Post breach

dealing with Advanced Threats

A new challenge emerges

Endpoint security is a key boardroom level concern - as late as November 2015, 71% of C-level IT and security executives have put endpoint at the top of their most vulnerable list[1]. This growing concern is attributed to a new emerging threat from sophisticated attacks, targeting intellectual property and high business impact information. Traditional defenses are rendered ineffective and 70% of security executives are not confident with the security measures they have in place. A new approach is required.

While antimalware software continues its battle to block mass produced crime-driven malware, a new type of more sophisticated, targeted threat emerges. In the wake of outing nation state cyber-weapons such as Stuxnet and Regin, it now seems like hardly a day goes by without news of yet another prominent company or government network being breached. 2,122 confirmed data breaches were reported in 2015 alone, estimated by one source as a 40% YoY increase in targeted attacks against large companies. Nation-state and politically motivated hacker groups (like Strontium), are actively targeting enterprise and government intellectual property and customer records.

This surge is fueled by the difficulties of antimalware suites and vulnerability patching to stop these attacks. Determined attackers easily circumvent malware defenses by avoiding using malware altogether (up to 60% of recorded cases[2]), opting instead to use legitimate operating system (OS) management and pen-testing tools by using simple social engineering methods to trick users to grant them access and privileges and crafted zero-days (0-day), abusing OS and application bugs to breach the network undetected. And the numbers are alarming – the top 5 zero-days of 2014 were actively exploited by attackers for a combined 295 days before patches were available[3]. While on average it took the attackers mere minutes to get in, it took security teams a whopping 221 days on average to discover the breach. An overwhelming 81% of executives surveyed said antimalware solutions are not part of their future for protecting against advanced attacks[4].

As the number of attacks continues to grow year over year, more and more commercial companies are realizing they have been hacked. Where in the past attackers have been targeting only high profile targets, current attacker interest ranges from political to industrial espionage, resulting in companies of all sizes and commercial markets being targeted.

---

[1] promisec Blog: Endpoint Security Infographic

[2] Verizon report: Verizon 2016 Data Breach Investigations Report

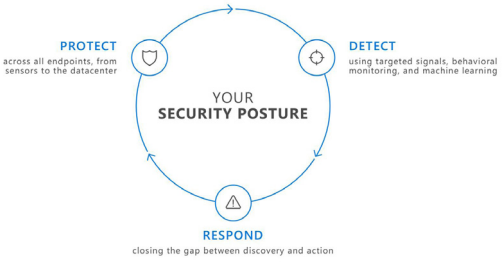
[3] Symantec report: 2016 Symantec Internet Security Threat Report

[4] promisec Blog: Endpoint Security Infographic

The Post-Breach approach

Antimalware endpoint solutions such as Windows Defender focus on a pre-breach approach – acting as the gate keeper, examining incoming files and memory for malicious content and blocking it in real-time. But, as illustrated above, as good as it might be, it is not breach-proof and cannot protect against determined, well-funded, often sophisticated attackers using zero-days, social engineering and non-malicious tools to gain access, privileges and control. A new Post-Breach security solution approach is required to complement pre-breach.

Unlike pre-breach, post-breach assumes a breach has already occurred – acting as a flight recorder and Crime Scene Investigator (CSI). It monitors security events on the endpoint and leverages large scale correlation and anomaly detection algorithms to alert on evidence of an ongoing attack. Post-breach leverages the attacker's need to perform multiple actions after the initial breach, such as performing reconnaissance, hiding and moving across the network to locate high-value assets, and executing information extraction. Post-breach provides security teams the information and toolset needed to identify, investigate, and respond to attacks that otherwise will stay undetected and below the radar. Finally, post-breach closes the loop back to pre-breach antimalware and other prevention capabilities by feeding them with missed signals and samples. As such, it complements the pre-breach security solution stack.



This new post-breach approach is globally recognized, carving a new security market segment, dubbed Endpoint Detection and Response (EDR) by Gartner or Specialized Threat Analysis and Protection (STAP) by IDC. Enterprises are encouraged to complement their endpoint protection threat prevention suite of solutions with more detection and response technologies[5] that focus on non-signature-based threats, and that have the capability to analyze threats seeking to avoid detection through mainstream security technologies[6].

---

[5] Gartner Report: Market Guide for Endpoint Detection and Response Solutions

[6] IDC Study: Worldwide Specialized Threat Analysis and Protection Market Shares, 2014: Rapidly Evolving Security Defenses

Estimated at $3 billion USD by 2019, with CAGR of 27.6%, many security players are currently entering this market, including big security vendors like Symantec and Dell, as well as startups like FireEye, Bit9 and CrowdStrike, with the latter raising more than $100 million USD in 2015 from Google[7]. When asked, 82% of C-level IT executives expressed a need for deeper endpoint analytics capabilities that will help them assist in breach detection and reponse[8].

The Windows Post-Breach Solution

With the release of Windows 10 Anniversary Update, Windows will be releasing its own post-breach solution named Windows Defender Advanced Threat Protection (ATP), to complement the existing endpoint security stack of Windows Defender, SmartScreen, and various OS hardening features. The new service, purposely built to detect and respond to advanced attacks, will be leveraging a combination of a deep behavioral sensor integrated into Windows 10, coupled with a powerful security analytics cloud back-end to enable enterprises to detect, investigate, and respond to targeted and sophisticated advanced attacks on their networks.

Windows Defender ATP will be offering enterprises:

- Advanced attack detection – using behavior-based and anomaly analysis across all enterprise endpoints to generate alerts. Differentiated from others by Microsoft's strong security analytics capabilities and unparalleled optics across its assets – Windows Defender, Bing, IE, and Office 365 that combined provide visibility into more than 1-billion endpoints worldwide.

- Investigation and Response – a security operations console that provides enterprises with an easy way to investigate alerts, proactively explore their network for signs of attacks, perform forensics of specific machines, track attacker actions across machines in the network and get detailed file footprint across the organization.

---

[7] Financial Times: http://www.ft.com/cms/s/0/dd7ba860-2965-11e5-8613-e7aedbb7bdb7.html

[8] promisec Blog: Endpoint Security Infographic

• Threat intelligence - internal and external reports and indicators for known attackers and of prominent attacks (for example Strontium), validated and enriched by an internal team of security black belts (security research lab) and third-party feeds.

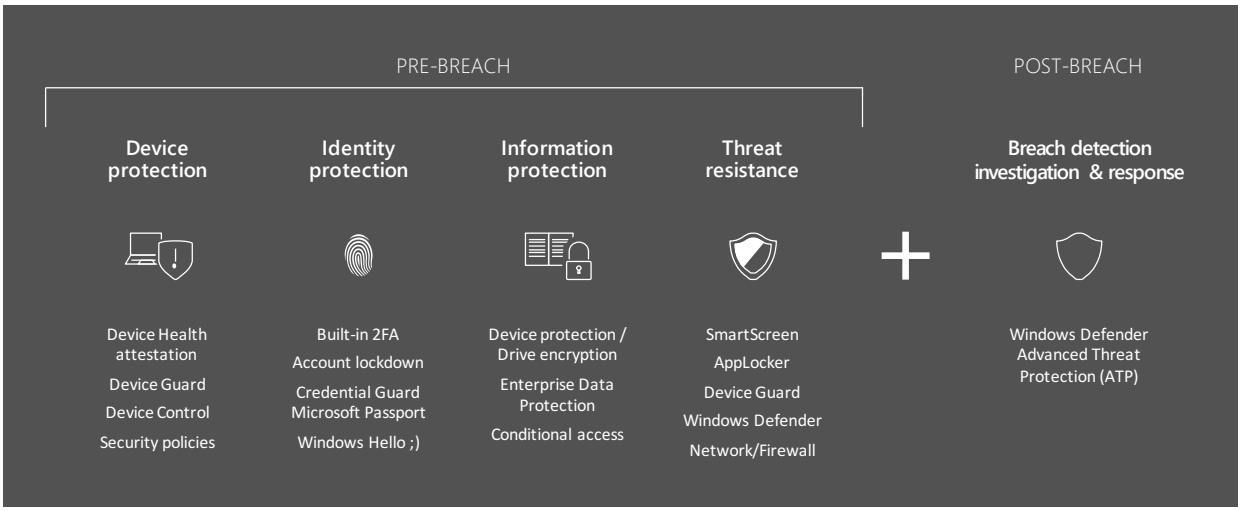


Figure 1: Windows Defender ATP in the context of the pre-breach and post-breach Windows 10 security stack

• Integrated solution – Windows Defender ATP integrates signals from Windows Defender, exposing previously undetected threats and helping organizations prevent them from propagating across the enterprise.

Windows 10 Defense Stack

With the growing threat from more sophisticated targeted attacks, a new post-breach security solution is imperative in securing an increasingly complex network ecosystem. Windows Defender ATP provides a comprehensive post-breach solution to aid security teams in identifying a definitive set of actionable alerts that pre-breach solutions might miss. From device protection through to breach detection, the endpoint security stack that Windows 10 offers, covers the end-to-end endpoint threat protection required to better secure enterprise networks from sophisticated advanced attacks.