD-Email testing criteria requirements and attain (or retain) certification, email security solutions must be at least 75% effective at detecting new and little-known malicious threats delivered via typical email threat vectors. As shown in Figure 9, the Fortinet ATP Solution did very well, detecting 99.8% of the malicious email threats it encountered with just 1 false positive in 1,612 total ATD-Email test runs.

![Detection Effectiveness of Fortinet ATP Versus Malicious Email Threats](image)

Effectiveness against Threats Delivered Multiple Ways

In the preceding two sections ICSA Labs presented the effectiveness results, first for standard ATD testing then for ATD-Email testing. Those sections described the solution’s efficacy against 804 malicious test runs in standard ATD testing and 810 malicious test runs in ATD-Email testing.

Used in those tests were 821 unique malicious test samples. Figure 10 below shows that 11 of the 821 were applicable only to standard ATD testing while 17 of the test runs were relevant only to ATD-Email testing.

The remaining 793 malicious samples in the center of Figure 10 were applicable to both and were therefore delivered twice - once via web download and separately as malicious email attachments (or at the other end of a malicious URL).

![821 Unique Malicious Test Runs](image)
One of the benefits of a solution like Fortinet’s that combines both network and email defense is that any email threats are typically held for sandbox analysis and can be stopped unlike network threats that are initially detected but require a more immediate response to further contain any threats and protect the organization’s network.

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 standard ATD and ATD-Email 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 821 unique malicious samples in standard ATD and ATD-Email testing, Figure 11 shows that there were more original samples used and fewer samples that required some kind of modification before use in testing. Of the 710 original samples, 168 were dropped, or left behind by other malware. Figure 12 reveals the source of the 542 malicious samples used in testing that were neither modified nor dropped.
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 13 below. The figure indicates how many malicious threats Fortinet ATP detected and missed from each malware category during testing. In addition, the green line atop Figure 13 represents the effectiveness percentage of Fortinet ATP against original malware belonging to each malware type.

Figures 14 through 17 provide a deeper glimpse into four of the six malware types: ransomware, trojan, spyware, heur, 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 the Fortinet ATP detected and missed across multiple malware families during the test cycle. In addition, the green line atop each figure indicates the effectiveness percentage of Fortinet ATP against original malware from each malware family.
Fig. 15 – Effectiveness against Ransomware Families of Trojans

Fig. 16 – Effectiveness against Families of Spyware

Fig. 17 – Effectiveness against Backdoors
As one would expect from a Fortinet ATP solution that was 99.3% effective overall in standard ATD and 99.8% effective overall in ATD-Email testing during the Q1 2020 test cycle, the solution was very effective at detecting malware across malware types and across malware families.

Prior ATD Reports

Following the 32 days of continuous advanced threat defense testing during the first quarter 2020 test cycle, the Fortinet, Inc. ATP Solution maintained both ICSA Labs’ standard Advanced Threat Defense (ATD) Certification and ICSA Labs Advanced Threat Defense – Email Certification.

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


Successful completion of this test cycle marks Fortinet’s 14th consecutive quarter satisfying the ICSA Labs ATD-Email certification testing criteria and its 18th consecutive quarter having met the ICSA Labs ATD certification testing criteria.

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 five statements below sum up what this ICSA Labs Advanced Threat Defense Certification Testing report should indicate to the reader:

1. ICSA Labs tested the Fortinet ATP 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. The Fortinet ATP Solution demonstrated superb threat detection effectiveness against over 820 unique new and little-known threats.

4. With its ATP Solution, Fortinet provides highly effective, comprehensive defense including excellent recognition of previously unknown email-borne threats with few false positives.
Authority

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

Sebastien Mazas, 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 more than 25 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

Fortinet, Inc.
Fortinet’s mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a leading global provider of network security appliances for carriers, data centers, enterprises and distributed offices. Because of our custom ASICs, hardware systems, network software, management capabilities and security research, we have a large, rapidly growing customer base, including the majority of the Fortune Global 100. Our market position and solution effectiveness has been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond Network Security to help secure the extended enterprise.

www.fortinet.com