FORTRA

WHITEPAPER (Digital Defense)

# Reduce Security Risk With Multi-Dimensional Endpoint Protection

## Effective Layering of Endpoint Protection To Dramatically Reduce Cost & Dwell Time

Gordon MacKay, EVP/Chief Technology Officer

### About AEP

Advanced Endpoint Protection (AEP), also sometimes referred to as Endpoint Protection Platforms (EPP) is deployed on endpoint devices and designed to:

- Prevent file-based and fileless malware
- Detect and block malicious activity from trusted and untrusted applications

As malware has evolved to bypass traditional signature-based antivirus solutions, vendors have risen to the challenge with detection and protection. These solutions are not cheap. NSS Labs 2019 analysis revealed the average cost of ownership for AEP vendor solutions is $322.00 per agent. But even at that price point, AEP is not a bulletproof solution.

**According to** Accenture's 2019 Global Survey, security breaches increased by 67% in just the past five years[1]. Today's malware has evolved to evade detection. Case in point is the emergence of fileless malware, which uses authorized applications and protocols to perform malicious actions.

These sophisticated programs are difficult to uncover. Even with the most advanced next-generation antivirus, AEP, or advanced Endpoint Detection and Response (EDR) solutions, they are still challenging to detect.

AEP is adept at blocking viruses and even zero-day malware using non-signature-based methods. However, it is vulnerable. This paper discusses some of the shortcomings of AEP and EDR solutions, as well as how to supplement them with powerful threat assessment/detection solutions such as Frontline Active Threat Sweep™ (Frontline ATS™) from Digital Defense. This solution:

- **Enhances Detection for Comprehensive Coverage:** Frontline ATS rapidly determines if endpoints have outdated agents, or ones that have been disabled.
- **Improves Security Effectiveness:** Applies a layered approach to endpoint protection that can effectively reduce the likelihood of malware penetrations.

**Reduces Costs:** Significantly reduces endpoint protection costs by utilizing the least expensive endpoint protection solutions or by leveraging anti-malware solutions which are bundled into the operating systems, and then coupling one of these offerings with agentless cloud malware detection.

**Gartner's November 2018 Market Guide for EDR Solutions[3] indicates attackers are increasingly writing malware which is intelligent enough to disable AEP and EDR agents. In other words, once the malware detonates on the endpoint, the malware seeks out the detection and protection mechanisms and disables them.**

## Calculating The Risk

Calculating risk is about understanding your odds. In a game of blackjack, for example, you have a rough understanding of your odds of winning or losing and those odds remain relatively the same over time. However, in today's cybersecurity fight against hackers, the odds of being infected by malware or a virus steadily increase over time and the stakes continue to get higher.

In blackjack, there is an upfront probability of winning outright with one in twenty-one hands. However, even with a single deck and with solid basic strategy play, the house has a 0.5% winning edge. Similarly, there is a chance that AEP will be enough to thwart a cyberattack, but the odds of that aren't very compelling.

In the Ponemon Institute 2018 State of Endpoint Security Risk report[4], 64% of respondent companies experienced 1 or more endpoint attacks which successfully compromised their assets and/or IT infrastructure over a twelve-month timeframe. To further illustrate the probability of successful endpoint attacks, we will use several statistical data points and some math to explore an organization's security risk.

**1 out of every 99**

emails is a phishing attack[10]

**50.7%** of phishing attacks are malware attacks[6]

Average security effectiveness of AEP runs at roughly **92%**[7]

**3%** phishing penetration[6]

**62.5%** of healthcare security incidents result in a data breach[6]

**28%** of endpoints are unprotected by anti-malware[7]

Average data breach cost in the United States is **$8.19M**[8]

The purpose of this math might be compared to that of the U.S. Military, which uses multi-dimensional warfare (i.e. Land, Sea, Air, Space and Information) during battles, and where the battlespace is viewed as an integrated whole with operations carried out on multiple fronts as a continuum of interrelated activities. In our case we are focused on two primary dimensions – premise and cloud. Since every organization will be at varying levels of maturity[5] with their information security programs, we have elected to calculate risk based on statistics gleaned from studies performed across a wide range of industries and organizations. Regardless of your particular organization's maturity level, the math illus-trates how a multi-dimensional approach to securing endpoints will reduce the risk of a security breach.

To determine the impact of these data points on a large healthcare organization in the United States, let's assume the following:

- **20,000** employees where **10,000** of the employee population has a computer assigned to them for their individual use
- **10,000** of the employee population each receives **100 emails** per day

Based upon the above, the related independent probabilistic math tells us the organization would receive 150 emails per day of infected malware attacks which make it to the endpoints of the organization. Assuming vulnerability to these attacks, this is what an AEP solution is up against each day.

## AEP Effectiveness

To gauge AEP efficacy, we turn to the 2019 NSS Lab comparison report. We see that security effectiveness depends on the vendor, but the average security coverage for vendors in the report is in the range of 92%. Looking at it another way, 8% of attack types would bypass protection.

Now let's take a step back and realize that not all endpoints will be running AEP agents. As previously cited, a study performed by Absolute Software found that 28% of endpoints are unprotected by anti-malware and that 21% were missing anti-malware protection because the agents were outdated or otherwise not working. Since we only have functional AEP coverage on 72% of the endpoints, this equates to 51 instances of malware which infect the endpoints every day in this organization.

This is not quite accurate because we don't know the distribution of malware types within the email, and we assume security effectiveness of 92% uniformly for all malware within the email. In other words, the security effectiveness as described and studied within the NSS Labs report, covers malware types but not the frequency of the types of malware which are received within emails. Therefore, please recognize our math assumptions may be a little aggressive in favor of the attacker. Some malware within emails will be clicked on and followed and the AEP agent will not detect it, nor will it provide protection. The point is, AEP is not 100% effective. Some advanced malware will infect the host and will bypass AEP protection.

Based on the proposed calculations, the organization experiences 51 malware infections per day, or 18,615 infections each year. Since out of these infections, roughly 65.2% result in a data breach, we can project the organization will be subject to at least one successful data breach per year, which will cost approximately $8.12M.

## Reducing Malware Dwell Time

This paper is not arguing that AEP is not required. In fact, we can reduce the probability of infectious incidents using AEP. However some malware will still inevitably get through and we must find ways to detect when this happens as quickly as possible. This is where EDR capabilities come to bear.

It is crucial to reduce the length of time a breach goes undetected (referred to as dwell time) in order to reduce the overall potential cost of a data breach. According to the IBM Security and Ponemon Institute 2019 Cost of a Data Breach report, it takes, on the average, 230 days to detect a data breach due to a malicious attack. This same study establishes that data breaches taking over 200 days to discover are 37% more costly than infections detected in under 200 days.

The problem with agent-based EDR solutions is they suffer from the same gaps we described for AEP. They don't provide 100% coverage and they inevitably fail. A further drawback is, as previously touched on, if malware has detonated on the endpoint, it may have the ability to disable the EDR agent. When this happens the agent-based EDR's detection capabilities are rendered useless, which could account for up to 28% of endpoints that are unprotected by anti-malware[7].

## A Layered Solution

More and more organizations are looking to lower the cost of protecting endpoints. One way to accomplish this objective is to utilize endpoint protection made available as part of operating systems (e.g. Microsoft Defender ATP). However, is the endpoint protection bundled with operating system software good enough? According to an evaluation study performed by MITRE, Microsoft Defender ATP experienced excellent coverage for the most critical, high-impact attack techniques, and was the AEP/EDR tested solution with the fewest misses among all participating vendors[9].

**According to the IBM Security and Ponemon Institute 2019 Cost of a Data Breach report, it takes, on the average, 230 days to detect a data breach due to a malicious attack. This same study establishes that data breaches taking over 200 days to discover are 37% more costly than infections detected in under 200 days.**

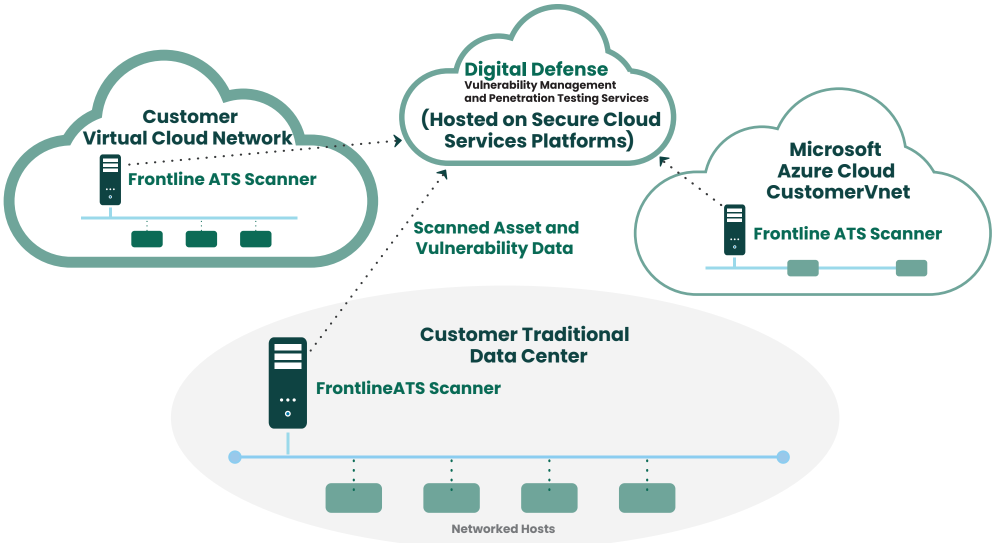
So organizations could go one step further by employing a lower cost agent-based AEP/EDR offering such as Windows Defender ATP and also supplement this type offering with an agentless threat assessment detection using Frontline ATS from Digital Defense to further improve endpoint protection. While there may be overlap between the capabilities of two different EDR offerings, often one will catch what the other misses. By layering Windows Defender ATP with Frontline ATS, one is able to bolster malware detection coverage, while keeping costs down.

Unlike agent-based EDR, Frontline ATS is an agentless network threat assessment and detection technology. It focuses exclusively on compromise detection. Frontline ATS discovers indications of compromise that have eluded other protection systems along with highlighting assets where protection systems have been disabled or are out of date. Frontline ATS is one of four systems currently available on Digital Defense's cloud-native SaaS vulnerability and threat management platform, Frontline.Cloud (See Figure 1).

Because Frontline ATS is agentless, there is very little risk of this type of offering being disabled by infectious malware. At a high level, Frontline ATS detection:

- Invokes a system-level reconnaissance of the file system as well as in-memory auditing to discover suspicious activity (indications of compromise).
- Identifies files which are unsigned. For each unsigned file, it then compares the unsigned file hash to cloud-based file reputation services to see if the file is highly suspicious or totally unknown (which often correlates with binary packing behavior and evasion).
- Uses several techniques to determine the presence of rogue code. Once a binary or process is flagged as potentially suspicious, it will go through the thread-start addresses and characteristics of running processes, comparing them to their reported binary and looking for deltas which would indicated the presence of DLL-injection payloads, which invoke payloads for in-memory only variants.

**FIGURE 1: FRONTLINE.CLOUD NETWORK DIAGRAM**



- Performs process and binary analysis using fuzzy hash logic which compares code sections to what appears to be running in memory, which helps uncover code that was injected, or originally existed in a packed state.

- Detect "living off the land" or LOLBin malware by also looking for PowerShell and scripting processes started with certain suspicious parameters which can indicate scripting-based payloads may be present.

Additionally, Frontline ATS has the ability to pinpoint endpoints with out-of-date or disabled endpoint protection to quickly flag at-risk endpoints. With this feature, Frontline ATS is able to inventory which endpoints have endpoint agents, which ones have them enabled and functioning, and which ones don't have endpoint protection at all.

If we add Frontline ATS into the aforementioned healthcare organization's overall endpoint protection program, we would drastically reduce dwell time per endpoint because it confirms the presence and operability of AEP systems, in this case Microsoft ATP EDR. Frontline ATS also provides an independent cloud-based threat sweeping capability that detects malware that has evaded premise-based defense mechanisms.

Let's take a second look at the math in relation to once we place Microsoft ATP EDR capability as well as Frontline ATS into the mix. In this scenario, we use Microsoft Defender ATP for both of its AEP blocking and EDR alerting capabilities. Based on the analysis carried out by organizations including, but not limited to NSS Labs, we assume the following:

- Microsoft Defender ATP AEP capabilities block 92% of attacks since this is in range of the NSS Labs tested AEP vendors. The math is the same as before and again we have 18,615 infections per year which bypass our AEP solution and infect endpoints in our healthcare company example. This is where we need some EDR capabilities to alert us in a timely manner on the malware that made it through so that we can prevent a data breach.

- Microsoft Defender ATP EDR agents are functioning on 72% of the endpoints.

- Microsoft Defender ATP EDR capabilities are able to detect and alert on 95% of all our attacks.

- Frontline ATS covers all endpoints.

- Frontline ATS has a range of 95% at detecting malware in parallel with the Microsoft Defender ATP.

Each year we have 18,615 infections. Microsoft Defender ATP EDR capability is then able to detect and alert on 12,733 of these instances, leaving 5,882 instances undetected per year. **With Frontline ATS layered into the mix providing full coverage agentless detection, at 95% security effectiveness, the new number of infections that bypass agent-based EDR and ATS together is 294 infections per year – less than 1 infection per day for 10,000 endpoints**. This dramatic reduction in infections results in a much more manageable task for an organization's Threat Hunting team.

## Conclusion

AEP/EDR solutions, when used alone, have a few blind spots, including:

- **Spotty Coverage:** Outdated agents or none at all on a certain number of the organization's endpoints[7].
- **Lower Security Effectiveness:** AEP is not 100% security effective and will miss some malware[2].
- **Increased Malware Risk:** Malware implementers are evolving their techniques and are even implementing features within the malware which are designed to disable AEP/EDR agents.

AEP is required because it does reduce the probability of infection. To further reduce the likelihood of successful cyberattacks, one may employ lower-cost AEP and combined EDR capabilities such as those offered with Microsoft Defender ATP, and supplement these offerings with other agentless threat detection solutions. A complementary solution such as Frontline ATS, a network-based threat sweeping solution, provides the ability to discover malware "slight of hand" against protection systems. Microsoft Defender ATP and Frontline ATS deliver better protection for significantly lower product costs and labor expenses. Lastly by integrating these complementary solutions with Security Orchestration and Automation and Response platforms an organization will realize a powerful Detect-to-Protect automation solution.

**Contact Us**

Sales@digitaldefense.com
For more information visit: www.DigitalDefense.com

## References

1. Accenture Ninth Annual Cost of Cybercrime Study - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

2.NSS Labs 2019 AEP Comparative Report Security Value Report - https://static1.squarespace.comstatic/5229cbf6e4b0dbbcb4a84d 1a/t/5c8 596db71c10b0a7ca15730/1552258779726/nss-labs-aep-comparative- report-security-value-map.pdf

3. Gartner 2018 Market Guide for Endpoint Detection and Response Solutions - https://www.gartner.com/en/documents/3894086/market-guide-for-end point-detection-and-response-solution

4. Ponemon Institute 2018 State of Endpoint Security Risk - https://www.ponemon.org/news-2/82

5. Digital Defense, Inc. Vulnerability Management Maturity Model VM3 - https://www.digitaldefense.com/resources/white-papers/vm3-whitepaper/

6. Verizon 2019 Data Breach Investigations Report - https://enterprise.verizon.com/resources/reports/dbir/

7. Absolute 2019 Endpoint Security Trends Report - https://www.absolute.com/go/study/2019-endpoint-security-trends

8. IBM Security and Ponemon Institute 2019 Cost of Data Breach Report - https://www.ibm.com/security/data-breach

9. MITRE Evaluation Test EDR Vendors - https://techcommunity.microsoft.com/t5/Microsoft-Defender-ATP/MITRE-

10. Avanan 2019 Global Phish Report - https://www.avanan.com/Global-Phish-Report

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.