Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **April 2019**
Sponsored by **Trend Micro**

The Critical Role of Endpoint Detection and Response

Executive Summary

Security professionals, business decision makers, boards of directors, regulators and others are increasingly concerned about cybersecurity issues and the potential for major business disruptions like data breaches, various types of security incursions, and other problems.

And they're right to be concerned: estimates of the costs of cybercrime vary from a low of roughly $600 billion[i] to several trillion dollars annually[ii]. Ransomware can shut down an organization's operations for an extended period and cost millions of dollars to remediate – and these threats are becoming more sophisticated and more evasive. Nearly eight in 10 successful attacks in 2017 involved fileless malware[iii], which can evade prevention defenses like antivirus.

Moreover, despite the enormous sums spent on security solutions each year, the problems are not getting better or are actually getting worse for many organizations. For example, an Osterman Research survey conducted in October 2018 found that CEO Fraud/Business Email Compromise (BEC) attacks are either remaining static or getting worse for 53 percent of organizations – for ransomware that figure is 56 percent[iv]. Major organizations have been recent victims of high-profile ransomware attacks, including the City of Atlanta[v], A.P. Moller-Maersk[vi], and Norsk Hydro[vii].

Conventional security solutions are useful and provide some level of protection. The variety of antivirus solutions, firewalls, secure web gateways, security incident and event management (SIEM) solutions, anti-ransomware solutions, cloud security tools and other systems provide protection against many threats. However, Osterman Research surveys, as well as those of many other analyst firms, find that the current level of protection is simply not adequate in many cases due to improving evasion tactics, end users who work outside of perimeter defenses (e.g., from airports, coffee shops or at home), infected USBs, fileless attacks, etc.

Despite the enormous sums spent on security solutions each year, the problems are not getting better or are actually getting worse for many organizations.

ORGANIZATIONS ARE TURNING TO EDR

To address these deficiencies, a rapidly growing number of organizations are deploying endpoint detection and response (EDR) solutions as a supplement to their existing security defenses. EDR solutions offer several important benefits:

- Continuous monitoring of the wide range of endpoints on or off corporate networks. This enables organizations to monitor not only malicious attacks from external sources, such as advanced persistent threats (APTs) that might result in data breaches; but also to keep tabs on anomalous activity from inside the organization, such as cryptomining or data theft from departing employees.

- Recording of the enormous volumes of activity that take place on the network in a way that other tools, such as SIEMs and endpoint protection platforms (EPP), typically don't or don't do as well.

- Leveraging artificial intelligence to continuously monitor systems for malicious activity to attempt to stop attacks before and as they execute.

- Integrating with advanced features such as sandboxing to look for sleeping threats.

- Enabling proactive hunting for indicators of attack to see things that have not yet been detected.

- Analysis capabilities that can enable security analysts, threat hunters and others to more quickly evaluate and block follow-on attacks. These include sweeping for indicators of compromise to see if others in an organization were infected, proactively hunting for indicators of attack, and determining the root cause of an incident and enabling protections against it.

- Remediating the changes caused by executed attacks with the ability to roll back endpoints to a previously known clean state.

- Creating granular policies to handle USB devices in order to block unknown and potentially malicious USB keys.

- Enabling protections for remote employees who can't rely on perimeter defenses.

Moreover, EDR solutions can provide business benefits by satisfying regulators, compliance staff, customers and others that an organization that deploys an EDR solution takes its security posture seriously. An EDR solution can demonstrate that threats will be monitored closely, highly detailed information about endpoint events will be retained for an appropriate length of time, and remediation of security threats will occur as quickly as possible.

In short, the increasing use of EDR represents the need to build upon and enhance the foundation of traditional antivirus and EPP solutions by working alongside them to provide better protection, reporting and other advanced capabilities.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Trend Micro; information about the company is provided at the end of this paper.

Security Problems are Getting Worse

ATTACKS CAN BYPASS PERIMETER DEFENSES

Improved perimeter defenses like email security, firewalls and EPP solutions have motivated threat actors to find new ways to reach endpoints in order to maximize damage while minimizing detection. For example, the NSS Labs 2018 Next-Generation Firewall Comparative Report[viii] found that three in five of the firewalls tested failed at least one evasion test, and one-half did not block attacks that came through non-standard ports; the 2019 SonicWall Threat Report[ix] found that in a sample of 700 million malware attacks, 19 percent came through non-standard ports. Moreover, threat actors are increasingly using methods like encryption to penetrate organizations that don't inspect encrypted traffic, as well as updating existing malware variants to bypass static filters.

THE ATTACK SURFACE HAS SHIFTED

Fifteen years ago, most organizations had on-premises infrastructure and very little else in the context of their computing environment. They operated an on-premises email system and other business-critical applications using in-house servers managed by their internal IT staff members, and operated primarily desktop computers and company-owned laptops. Moreover, the comparatively few employees who had mobile devices – in an era before smartphones – had them supplied by their employer, and most of their data and computing assets were kept behind a relatively defensible perimeter that could be protected reasonably well using a conventional security infrastructure.

Fast forward to today and the situation has changed dramatically:

- The vast majority of organizations are operating a wide range of cloud services within hybrid environments for mission-critical and non-mission-critical purposes. For example, one source estimates that there are nearly 1,200 cloud services in use in the typical large enterprise and that the vast majority of these are not "enterprise-ready"[x].

- Mobile devices – many of which are owned and controlled by employees – are commonly used to access corporate data resources and sensitive data assets.

The increasing use of EDR represents the need to build upon and enhance the foundation of traditional antivirus and EPP solutions.

These devices typically contain a large number of apps, many of which can be exploited to steal login credentials and other sensitive information.

- IoT devices are becoming commonplace and the number of these devices in use is skyrocketing.

- Employees continue to use conventional endpoint devices like desktop and laptop computers.

- The "Bring Your Own" trend has expanded from personally-owned and managed devices (BYOD) to personally-owned and managed cloud, mobile and desktop/laptop applications of many types.

In short, today's modern network comes with an expanded attack surface. There is no longer a defensible perimeter that can fully protect corporate data.

BAD ACTORS HAVE BECOME MORE SOPHISTICATED

A key reason for the success of cybercrime is that cybercriminals are well funded (often because they are enabled by organized crime), have the technical resources needed to create new and ever more capable attack methods, and tend to collaborate with one another to share new techniques and processes. For example, a study by Bromium found that the most successful cybercriminals can make up to $2 million annually, and even beginners and hobbyists can generate an income of $42,000 annually[xi]. Cybercriminals can generate individual earnings that are up to 15 percent higher than traditional crimes[xii]. Moreover, laundered funds from cybercriminal activity are estimated at up to $200 billion per year[xiii]. In short, money is a key motivator for virtually any activity and cybercrime is no exception.

The result has been that cybercriminals have been able to develop new and ever more sophisticated techniques to penetrate corporate defenses. This has led to new penetration techniques, fileless malware, and an increased emphasis on compromising credentials and account takeover.

Today's modern network comes with an expanded attack surface. There is no longer a defensible perimeter that can fully protect corporate data.

THE CONSEQUENCES OF SECURITY LAPSES HAVE BECOME MORE SEVERE

While security breaches have always carried with them serious financial, reputational and other consequences, regulations like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), among many others, have made the consequences of security problems much more severe. For example, if a bad actor is able to penetrate the defenses of a company that has not properly protected its sensitive corporate data, such as Personally Identifiable Information (PII) or Protected Health Information (PHI), the company can face enormous financial penalties. Moreover, new privacy regulations and individual requirements within them (such as Article 33 of the GDPR) require reporting of a data breach within 72 hours. Organizations that do not have the ability to detect that they have been breached – let alone understand the cause of the breach and how to remediate it – can run afoul of regulations that require rapid response to breaches and other security issues.

THE SKILLS SHORTAGE IS COMPOUNDING THE PROBLEM

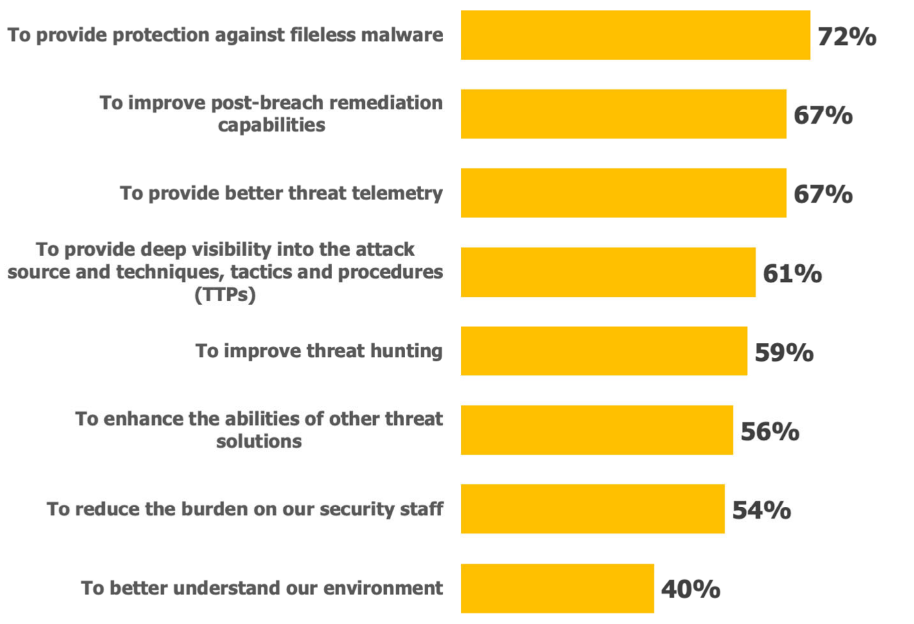
The very well-publicized cybersecurity skills shortage is compounding these problems. Because many organizations cannot find or afford a sufficient number of highly skilled security analysts and other security staff members, they often will not have the resources necessary to investigate, analyze and remediate security alerts and the various threats they encounter.

The Problems that EDR Solves

WHY ARE ORGANIZATIONS DEPLOYING EDR?

The market for EDR solutions is growing at a rapid pace, from $238 million in 2015 to $1.54 billion in 2020[xiv]. The rapid growth of the EDR market, particularly with regard to the more mature and slower growing EPP market, can be attributed to the variety of benefits that EDR solutions offer, as discussed above. However, our research found that the most important reasons for deploying an EDR solution are its ability to protect against fileless malware, the ability to improve post-breach remediation capabilities, and their ability to provide improved threat telemetry over conventional security solutions, as shown in Figure 1.

Figure 1
Reasons for Deploying an EDR Solution
Percentage responding "important" or "extremely important"



Source: Osterman Research, Inc.

The market for EDR solutions is growing at a rapid pace.

WHAT IS EDR?

Endpoint Threat Detection and Response (later shortened to Endpoint Detection and Response) was a moniker originally coined by a Gartner analyst in a July 2013 blog post[xv]. The analyst's blog, as well as a Gartner report that was published 16 months later, framed EDR as follows:

- "...tools primarily focused on detecting and investigating suspicious activities (and traces of such) other problems on hosts/endpoints."
- Tools that are focused on "...the endpoint (as opposed to the network), threats (as opposed to just malware and officially declared incidents) and tools' primary usage for both detection and incident response."
- "These tools record many detailed endpoint and network events, and store this information in a centralized database for deep detection, analysis, investigation reporting and alerting. Analytic tools are used to continually search the database to identify the tasks that can improve the security state to deflect common

> attacks, to provide early identification of ongoing attacks (including insider threats), and to more rapidly respond to detected attacks."

In short, EDR solutions continuously monitor, record and analyze all activities and events on the endpoint. While traditional EPP solutions will allow or block a specific activity based on signatures or identification of suspicious activity, EDR provides *continuous* monitoring and the ability to record and store information on endpoint activities for purposes of conducting investigations and future analysis. The analytics capabilities are an essential element of EDR solutions, since they help security researchers, security analysts and threat hunters to understand what has gone wrong and how to prevent future threats.

Although EDR is, for all intents and purposes, a post-breach solution in that it analyzes attacks that have already occurred (or have been attempted), it can also be used proactively to analyze threats and sources for their future propensity to attack. The ultimate goal of EDR is not only to detect and address threats, but to proactively look for them. At the same time, some vendors attempt to complement their EDR tracking and visibility capabilities with, so called, "last line of defense" features aimed at blocking post-breach damage.

THE PROBLEMS EDR SOLVES

EDR solutions build upon the capabilities of conventional security solutions:

- **Lack of post-breach threat detection**
  Despite the ability of many EPP solutions to detect threats, they typically cannot detect incursions when they occur as well as EDR solutions because of the evolving sophistication of threat actors. In fact, many bad actors are able to penetrate networks undetected and remain undetected for substantial lengths of time while they search for and exfiltrate corporate data assets. The length of time that cybercriminals have between their initial incursion and when they're detected – known as dwell time – has decreased substantially over the past several years. For example, FireEye Mandiant reports that the average dwell time has gone from 416 days in 2011 to 78 days in 2018, while the proportion of investigations in which dwell times were longer than 700 days has gone from 21 percent of the total in 2017 to just 12 percent in 2018[xvi]. While the trendline of decreasing dwell time is certainly good news, it's important to keep in mind that 78 days for a bad actor to hunt around a corporate network is still a very long time, and that many terabytes of sensitive data can be downloaded during that period.

  Part-and-parcel with the lack of post-breach threat detection for many current security solutions is that many lack of any kind of alerting that something suspicious has occurred. Because bad actors study and can evade existing antivirus and whitelisting prevention in place, they can command and control a compromised asset without raising suspicion. While some organizations are flooded with alerts and will sometimes ignore or fail to act upon them properly (as in the case of Target in their well-publicized data breach in 2013[xvii]), alerts based on static indicators of compromise may never be triggered by a sophisticated attacker. The key problem to address is surfacing critical alerts in a way that organizations that enables security teams to understand the problem and prioritize next steps.

EDR solutions build upon the capabilities of conventional security solutions.

- **Lack of deep visibility and analysis capability**
  With many conventional solutions, security analysts will often lack the information they need to understand how a breach occurred or how to prevent it in the future, and they often lack the ability to analyze threats and conduct thorough investigations. The result is long remediation times for many threats because researchers don't have all of the tools they need to understand the root cause, how the problems occurred, who has been impacted, what needs to be done, and so forth. With many conventional security solutions a sufficient amount of information on endpoint activity is not recorded, the information that

is captured is not stored or appropriately accessible, and analysis tools are lacking. SIEMs address these shortcomings to some extent, but not as extensively as EDR solutions. EDR solutions address this lack of deep visibility by providing auditing and threat hunting capabilities, as well as a deeper understanding of attackers' tactics, techniques and procedures.

EDR solutions address each of these problems by:

- Continuously monitoring all endpoint activities to detect targeted and sophisticated threats like APTs, lateral movement within networks, use of stolen credentials, unusual insider activity, and various other – and often subtle – anomalies and activities perpetrated by attackers.

- Recording all events that take place on endpoints and across the network to provide a comprehensive dataset for purposes of further investigation and remediation.

- Providing the ability to analyze events to aid security researchers, security analysts, threat hunters and others as they investigate and remediate security incidents.

Moreover, EDR solutions address not only the technical issues involved with monitoring and analyzing threats, but they also provide business benefits, as well. These include the ability to satisfy regulators, boards of directors, customers, business partners, vendors and others that an organization with a properly managed EDR solution is serious about addressing data security, as well as remediating security breaches as quickly as possible.

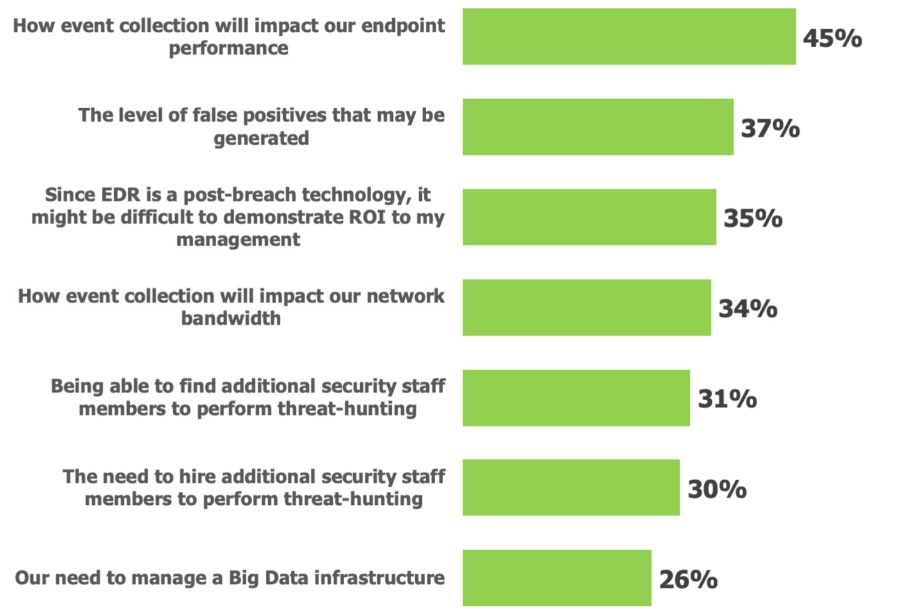
Issues to Consider

It's important to note that an EDR solution cannot be viewed as merely a simple solution that is added to a security infrastructure and can then be left to do its work unmanaged. While EDR solutions can use automation to some extent, they require investments in security labor to make full use of their features and functions.

While EDR solutions can use automation to some extent, they require investments in security labor to make full use of their features and functions.

Consequently, our research found that many of those most familiar with EDR solutions are concerned about a number of issues with regard to the EDR solutions themselves. For example, as shown in Figure 2, the most serious concern – noted by 45 percent of those surveyed – is how the event collection process will impact the performance of endpoints on the network. Also of concern are the potential generation of false positives, difficulties in demonstrating the return-on-investment (ROI) of EDR solutions, and potential impacts of EDR solutions on network bandwidth.

Figure 2
Concerns About EDR Solutions
Percentage responding "concerned" or "extremely concerned"



Source: Osterman Research, Inc.

Some Best Practices to Consider

It's important to consider that an EDR solution is not a replacement for most elements of an existing security infrastructure, but a supplement that will provide improved monitoring, insight and forensics capabilities. Osterman Research recommends a number of practices to consider in the context of evaluating and deploying an EDR solution:

SECURITY AWARENESS TRAINING

While not ostensibly an element of an EDR solution, security awareness training should be an important consideration in any security plan because users are the means by which many attacks occur. Bad actors will often attack networks by first attacking the weakest part of an endpoint – their users. Well trained users will be less susceptible to social engineering, phishing, spearphishing, BEC and other cybercriminal practices, thereby enhancing overall security and reducing the likelihood that an attack will be successful. It's important to note that security awareness training by itself will address only part of an organization's security gaps, but it is an important element.

GIVE EDR THE ATTENTION IT DESERVES

It is essential to give an EDR solution the attention that it deserves in the overall context of the security infrastructure. An EDR solution is not a "set-it-and-forget-it" technology, but instead must be integrated into the existing and future security infrastructure, and it must be given the labor and other resources necessary to make it effective. For example, an EDR solution will generate voluminous amounts of data that security researchers can use to understand threats, perform root cause analysis, and so forth. An organization needs the appropriate level of security staffing and expertise to ensure that the EDR solution provides the value for which it was implemented.

It is essential to give an EDR solution the attention that it deserves in the overall context of the security infrastructure.

CONSIDER MANAGED SOLUTIONS

Related to the point above, decision makers who are considering the deployment of an EDR solution should ask themselves a few key questions:

- Do we have the internal resources and skill sets necessary to prevent things like attacks, infections, data exfiltrations, malicious encryption, etc.?
- Do we have the necessary budget?
- Even if we have the budget, will we be able to find skilled employees?

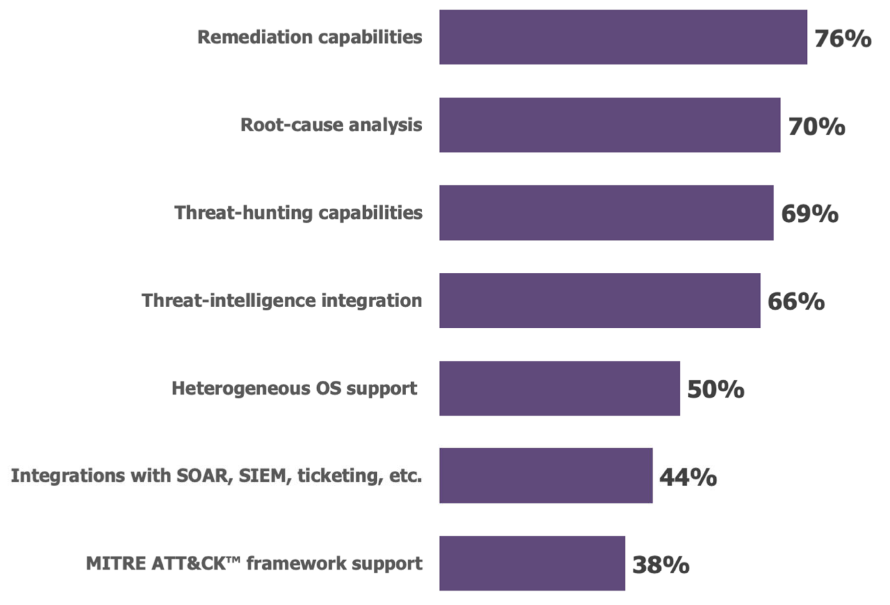
Organizations without the necessary internal resources to support an EDR solution fully may want to consider the use of a managed EDR provider (aka MDR), particularly when considering time- and expertise-consuming tasks like root cause analysis. If a managed EDR provider will be considered, it's important to understand how the provider will process and protect sensitive security data, the bandwidth requirements necessary to send enormous volumes of data to a third-party provider's data center, privacy issues that might come into play, regulatory obligations that must be satisfied, and so forth.

WHAT ORGANIZATIONS VALUE IN AN EDR SOLUTION

EDR solutions are being deployed for a number of reasons. As shown in Figure 3, the primary reason for deploying an EDR solution – cited by 76 percent of those surveyed – is to provide remediation capabilities. Also important are the ability to perform root-cause analysis, threat-hunting capabilities, and integration with threat-intelligence solutions.

EDR solutions are being deployed for a number of reasons.

Figure 3
Importance of Various EDR Capabilities
Percentage responding "important" or "extremely important"



Source: Osterman Research, Inc.

KEY QUESTIONS TO ASK

Osterman Research recommends that prospective EDR vendors be asked a number of questions about their offerings, services and the like:

- How complete is the data collection? Does it include all relevant data on the endpoints that may have been involved in an attack, the root causes of the problems, how malicious processes started, and all of the assets that may have been involved?
- How much data will be generated by the EDR solution? What impact will this have on storage requirements? If a managed EDR provider is used, what impact will data volumes from the EDR solution have on network bandwidth?
- To what extent is the threat detection and data analytics process automated? Can it help to prioritize alerts?
- How easy is it to whitelist/blacklist applications?
- What are the additional staffing requirements to deploy and manage the solution on an ongoing basis?
- What future-proofing capabilities does it have for when attacks on processors becomes a reality?
- Are multiple detection technologies used to improve the efficacy of the solution?
- To what extent does the solution generate false positives?
- Does the solution have real-time access to various sources of threat intelligence? What sources of threat intelligence can be used today and in the future?
- Does the solution provide visibility across all endpoints on the network?
- Can you block access to known malicious IP addresses, domains, and URLs?
- What workflow capabilities are available to manage response and remediation activities?
- What response capabilities are available when a threat is detected: user deactivation, network isolation, process isolation, threat blocking?
- What is the vendor’s roadmap in the EDR space?
- How well does the vendor’s EDR solution integrate with other security solutions (e.g., Firewalls, SIEMs)?
- Can you enforce the use of the EDR client if someone is trying to access the internet behind or corporate firewall?
- Can you easily deploy MITM TLS certificate roots to endpoints through the client?
- Does the vendor take a “next-generation EDR” approach and utilize new approaches to preventing threats, such as understanding known, good behavior and blocking activities that do not match?
- Can the vendor’s EDR solution work in an air-gapped environment (if needed)? Can the solution be deployed both on-premises and in the cloud?
- Can you create granular policies to manage known and unknown USB devices?

Osterman Research recommends that prospective EDR vendors be asked a number of questions about their offerings.

Summary

While conventional security solutions are important and useful at preventing a variety of threats, EDR solutions can provide additional capabilities that can significantly improve an organization's security defenses. By continuously monitoring all endpoint activity, retaining this data, and providing robust analytics capabilities, EDR solutions provide protection in a way that conventional security solutions do not.

Sponsor of This White Paper

Trend Micro, a global leader in cybersecurity, is passionate about making the world safe for exchanging digital information, today and in the future. Artfully applying our XGen™ security strategy, our innovative solutions for consumers, businesses, and governments deliver connected security for data centers, cloud workloads, networks, and endpoints. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

With over 6,500 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. www.trendmicro.com.

TREND MICRO™

www.trendmicro.com

@TrendMicro

+1 888 762 8736

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

[i] https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html

[ii] https://securityaffairs.co/wordpress/50680/cyber-crime/global-cost-of-cybercrime.html

[iii] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

[iv] Source: *Addressing the Top 10 Security Issues Organizations Face*

[v] https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[vi] https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#7aef522d4f9a

[vii] https://www.wsj.com/articles/norsk-hydro-repairs-systems-and-investigates-after-ransomware-attack-11554852893

[viii] https://www.sonicwall.com/resources/analyst-report/2018-nss-labs-next-generation-firewall-comparative-report-security/

[ix] https://www.sonicwall.com/lp/2019-cyber-threat-report-lp/

[x] Source: Netskope Cloud Report, Winter 2018

[xi] https://www.infosecurity-magazine.com/news/cybercriminals-earn-millions/

[xii] https://www.thesslstore.com/blog/2018-cybercrime-statistics/

[xiii] https://www.darkreading.com/attacks-breaches/cybercriminals-launder-up-to-$200b-in-profit-per-year/d/d-id/1331298

[xiv] https://www.statista.com/statistics/799060/worldwide-edr-epp-market-size/

[xv] https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/

[xvi] Source: M-Trends 2019

[xvii] https://www.darkreading.com/attacks-and-breaches/target-ignored-data-breach-alarms/d/d-id/1127712