Solution Showcase

Morphisec: Advanced Prevention for Endpoint Security

Date: April 2018 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: When it comes to security defenses, CISOs face an ongoing conundrum. Each year, organizations increase their security budgets, buy new types of threat defenses, and add to their layered defense-in-depth architecture. Unfortunately, these investments can result in technology complexity and operational overhead. And despite the presence of incremental security investments, sophisticated attacks often circumvent existing security controls, resulting in costly security incidents and data breaches. What's needed? New types of advanced prevention defenses designed to reduce the attack surface and improve threat detection/prevention efficacy, without creating a security operations burden or disrupting business operations. Morphisec's "moving target defense" is an example of this type of advanced prevention technology for endpoint security.

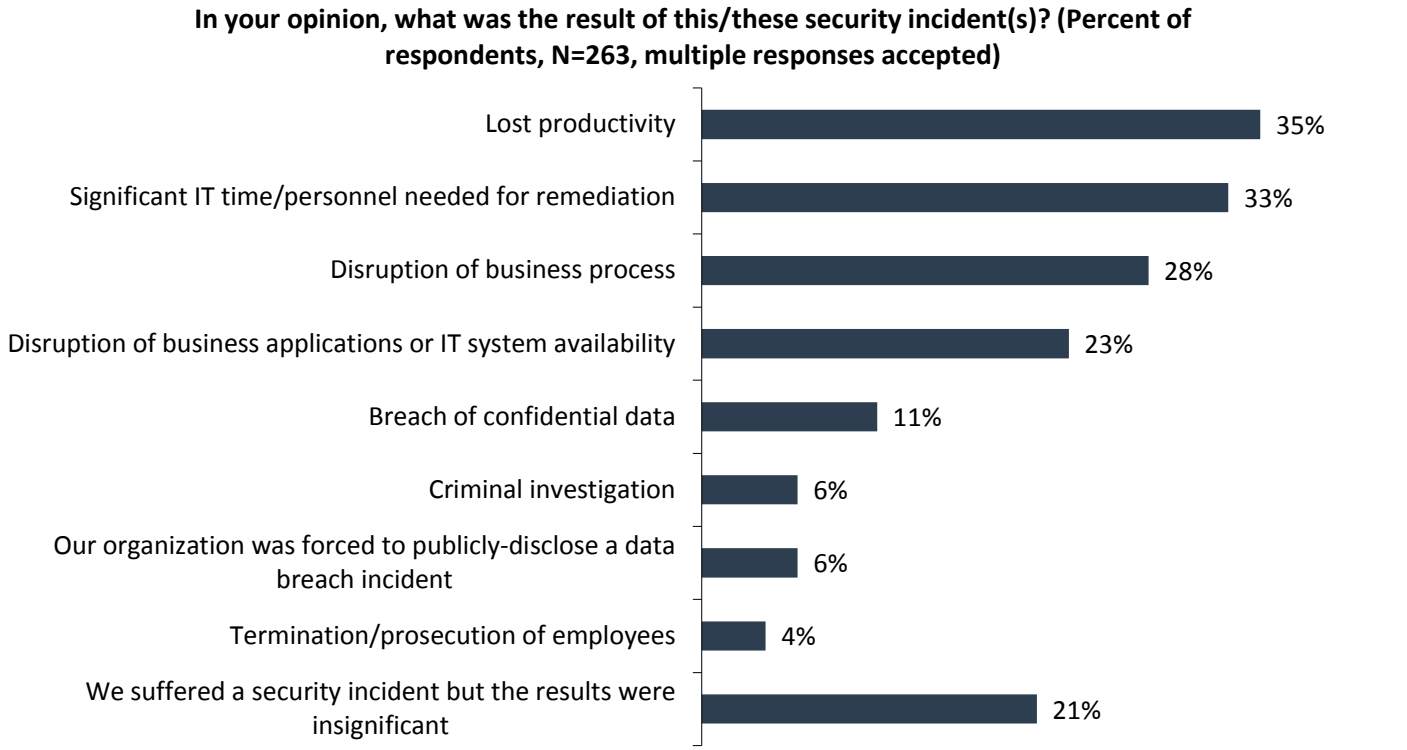
Overview

According to ESG research, 63% of organizations plan to increase spending on cybersecurity personnel, services, and technologies in 2018. Cybersecurity budgets are increasing because:

- Cyber-attacks continue unabated. There were 626 publicly disclosed data breaches reported in 2017, exposing more than 1.9 billion personal records (source: privacyrights.org). Frightened business executives read headlines about waves of cyber-attacks and are more than willing to fund new cybersecurity projects, hoping to avoid becoming the next victim. This leads to increasing cybersecurity budgets and investments in new security tools on an annual basis.
- Cyber-defenses are not working. CISOs have built complex defense-in-depth cyber-defenses over the past 20 years, but skilled attackers are able to bypass security controls, compromise systems, and steal valuable data. This causes organizations to deploy additional security layers, hoping that they've picked the right defenses this time. Recent data from a research report by ESG and the Information Systems Security Association (ISSA) illustrates this point—54% of cybersecurity professionals claim that, despite their security investments, their organization suffered at least one security incident over the past two years (note that 34% of respondents either didn't know if their organization suffered a security incident or preferred not to say). These security incidents can carry steep costs. Of those organizations suffering a security incident, 35% say they lost productivity, 33% claim that the incident required significant IT time/personnel for remediation, and 28% insist that security incidents led to disruption of a business process (see Figure 1).[1]

[1] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals*, November 2017.

Figure 1. Results of Security Incidents



Source: Enterprise Strategy Group

Many organizations find themselves caught in an endless cybersecurity cycle. Reacting to a perpetual wave of cyber-attacks, they increase cybersecurity spending and deploy new security controls on an annual basis. Unfortunately, these defenses are not only ineffective but also make cybersecurity operations increasingly complex. In fact, 72% of organizations believe that security operations are more difficult today than they were two years ago, due to factors like the increasingly dangerous threat landscape, growing volumes of security alerts, and the presence of security monitoring gaps.[2] Regrettably, many CISOs find that more cybersecurity spending leads to more aggravation.

It is also worth noting that many organizations are forced to manage security complexity with security teams that are often understaffed and lacking the right skills. This problem is illustrated by recently published ESG research, as 51% of organizations report a "problematic shortage" of cybersecurity skills in 2018.[3]

It seems clear that the current approach to cybersecurity is not working well. Despite continuing infosec investments, data breaches continue while security complexity increases. Rather than follow this failed approach, CISOs need to take a step back, respond to attacker behavior, and invest in new types of defenses that truly make a difference.

The Rise of Advanced Threat Prevention

While many organizations have invested in new types of threat defenses, there is a fundamental problem—cyber-adversaries are often quite knowledgeable about new types of security tools and layered defenses. This gives hackers a "battlefield advantage"—since they can anticipate typical threat defenses, they use their time and resources to create tactics, techniques, and procedures (TTPs) for circumventing common security controls.

[2] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.
[3] Source: ESG Research Report, *2018 IT Spending Intentions Survey*, February 2018.

To alter the balance of power, ESG suggests new types of security defenses called advanced prevention. Advanced prevention tools use new types of technologies to greatly reduce the attack surface and/or increase the ability to block exploits and malware from penetrating networks and compromising systems. In this way, advanced prevention defenses can:

- **Give the advantage back to defenders.** Advanced prevention defenses often include nuanced or deception technologies into their tools, adding new and unexpected technology hurdles for hackers to overcome. In this way, advanced prevention defenses change basic economics, making cyber-attacks more complex, expensive, and time-consuming. Facing this obstacle, many hackers would rather choose another target than reverse engineer unfamiliar security controls.
- **Offer high efficacy without added complexity or business disruption.** Advanced prevention tools use new types of techniques to greatly reduce the attack surface and improve the efficacy rates for detecting and blocking cyber-attacks. Generally, advanced prevention tools offer these capabilities "out of the box," without the need for custom configuration setting, tuning, or advanced administrator training. In this way, advanced prevention defenses can help improve security efficacy without adding operations overhead or disrupting business processes.
- **Fit into an enterprise security architecture.** Advanced prevention defenses are also non-disruptive because they are meant to complement existing security defenses and analytics tools. For example, advanced prevention defenses can be layered on top of standard endpoint security technologies, providing protection for unknown and zero-day cyber-attacks. When advanced prevention defenses encounter new types of attacks, they can dissect TTPs, collect information, and then share this telemetry with security analytics tools such as SIEM or behavioral analytics systems. In this manner, advanced prevention defenses can play a key role in an enterprise security operations and analytics platform architecture (SOAPA).

Advanced prevention defenses can not only improve prevention and then detection efficacy, but also help streamline security operations by:

- **Reducing security alerts/alarms.** Security professionals commonly complain about the growing volume of security alerts generated by multiple types of threat detection engines. This volume makes it difficult to analyze and prioritize alerts, let alone remediate root cause problems in real time. With their high rate of efficacy, advanced prevention defenses can help organizations reduce the cacophony of security alerts, making it easier to find and fix the root causes of problems in an accelerated timeframe, making detection and response solutions more effective.
- **Decreasing the burden on cybersecurity staff.** Recent ESG/ISSA research reveals that 70% of organizations have been impacted by the global cybersecurity skills shortage. What type of impact? Sixty-three percent of firms claim that the skills shortage has increased the workload on existing security staff, 39% say that the security skills shortage has reduced the amount of time security staff spends with the business, and 38% admit that they've suffered higher rates of employee burnout.[4] Advanced prevention defenses can help here by blocking security attacks at their source. This can reduce the workload and thus free cybersecurity staff to work with business executives to categorize cybersecurity and business risk, add the right controls, and monitor ongoing changes for further risk mitigation actions.

By blocking attacks and reducing cybersecurity noise, advanced prevention defenses can also help bolster business resiliency, maintaining high performance and keeping key IT assets available without disruption. CISOs and business executives will be particularly attracted by this benefit.

[4] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals*, November 2017.

Morphisec for Advanced Prevention

Morphisec, an Israeli-based cybersecurity vendor, delivers advanced prevention defenses for endpoint systems. Morphisec's mission is to take the advantage away from cyber attackers and place it in its customers hands. This is accomplished through something Morphisec calls "moving target defense," a technique that scrambles system memory in order to prevent zero-day/unknown attacks at their early lifecycle stage (before detected and signed by others and before software patches become available). Morphisec does not rely on any prior knowledge of attack techniques, making it an advanced prevention defense against some of the most damaging types of attacks (i.e., WannaCry, Petya, NotPetya, watering hole attacks, etc.).

Simply stated, Morphisec alters the attack surface in a way that is unfamiliar to cyber-adversaries. As a result, common attacks can't execute and are then blocked by default. When cyber-adversaries resort to sophisticated system scanning, and probing activities, they are easily detected and monitored, with TTP telemetry shared with security analytics systems.

Morphisec also qualifies as an advanced prevention defense because it only requires that a small agent be installed on all endpoints, with no further configuration or customization. Organizations can then rely on the combination of traditional endpoint security software for detecting/blocking known attacks and Morphisec for detecting/blocking previously unknown attacks. Other complex endpoint security agents/tools can then be removed from systems, reducing complexity and performance issues.

As described above, Morphisec can improve security efficacy while streamlining security operations by reducing security alert volumes and freeing up staff to focus on more pressing strategic initiatives. Morphisec will also help organizations greatly reduce the number of systems requiring expensive and disruptive system reimaging due to system compromises. Moving target defense also blocks exploitation against software vulnerabilities, helping organizations better manage software patching cycles. Finally, Morphisec's lightweight agent simply blocks attacks without requiring a lot of system resources. This safeguards systems while maintaining high availability, performance, and user productivity. CISOs will especially appreciate this contribution toward business resiliency.

The Bigger Truth

While organizations are willingly increasing cybersecurity spending, CISOs still face a difficult challenge in choosing the right security defenses that can improve threat defense efficacy without adding complexity or operational overhead. Given the global cybersecurity skills shortage, few organizations have the luxury of giving the cybersecurity staff more things to do, so CISOs must choose wisely or they can create more problems than they solve.

ESG believes this situation creates a pressing need for advanced prevention defenses, as these types of tools are designed to provide turnkey solutions that can simply and effectively reduce the attack without adding to the already overwhelming cybersecurity operations burden.

Many vendors promise advanced prevention but CISOs should carefully research and evaluate solutions, ensuring that they actually can deliver maximum results with minimal efforts. Those organizations looking to improve endpoint security in this way should consider Morphisec and its "moving target defense."