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

ICSA labs
An Independent Division of Verizon

January 2, 2019

Solution Tested

FORTINET

Advanced Threat Protection Solution

Components

FortiGate 500D: v6.0.2, build0163 (GA)
FortiClient: v6.0
FortiSandbox-3000D: v3.0.1, build0029
FortiMail VM04 - v6.0.2 (GA)

Test Cycle
Q4 2018

32 Days
continuous testing

Threat Vectors

ICSA Labs delivers malicious threats with the primary threat vectors leading to breaches in enterprises according to Verizon's Data Breach Investigations Report (DBIR)

STANDARD ATD TEST SET

TEST RUNS
1023

MALICIOUS SAMPLES
512

INNOCUOUS APPS
511

ATD-EMAIL TEST SET

TEST RUNS
1110

MALICIOUS EMAIL
544

INNOCUOUS EMAIL
566

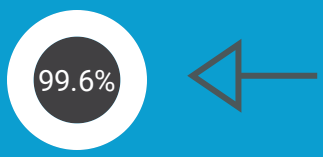
WWW.ICSALABS.COM

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

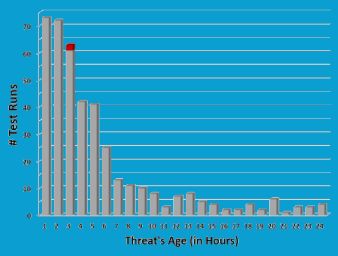
Standard ATD Effectiveness

Malicious Threats Detected / Not Detected

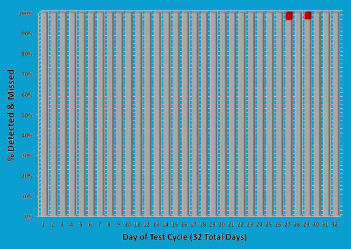
510 2



Fortinet ATP was nearly 100% effective during the Q4 2018 test cycle, detecting all but 2 malicious threats



Of 145 threats 2-hour old or less, Fortinet ATP missed none



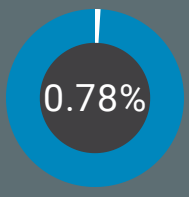
On 30 of 32 days during the Q4 2018 test cycle Fortinet ATP was 100% effective and always at least 96.4% effective

Standard ATD False Positives

Just 4 innocuous apps were improperly categorized as malicious

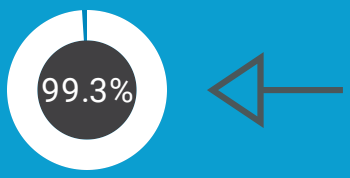
507 4

Low Percentage of FPs



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 Q4 2018 test cycle, detecting all but 4 malicious emails

540 4

Malicious Threats Detected/Not Detected in Email

ATD-Email False Positives

564 2

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

Percentage of FPs

ICSA Labs ATD Certifications
Attained by Fortinet ATP Solution

Standard ATD

ATD-Email

Consecutive Test Cycles Successfully Passed ATD:	Consecutive Test Cycles Successfully Passed ATD-Email:
13	9