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).

**Threat Vectors**

**STANDARD ATD TEST SET**
- Test Runs: 1563
- Malicious Samples: 944
- Innocuous Apps: 619

**ATD-EMAIL TEST SET**
- Test Runs: 1580
- Malicious Email: 948
- Innocuous Email: 632
Standard ATD Effectiveness

Malicious Threats Detected / Not Detected

932

12

98.7%

Fortinet ATP was nearly 100% effective during the Q4 2019 test cycle, detecting all but 12 malicious threats.

Of 484 threats 5-hours old or less, Fortinet ATP missed 10; 4 of the 10 were less than 1-hour old.

On 22 of 33 days during the Q4 2019 test cycle Fortinet ATP was 100% effective and always at least 94.1% effective.

Standard ATD False Positives (FPs)

Just 6 innocuous apps were improperly categorized as malicious.

Low Percentage of FPs

0.97%

613

6
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 2019 test cycle, detecting all but 19 malicious emails.

- Malicious Threats Detected/Not Detected in Email:
  - 929 detected
  - 19 not detected

**ATD-Email False Positives**

- Fortinet ATP handled all but 5 legitimate, non-malicious email messages properly.

- Percentage of FPs:
  - 0.79%

**ICSA Labs ATD Certifications Attained by Fortinet ATP Solution**

- Standard ATD
- ATD-Email

- Consecutive Test Cycles Successfully Passed ATD: 17
- Consecutive Test Cycles Successfully Passed ATD-Email: 13

WWW.ICSALABS.COM