Advanced Threat Defense (ATD) Testing Report
Standard ATD and ATD-Email

July 9, 2019

ICSALabs
An Independent Division of Verizon

Test Cycle
Q2 2019
32 Days continuous testing

FortiGate 500D: v6.2.0, build0866 (GA)
FortiClient: v6.0
FortiSandbox-3000D: v3.0.4, build0060
FortiMail VM04 - v6.0.4 (GA)

Threat Vectors

In testing, ICSA Labs delivers malicious threats with the primary threat vectors that lead to enterprise breaches according to Verizon’s Data Breach Investigations Report (DBIR)

STANDARD ATD TEST SET

TEST RUNS: 1223
MALICIOUS SAMPLES: 692
INNOCUOUS APPS: 531

ATD-EMAIL TEST SET

TEST RUNS: 1286
MALICIOUS EMAIL: 756
INNOCUOUS EMAIL: 530

www.icsalabs.com
Advanced Threat Defense (ATD) Test Report
Standard ATD and ATD-Email

Standard ATD Effectiveness

Malicious Threats Detected / Not Detected

Fortinet ATP was nearly 100% effective during the Q2 2019 test cycle, detecting all but 3 malicious threats.

Of 224 threats 4-hours old or less, Fortinet ATP missed just 3.

On 29 of 32 days during the Q2 2019 test cycle Fortinet ATP was 100% effective and always at least 96.3% effective.

Standard ATD False Positives (FPs)

Just 4 innocuous apps were improperly categorized as malicious.

Low Percentage of FPs

www.icsalabs.com
Advanced Threat Defense (ATD) Test Report
Standard ATD and ATD-Email

ATD-Email Effectiveness

Fortinet ATP was nearly 100% effective at blocking malicious threats in email during the Q2 2019 test cycle, detecting all but 3 malicious emails.

Malicious Threats Detected/Not Detected in Email

753
3

ATD-Email False Positives

Fortinet ATP handled all but 2 legitimate, non-malicious email messages properly.

Percentage of FPs

528
2

0.38%

ICSA Labs ATD Certifications Attained by Fortinet ATP Solution

Standard ATD

ATD-Email

Consecutive Test Cycles Successfully Passed ATD:

15

Consecutive Test Cycles Successfully Passed ATD-Email:

11

www.icsalabs.com