LightReading SECURITY NOW

Sponsored by

IBM Security

SECURITY NOW SPECIAL REPORT

ENDPOINT ECOSYSTEMS - COLLABORATING TO CONQUER SECURITY THREATS

IBM BigFix

Predators are ready to strike your most vulnerable position.

You may not see them, but they're out there: a network of predators collaborating to identify any sign of weakness you may have. Because weakness is opportunity. IBM BigFix® can help you integrate your tools, teams and processes to create a collaborative endpoint management and security ecosystem. We'll eliminate vulnerabilities to ensure you wage a synchronized, streamlined defense against unscrupulous attackers who are intent on taking you down.

© Copyright IBM Corporation 2018. IBM, the IBM logo, ibm.com and BigFix are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.

TABLE OF CONTENTS

3

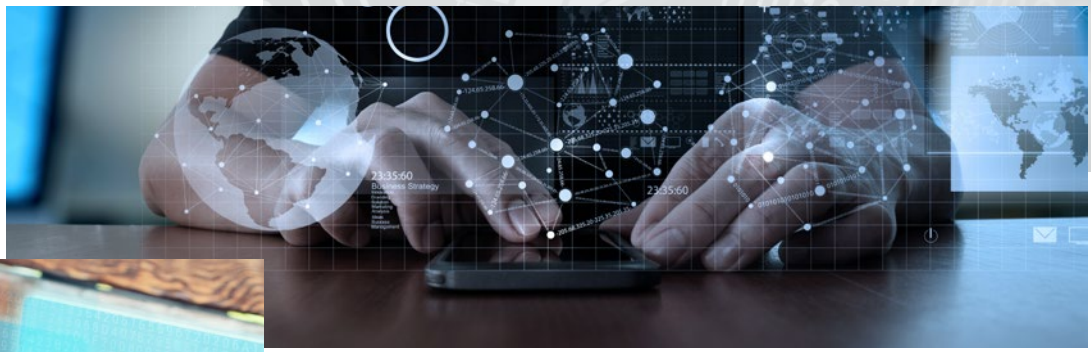
EDITORIAL FORWARD - ENDPOINT ECOSYSTEMS -- COLLABORATING TO CONQUER SECURITY THREATS

By Phil Harvey

4

COLLABORATION: CRITICAL FOR ADDRESSING SECURITY AND A STRATEGIC WAY TO TARGET ENDPOINT VULNERABILITY

By Maxine Holt



8

BEST PRACTICES FOR A COLLABORATIVE ENDPOINT ECOSYSTEM

By Dawn Kawamoto

10

ECOSYSTEM COLLABORATION FOR DEFENSE IN DEPTH

By Teresa Worth

12

ENDPOINT SECURITY: 3 BIG OBSTACLES TO OVERCOME

By Joe Stanganelli

14

WANNACRY: HOW THE NOTORIOUS WORM CHANGED RANSOMWARE

By Jeffrey Burt

LightReading SECURITY NOW

THE PREMIER ONLINE COMMUNITY FOR IT SECURITY NEWS, RESEARCH AND MORE.

NEWS DELIVERED STRAIGHT TO YOUR INBOX

ALL SECURITY, ALL THE TIME

SIGN UP TODAY

Sign up for the
Security Now newsletter today.

www.securitynow.com/register

EDITORIAL FORWARD

Endpoint security in the enterprise is getting more complicated by the day.

Employees are traveling more frequently and using their own devices for business purposes, adding layers of complexity to the already tough job the IT department has of protecting company data and endpoint devices. Tablets and smartphones now can hold copies of entire customer databases, and connect to cloud services and removable media where even more sensitive company info is kept.

Experts agree that keeping up with the many threats aimed at corporate assets is tough, and always changing. The research firm Ovum recommends a balance of educating people, improving processes and using technology strategically to help mitigate endpoint threats. What's more, the right way to do endpoint security is no longer a 'fix it once, and it's done' approach. As Ovum's analysts wrote in this e-book:

"There is too much to do, and the current model for tackling security is failing. It needs focus, speed, and better alignment of effort to threat. Where have we heard something like that before? DevOps. This different way of working is increasingly used to transform and optimize software development. Intelligently combining security and operations is now required to transform security. A different, more collaborative approach is called for to make better use of the resources available."

Indeed, collaboration, along with adequate technology and partner ecosystems, will move endpoint security forward, taking on that inherent complexity one threat at a time and keeping the enterprise ahead of the game.

Endpoint security goals haven't changed -- companies still want to protect their data, safeguard their services, shield their users and defend their devices. But the methods have changed, and now organizations need to extend a risk-based, holistic approach to security to include the endpoints, and they should make sure that their endpoint security approach is not static. As IBM's Teresa Worth wrote, effective endpoint security "moves, adapts and scales to keep pace with cybercriminals and accommodates ever-evolving business needs." ■

Phil Harvey
US News Editor
SecurityNow/Light Reading

COLLABORATION: CRITICAL FOR ADDRESSING SECURITY AND A STRATEGIC WAY TO TARGET ENDPOINT VULNERABILITY

The issue of security looms large over any information and communications technology (ICT) project and places an increasingly complex set of demands on any organization.

By Maxine Holt

Ovum has noted that a growing number of organizations are taking a more positive approach to tackling security. However, progress is slow: The latest ICT Enterprise Insights research shows that only about 8% of organizations worldwide have completed building a proactive approach to cybersecurity and digital risk – more than one-third of organizations have not yet started or are only in the early stages.

Organizations without a proactive security strategy will face significant challenges and security issues. The number and diversity of endpoints connecting with enterprise networks is increasing considerably. The cyberthreat landscape is morphing and evolving at a rapid pace, yet the staff and skills available to tackle these threats are in short supply.

There is too much to do and the current model for tackling security is failing. It needs focus, speed, and better alignment of effort to threat. Where have we heard something like that before? DevOps. This different way of working is increasingly used to transform and optimize software development. Intelligently combining security and operations is now required to transform security. A different, more collaborative approach is called for to make better use of the resources available.

ENDPOINT SECURITY NEEDS ADDRESSING, BUT THE SCALE AND RESOURCES REQUIRED ARE DAUNTING

Increasingly, it is not only the Chief Information Security Officer (CISO) who is painfully aware of the impact of inadequate security. Individuals regularly see major services and organizations being compromised through widely reported security breaches. Many CEOs now recognize security is no longer "just"' an IT issue, but a business one, focused on preventing reputational damage.

Dealing with security is a growing challenge, in no small part due to the sprawl of sophisticated technology endpoints. When these were once all PCs, the challenge was difficult, but contained. Now, device diversity from smartphones and tablets to the Internet of Things (IoT) makes the problem complex to define, let alone manage. Devices can be delivered with insecure default settings, deployed without central knowledge or control and exploited though novel or unusual vulnerabilities.

Digital transformation initiatives have resulted in a rapid escalation of the cyberattack surface. At a time when even the most process-driven organizations can struggle with patch management, digitally focused enterprises require a more clinical approach to endpoint hygiene and management. Furthermore, organizations trying to improve their endpoint management stance face challenging resourcing issues:

- **Skills Gap:** In addition to technical skills, which can often be taught, there are also gaps in soft skills and attitude. As all companies become increasingly technology dependent, business too needs better technology understanding.
- **Silos:** Internally, security people and the work they do are set apart from others, either in an Information Security function or as part of the IT function. They may have lots of tools (possibly too many), but there is often a lack of awareness, alignment, cohesion and collaboration between these functions, individuals, and the rest of the organization.
- **Closed Sector:** The internal collaboration issue is matched externally. Cybersecurity problems and challenges are hard to air and share, and companies are reticent about disclosure.
- **Pent-up Vulnerability:** Data about past breaches is building to create new social engineering intelligence for better targeted cyberattacks, e.g. phishing.
- **Compliance:** New mandates such as GDPR are increasing compliance demands. This directs focus toward security accounting processes, which is not always about reducing risks.
- **Fragmentation:** There is a proliferation of tools and services to tackle security issues, but little harmonization, consistency or data sharing. Integration and reworking data take precious time and effort that is not available.

MAXINE LEADS OVUM'S SECURITY PROPOSITION, DEVELOPING A COMPREHENSIVE RESEARCH PROGRAM IN THIS AREA TO SUPPORT VENDOR, SERVICE PROVIDER, AND ENTERPRISE CLIENTS. HAVING WORKED WITH ENTERPRISES ACROSS MULTIPLE INDUSTRIES IN THE WORLD OF INFORMATION SECURITY, MAXINE HAS A STRONG UNDERSTANDING OF THE CHALLENGES FACED AND HOW ORGANIZATIONS CAN LOOK TO OVERCOME THESE CHALLENGES.

Organizations are stretched, and simply trying to make incremental improvements is insufficient. A step change is required. Cybercriminals and those seeking to exploit vulnerabilities are combining and sharing all their available resources, trading with each other in a collaborative ecosystem. It is time for those on the defensive side to do the same, inside and beyond the organization.

THE NARROW-MINDED VIEW OF SECURITY AS A TECHNOLOGY ISSUE IS BROADENING INTO A BETTER UNDERSTANDING OF RISK AND BUSINESS IMPACT

Boards recognize the effects of security failures, which can encompass reputational damage, lost business and loss of trust. Closer alignment between those responsible for security and the business will bring about a much-needed shift in focus. Organizations mature in information security have an overarching security strategy that aligns with business strategy and objectives, and a progressive Chief Information Security Officer (CISO) engaging with the business.

This approach does not happen overnight, and neither can one individual make the necessary changes in isolation. The role of CISO increases its business focus, and changes across the organization are driven by progressive boards. There is increasingly widespread recognition that security is not simply a technology issue that needs to be controlled: Risk must be put into business context and mitigation applied.

The speed with which organizations evolve their approach will vary. This is mostly an issue of attitude and culture, rather than organizational size, hence it is not an overnight adjustment. Responsive organizations with a culture that can adapt and build new trust relationships will benefit most from this shift. Internally, this will involve bringing lines-of-business, IT operations and security specialists closer together so they can understand and support each other's priorities in line with organizational objectives.

The external sharing of security information is an even greater challenge. CISOs may already meet and share insights with their peers (for example, under the Chatham House Rule), but more formalized and anonymized mechanisms will be required for the larger scale and dynamic sharing of threat intelligence. This already happens in pockets around specific products and to an extent in some industry sector bodies, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).

But trust relationships are slow to build, especially where competitors are involved. Yet the cyberthreat landscape is expanding at a rate that makes it imperative for organizations to work together. A framework is needed around which a new, more integrated approach can be built.

EMBEDDING A SHARED APPROACH TO RISK AND SECURITY INTO PROCESSES AND MINDSETS

Technology can usefully underpin the process of building trust and collaboration, especially to create a common platform for the rapid sharing of threat intelligence in a sufficiently timely manner. However, it also requires a change in people and process and – for many organizations – a shift in the corporate culture.

Overall, a more balanced approach between people, process and technology is required ***(see Figure 1).***

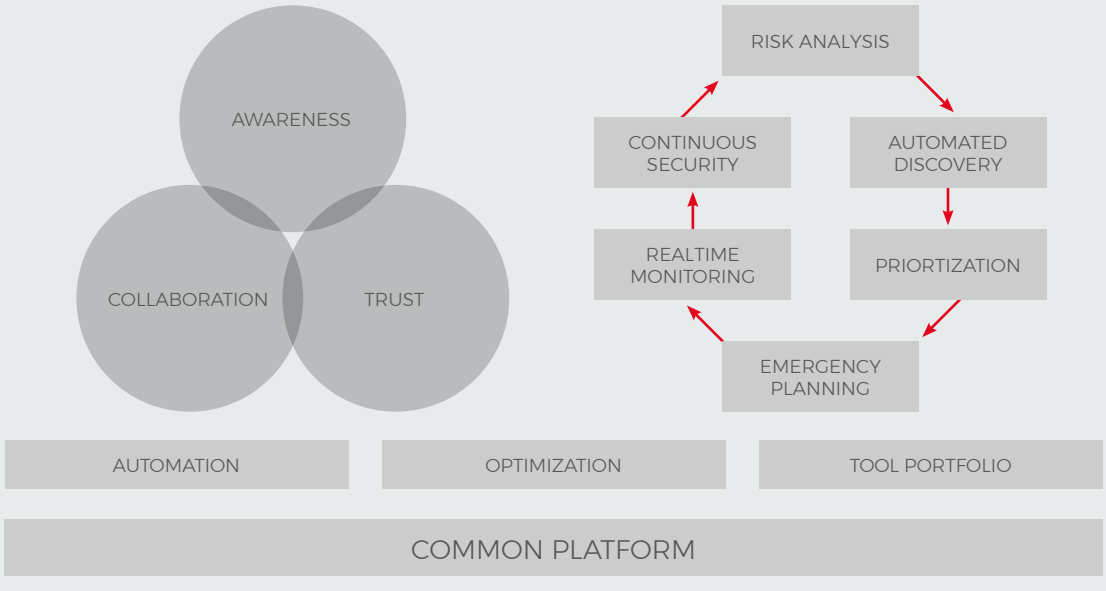
Technology

Technology is one area where there has been considerable effort and innovation, leading to a plethora of security tools and products. However, many organizations consider some of these tools and products oversold and under-delivered, leading to a requirement for consolidation and integration.

Endpoint vulnerability needs to be addressed with a multi-layered, end-to-end approach encompassing multiple aspects and tools:

- **Endpoint:** Installed software/agents must be lightweight and low impact, but offer continuous observation, enabling anomaly detection. All devices need authentication as well as identity and access management.
- **Mobility:** The additional risk of mobile has often been viewed as a special case of endpoint management requiring further specialized tools. However, Ovum finds this introduces too much complexity and mobile endpoint management needs to be consolidated with other endpoints into a single unified approach. Multiple tools may still be involved, but these must be integrated into a common platform.
- **Data:** Increased use of cloud has led to more effort to protect data on the move in transit and at rest on endpoints. Adoption of encryption must grow alongside planned investment in endpoint security. Recent high-profile breaches, alongside regulations such as GDPR, have focused attention on data value, which means that organizations need tools to differentiate their security stance based on the purpose, business risk and ownership of specific data. ›

FIGURE 1: COMBINED APPROACH OF PEOPLE, PROCESS AND TECHNOLOGY IN INFORMATION SECURITY



DEALING WITH SECURITY IS A GROWING CHALLENGE, IN NO SMALL PART DUE TO THE SPRAWL OF SOPHISTICATED TECHNOLOGY ENDPOINTS.

- **Analytics:** A range of threat intelligence and analytics tools are required to provide complete vulnerability and risk management – from continuous monitoring for user behaviors to advanced threat intelligence and detection.

- **Automation:** A continuous approach to security relies on automation to not only speed security performance, but also to remove manual errors. Automation tools need to be applied to aspects where there is greater risk of human error as well as for optimization.

- **Artificial Intelligence (AI):** It is not a "silver bullet" but AI can play a significant role in augmenting and amplifying the capabilities of individuals. Rather than thinking of it as an instant replacement solution, consider the impact of augmentation on skills development.For example, many organizations use chatbots to turn the efforts of one person into several, but the individual needs new skills to handle the "portfolio" of activities and a consistent model within which to work.

- **Response and Remediation:** Rapid incident investigation, analysis and response is vital – not only to detect, but also to ensure that any cleanup and fix is rolled out to all endpoints as rapidly as possible. Tools that foster the integration of security and operations into a continuous SecOps model are required.

- **Centralized Management:** A diverse set of tools is too complex to manage independently. A "single pane of glass" is required to simplify operations and allow for the coordination and implementation of changes in minutes across all endpoints.

Coordination and integration are required to support a more collaborative culture among individuals as well as more continuous and security-centric processes. Rather than simply a collection of diverse products, organizations require a portfolio of tools from multiple vendors that exploit open connections as part of an ecosystem. To build this will require a common and widely supported framework or platform. Based on an open model, this encourages innovation in new tooling and services, but also ensures that results and insights can be shared. This means that not only can individual products benefit more readily from the findings of other tools, but that individuals and organizations can share information on a common footing.

People

Building a pragmatic security culture is vital. It cannot be dictated or commanded, but attitudes must be fostered and grown. This type of change can only be delivered with the full support and commitment from those at the top of the organization in the following aspects:

- **Security Awareness Leading to Behavior Change:** Foster employee engagement and improved understanding of security risk and how it impacts individuals and the organization. This will include specific educational material, but also needs to be practiced and role-played to become embedded behavior for everyone – employees, contractors and those partners and suppliers engaging with the organization. Less training, more ingraining.

- **Business Risk Awareness:** Risk is calculated using likelihood multiplied by impact. Beyond the technical issues of vulnerability and threats, there will be an impact on the business should a threat materialize. IT and security operations do not have sufficient knowledge of the business. Technology is part of the organization's value chain, and to address the gap, business mentoring may prove useful.

- **Build Trust:** Break down internal and external silos. Collaboration comes from disparate people working together toward a common goal. Each bring their own unique talents and skill sets. They may have specific responsibilities, but a diverse team focused on a shared goal can be a catalyst for wider change.

- **Experiment to Learn:** The mantra of the Agile and DevOps approaches to software development is around learning through blame-free experimentation, assessing results in the context of the end user, making improvements – and repeat. Experimentation in security needs to have clear limits, but new approaches need to be found. Now is the time to encourage creativity and innovation when it comes to security.

Process

In addition to ingraining security into the everyday thinking of individuals, it needs to be embedded into business processes. Introducing secure and risk aware thinking through the entire lifecycle, in a manner advocated by SecOps and DevSecOps, will cultivate the changes required:

- **Start Earlier:** Perform risk analysis and threat modeling upfront, rather than incident and breach response, and damage limitation after the fact. Identify potential vulnerabilities, consider the likelihood of those vulnerabilities materializing, asses the business impact and focus effort on risk mitigation, prioritizing the most critical risks.

- **Automated Discovery:** Records will be incomplete or inaccurate, changes too dynamic, systems too diverse. Automated data discovery fills many of the gaps and provides a foundation for analysis, classification and further automation through machine learning.

- **Emergency Plan:** Things go wrong or will be missed. Plan in advance how to respond rapidly so that changes can rapidly be made. Consider increasing automation to optimize the roll-out of changes in critical situations.

- **Real-Time Monitoring:** The time to respond to and recover from security incidents and breaches can be dramatically reduced by recording and detecting anomalous changes as they happen.

- **Secure Continuously:** Security should not be seen as something to do or include at specific points in a process or (even worse) be "added" at the end. Every element, every task, every resource has an impact on security and must be considered continuously throughout all processes.

The combination of an open security collaboration platform with business-focused processes and a risk-aware culture will deliver a much-needed step change in an organization's ability to not only respond to security issues, but to move ahead. Those who try to simply repeat the step-by-step security models of the past, or place too much emphasis on the technology, will fail. The security model of the future is agile, ingrained, and business-ready. ■

IBM BigFix

A strong collaborative force is your best defense against predators.

Every day, your enemies are working together to take you down. Protect yourself with a collaborative endpoint management and security platform. IBM BigFix® helps you address vulnerabilities and integrate your tools, teams and processes to present a formidable defense against those who are intent upon exploiting any vulnerability they can find. Think about it. The bigger you are, the harder you'll fall. Stand up to your attackers with the IBM BigFix collaborative endpoint management and security ecosystem.

© Copyright IBM Corporation 2018. IBM, the IBM logo, ibm.com and BigFix are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.

BEST PRACTICES FOR A COLLABORATIVE ENDPOINT ECOSYSTEM

Enterprises are facing a growing array of endpoints from laptops to mobile devices and now IoT devices. Here are some best practices when creating and securing a collaborative endpoint ecosystem..

By Dawn Kawamoto, Technology Journalist

Enterprises face the challenge of securing an ever-growing array of endpoints, from laptops to mobile devices and now Internet of Things (IoT) devices.

That challenge is compounded as bad actors increasingly launch ransomware attacks across the globe, distributed denial-of-service (DDoS) attacks, phishing attacks and other nefarious activities. And these attacks can happen very quickly -- 87% of the past year's security incidents took just minutes or less to compromise a system and 68% of the cases took months or longer to discover, according to Verizon's 2018 Data Breach Investigations Report (DBIR).

"Ten years ago, malware analysis was often the only technique used. Today, endpoint security is a more complex topic with a set of different tools and approaches," Johannes Ullrich, dean of research with the SANS Technology Institute, said. "Anti-malware is still part of the mix. But it itself has changed and is using more behavioral analysis."

Other approaches include whitelisting in various forms and collecting more logs from the endpoint for central analysis, he added.

Is this good enough?

"It is...if it is all done. But implementation of all these techniques is still spotty, and they need to stay up to date with current threats," Ullrich said.

INDUSTRY SHIFT

Over the last three years, unified endpoint management (UEM) is gaining significant traction in the enterprise, David Monahan, managing research director of security and risk management for Enterprise Management Associates, said.

UEM solutions corral disparate operating systems, platforms and endpoints so that endpoints' data, apps and content can be updated, managed and secured using a single solution.

"Before, it was a very silo approach where people tried a lot of point solutions where it did just one thing like patching or malware removal, but people got tired of having to do all the work themselves and move data back and forth, for example, whereas now there is third-party integration," Monahan said, pointing to technology advances as the catalyst for this change. These advances include Representational State Transfer (REST) APIs, or RESTful APIs, which allow flexibility and the ability to better share information on the backside.

He noted market leaders such as IBM's BigFix and others have developed ways to integrate third parties onto a single virtual platform to make the security process more efficient to receive information and remediate the problem.

Another shift in the industry is staffing instead of budget becoming a roadblock. In the past chief information security officers often lamented that a lack of adequate budget allocation prevented them from moving forward with the security initiatives they desired, but they now often list a lack of skilled security talent as the main barrier.

Indeed, a global cybersecurity workforce shortage is expected to soar to 1.8 million people by 2022 – a 20% increase since 2015, according to a report by security industry trade group ISC(2).

"It is not a lack of budget that has created this problem, it's a lack of people," Monahan says. "There are more devices to secure, more security alerts, and more breaches, so enterprises need to look at automation [with their UEM]."

CONSTRUCTING A COLLABORATIVE ENDPOINT ECOSYSTEM

Below are a number of strategies to create a collaborative endpoint ecosystem along with Ullrich's advice on best practices to implement them.

- **Visibility of Devices**
  Two approaches can be taken. One is to scan your network for devices, but this may not work well since endpoints, especially IoT devices, may have their own firewall to prevent this. The other approach is to have security on the perimeter where employees are automatically prompted to register their device to gain access to the network, so any unregistered devices will automatically send a security alert.

- **Endpoint Integration and Streamlining**
  IT administrators will need to make some hard decisions on how much risk is acceptable. They could, for example, put all IoT devices together on one network, given a number of these devices do not allow companies to install software on them. Printers, which are increasingly considered an IoT device, could also be put together on one network, but it's a challenge because computers are often tied to printers, making it difficult to put them on a separate network.

- **Partner Integration Solutions**
  Have a discussion with each vendor of products that will reside on your platform. Ask them questions about how they plan to integrate their product to your specific platform, how they will handle the patching of their product on your platform and what type of endpoints will work with their product.

- **Security Dashboard Visibility**
  While it is important to look for the total number of vulnerabilities on a corporate network, or how many unregistered devices are on it, one of the first steps an enterprise should take is to set a policy of what to do with an unregistered device that is found on the network. If you have an unregistered endpoint on your network that is performing mission-critical functions, do you kick it off?

- **Patch Management**
  While most companies agree it is important to apply patches as soon as possible, it is equally important that the system verifies the patch was actually applied. Often, this feedback is missing from the security dashboard.

DAWN KAWAMOTO IS AN AWARD-WINNING TECHNOLOGY AND BUSINESS JOURNALIST, WHOSE WORK HAS APPEARED IN CNET'S NEWS.COM, DARK READING, THESTREET.COM, AOL'S DAILY-FINANCE, AND THE MOTLEY FOOL.

MARKET LEADERS SUCH AS IBM'S BIGFIX AND OTHERS HAVE DEVELOPED WAYS TO INTEGRATE THIRD PARTIES ONTO A SINGLE VIRTUAL PLATFORM TO MAKE THE SECURITY PROCESS MORE EFFICIENT TO RECEIVE INFORMATION AND REMEDIATE THE PROBLEM.

DAVID MONAHAN, MANAGING RESEARCH DIRECTOR OF SECURITY AND RISK MANAGEMENT FOR ENTERPRISE MANAGEMENT ASSOCIATES

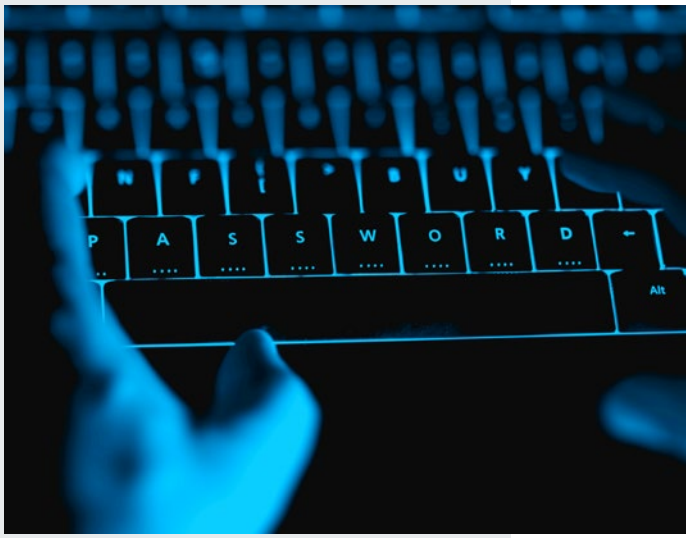
SUMMARY

With the ever-increasing rise in security incidents and breaches, along with a rapidly expanding landscape of endpoint devices, enterprises are hit with a double whammy of challenges. Creating a collaborative endpoint ecosystem can help mitigate some of the pain. And, according to Ullrich, enterprises that follow best practices that include ensuring device and security dashboard visibility and others outlined above, will be well-poised to streamline their collaborative endpoint ecosystem and foster greater security. ■

ECOSYSTEM COLLABORATION FOR DEFENSE IN DEPTH

Cybercriminals are collaborating on a global scale. They share vulnerability and credential exploitation information, corporate infrastructure details as well as easy-to-use, sophisticated, automated tools and weapons. And the impact to business is significant.

By Teresa Worth, IBM



Point-product technologies and linear-driven security strategies are no longer enough amidst the challenges of today's highly interconnected technology innovations. Organizations need IT and security tools, teams and processes that work together to protect critical assets and stay ahead of the bad guys.

TOOL-RICH, RESOURCE-POOR.

Historically, companies have purchased whatever new tool was available to combat the most recent threat – many of which only run on a specific operating system and are used for a single purpose (although they may have other robust capabilities). This has resulted in a plethora of redundant tools operating in isolation across various security and IT operations silos. (When IBM enters an engagement, it typically sees organizations have as many as 85 security products from 40 different vendors.) This increases the level of complexity in IT environments and the amount of time, effort and expense required to manage all these tools.

A recent SANS Institute report shows that lack of automation and tool interoperability is one of the top three barriers for effectively implementing endpoint security. Combine this tool-overload (and resulting inability to effectively communicate and share information) with a security skill set shortage and it's not surprising that organizations are tool-rich and resource-poor with overburdened IT teams.

COLLABORATIVE DEFENSE IN DEPTH

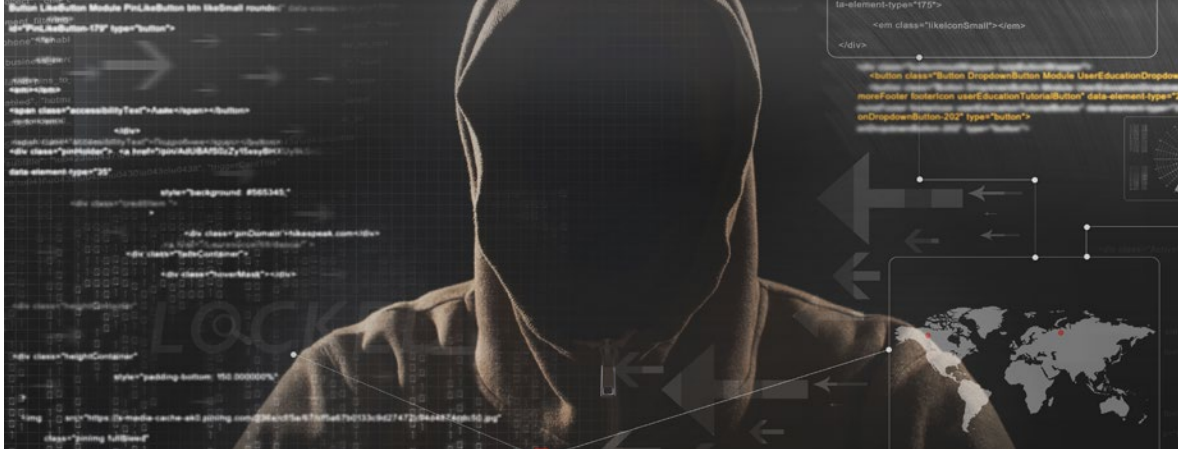
Security needs to become more agile so that it moves, adapts and scales to keep pace with cybercriminals and accommodates ever-evolving business needs. This requires the integration of tools, teams and processes. Through a collaborative approach, we're better able to solve the disparate security challenges that an organization faces by encouraging convergence, integration and streamlined threat defense.

Collaborative defense in depth starts with technology at its core. By embracing the practice of building strong, open integrations—both within a security vendor's portfolio and between solutions from other vendors—organizations can accelerate threat defense and extend security capabilities beyond what each technology could provide on its own. Once technology integrations have been addressed, the strategy can then focus on collaboration of people and processes.

COLLABORATIVE DEFENSE IN DEPTH STARTS AT THE ENDPOINT

When cybercriminals collaborate, they look for easy vulnerabilities to exploit and often focus on endpoints such as servers, PCs, ATMs and point-of-sale systems because unpatched vulnerabilities provide the easiest, fastest ROI for hackers. Insufficient visibility, sporadic endpoint hygiene (you can't fix what you can't see) and an older model of siloed teams using multiple, non-integrated tools is core to why these attacks are successful. With growing threats such as ransomware (e.g. WannaCry) widely reported in the press affecting millions of people, it makes sense to begin your collaborative journey at the endpoint.

Let's explore this further. First, insufficient visibility into your endpoint landscape provides poor context for the current state of your endpoints – especially in highly distributed environments. This impacts your ability to effectively prioritize and respond to your



most critical vulnerabilities. Second, by not being able to consistently update all endpoints simultaneously, your teams are constantly playing catch up – trying to get everything patched at the same level. This sporadic endpoint hygiene and inconsistency can open you up to attacks.

Finally, there's the issue of non-integrated tools, teams and processes. Security and IT Ops teams have different responsibilities. IT security teams are responsible for identifying endpoint vulnerabilities and prioritizing remediation efforts, but they often can't execute any changes on the endpoints. What's worse, they frequently don't have access to accurate, real-time endpoint data to make informed decisions. IT infrastructure teams have the responsibility of making all changes on endpoints, but this can be overwhelming given the number of endpoints and constant changes. Plus, they often don't have insights into the level of risk, so it's hard for them to prioritize endpoint management activities. These two teams are typically siloed and use disparate, non-integrated tools. This exacerbates the lack of visibility and sporadic hygiene problems – and can delay your ability to respond to potential threats and active attacks.

Improve Performance
Using solutions that integrate across your ecosystem helps you improve your IT operations and security performance by extending existing capabilities and addressing any functional gaps that may exist within a particular tool. This enables security and infrastructure teams to see and act on the same endpoint data without switching between multiple applications –enabling faster, better decision making. This integration also lets your staff use solutions they're already familiar with rather than having to deal with training and ramp-up delays.

Optimize ROI
Using integrated solutions also optimizes your return on investments by better utilizing existing solutions. This stretches limited IT budgets and leverages existing IT skill sets. This also helps you simplify your environments because you may be able to consolidate tools, thereby reducing tool management overhead.

IBM BIGFIX: A FOUNDATION FOR COLLABORATIVE DEFENSE

IBM BigFix is an endpoint management and security platform for IT Operations and Security professionals. BigFix lets you discover, manage and secure your endpoints – fast. IBM is working hard to integrate BigFix with other IBM products as well as third-party solutions. Current areas of integration focus include:

- **SIEM:** Security information and event management
- **IR:** Incident response
- **EDR:** Endpoint detection and response
- **EPP:** Endpoint protection platform
- **VM:** Vulnerability management

Existing BigFix integrations enable SOC teams using IBM QRadar and IBM Resilient to see endpoint data within their existing security information and event management (SIEM) and incident response (IR) tools. And the faster the security team can see how many endpoints are affected by a new threat, the better able they are to prioritize and implement remediation and response actions.

BigFix integrations with endpoint detection and response (EDR) tools enable your security team to remediate vulnerabilities quickly and at scale. It also ensures EDR sensors are up and running properly to better identify threats within your environment. Likewise, BigFix integrations with EPP, anti-virus and anti-malware tools ensure that agents are consistently deployed and actively operating in good health on all endpoints.

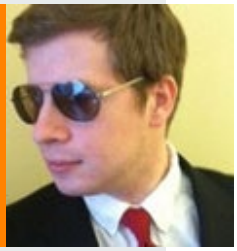
And don't forget about working with your network access control (NAC) solutions. BigFix integration with NAC systems enables you to understand the compliance posture of your endpoints to orchestrate remediation workflows and, if needed, isolate them from your network.

Additional integrations are in progress with vulnerability scanning tools to provide closed-loop vulnerability management, including the ability to prioritize remediation (based on the number of systems at risk and the risk level of each vulnerability) and automate remediation at scale.

Bottom line, the more closely your IT security and infrastructure tools, teams and processes work together, the more you will be able to improve security and operations performance, optimize ROI on your existing investments and simplify your IT environments. ■

A RECENT SANS INSTITUTE REPORT SHOWS THAT LACK OF AUTOMATION AND TOOL INTEROPERABILITY IS ONE OF THE TOP THREE BARRIERS FOR EFFECTIVELY IMPLEMENTING ENDPOINT SECURITY. COMBINE THIS TOOL-OVERLOAD WITH A SECURITY SKILL SET SHORTAGE AND IT'S NOT SURPRISING THAT ORGANIZATIONS ARE TOOL-RICH AND RESOURCE-POOR WITH OVERBURDENED IT TEAMS.

JOE STANGANELLI, PRINCIPAL OF BEACON HILL LAW, IS A BOSTON-BASED ATTORNEY, CORPORATE-COMMUNICATIONS AND DATA-PRIVACY CONSULTANT, WRITER, AND SPEAKER.



ENDPOINT SECURITY: 3 BIG OBSTACLES TO OVERCOME

In a report released in March on the topic of next-generation endpoint security, Enterprise Security Group (ESG) analyst Jon Oltsik observed that enterprises and antivirus vendors alike find keeping up with endpoint security difficult because of the sophisticated nature, prolific volume and exponentiating complexity of attacks.

By Joe Stanganelli, Principal, Beacon Hill Law

CISOs could anticipate that 40% to 50% of new sophisticated malware attacks could evade endpoint AV, compromise PCs, and act as a beachhead for advanced cyber-attacks," wrote Oltsik. "CISOs realize today that, regardless of the controls they deploy, some malware will sneak through, so they need continuous monitoring and visibility of endpoint behavior."

"Continuous," however, has practical limits.

ESG found that the top endpoint-security challenge—as indicated by 25% of the 385 cybersecurity professionals surveyed for ESG's report—was respondents' InfoSec teams taking too long dealing with too many security alerts, many of which are "false alarms." This suggests a—ahem—continuous trend.

In a separate ESG study last year on the topic of security operations challenges, 36% of the 150 IT and cybersecurity professionals surveyed reported that "keeping up with the volume of security alerts" was their top incident response challenge. Little wonder that enterprise security alerts are commonly treated as so much noise. Of those surveyed, 31% admitted that their organizations ignore at least 50% of their security alerts; an additional 34% reported that their organizations ignore 26% to 50% of their security alerts.

ENDPOINT-SECURITY OBSTACLE NO. 1: INSUFFICIENT AUTOMATION

ESG and other pundits have concluded that proper endpoint-security management demands enhanced automation and machine-learning tools—with the clearing out of security alerts being but one use case.

In an Industrial Internet Consortium (IIC) whitepaper on best practices in endpoint security, published in March, IIC emphasized automated protocols as a common denominator for both secure endpoint identities and secure attestations. Automation driven by public-key cryptography standards (PKCS), reported IIC, is critical to ensuring safety and certainty in the digital supply chain of certificates, firmware updates, etc. -- helping to keep at bay any malware that might otherwise slip through (sub) standard AV solutions.

Indeed, 17% of the ESG next-generation endpoint security study respondents identified their AV software as their top endpoint-security challenge, while 19% pointed to too many manual processes because of their lack of integrated endpoint-security automation. (It should be noted that respondents were allowed to select up to two responses.)

When it comes to malicious bots and the like, some contend that fighting AI with AI can be a losing battle. Consequently, a wholesale ban on non-whitelisted bots can help cut down on endpoint-security alerts and keep them manageable.

Nonetheless, IIC maintains that automated endpoint updates should be reliable without in-house whitelists or blacklists (typically manually input) as a matter of scalability.

"The number of attacks on industrial endpoints has grown rapidly in the last few years and has severe effects," Steve Hanna, co-author of the IIC whitepaper, said when the best practices document was released. "Unreliable equipment can cause safety problems, customer dissatisfaction, liability, and reduced profits."

ENDPOINT-SECURITY OBSTACLE NO. 2: LEGACY DEVICES

Despite these admonitions against equipment unreliability, the authors of the whitepaper make allowances for legacy endpoints. Still, they concede (1) that some of the most effective endpoint-security measures are embedded in hardware (typically not an option for legacy devices), and (2) that inadequately secure legacy endpoints must rely on network-security measures.

This latter point defeats the purpose of endpoint security. Why struggle against the most modern, most secure endpoints when there are more vulnerable legacy endpoints to be pwned?

To be fair, it is feasible to implement lower levels of trust across legacy endpoints—but perhaps impractical. Legacy endpoints are maintained for a reason (usually involving cost). Presumably, therefore, these legacy endpoints still need levels of accessibility appropriate for more up-to-date endpoints—despite the confidentiality and integrity risks.

THE NUMBER OF ATTACKS ON INDUSTRIAL ENDPOINTS HAS GROWN RAPIDLY IN THE LAST FEW YEARS AND HAS SEVERE EFFECTS

STEVE HANNA
CO-AUTHOR OF THE IIC WHITEPAPER

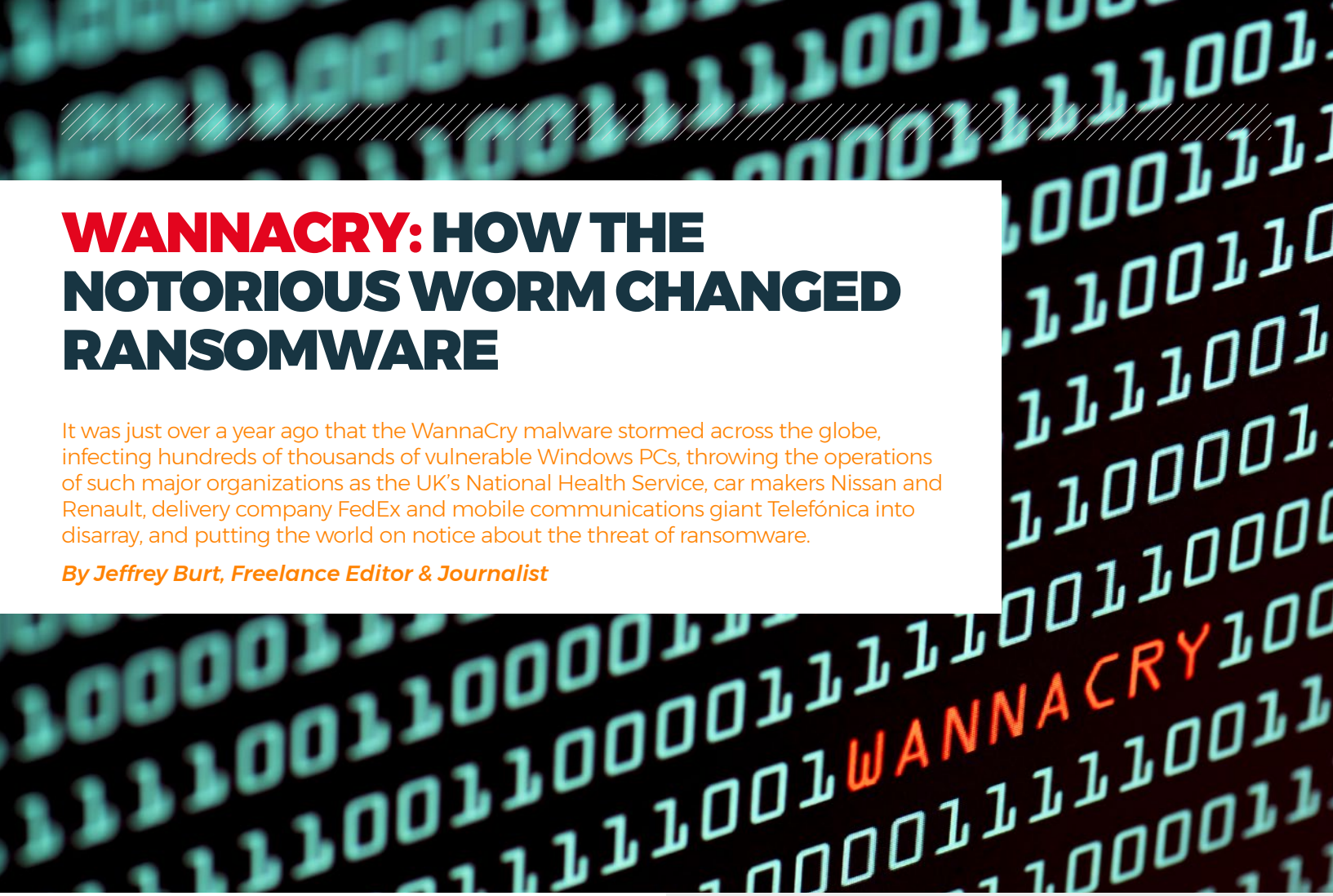
ENDPOINT-SECURITY OBSTACLE NO. 3: POOR SECURITY CULTURE

This preference among enterprises—even among InfoSec workers—to mortgage endpoint security for agility's sake is further evident in ESG's latest findings:

- Respondents' second-biggest endpoint-security challenge (23%) was that regular re-imaging of infected endpoint devices creates more work for respondents' helpdesks and "imped[es] end-user productivity."
- 17% of respondents also complained that "imped[ed] end-user productivity" caused by endpoint-security agents slowing down endpoint processes was their organization's top endpoint-security challenge.
- 14%, meanwhile, said that their top endpoint-security woe was lacking the budget for "the right endpoint-security products".

ESG is not alone in making such findings. Verizon Wireless, for instance, reported in February that nearly one-third of 600 surveyed mobility professionals admitted that their organizations sacrificed mobile security in favor of business agility -- at significant risk. (See: Verizon Mobility Security Index Shows Enterprises Not Doing Enough.)

More depressingly, in a world where enterprises can be split into the hacked and the unaware of being hacked, a doubtlessly overly optimistic 10% of the ESG survey respondents reported having no endpoint-security challenges whatsoever. ■



WANNACRY: HOW THE NOTORIOUS WORM CHANGED RANSOMWARE

It was just over a year ago that the WannaCry malware stormed across the globe, infecting hundreds of thousands of vulnerable Windows PCs, throwing the operations of such major organizations as the UK's National Health Service, car makers Nissan and Renault, delivery company FedEx and mobile communications giant Telefónica into disarray, and putting the world on notice about the threat of ransomware.

By Jeffrey Burt, Freelance Editor & Journalist

The fast-spreading worm essentially encrypted the files, documents, photos and any other data on the victim's computer and displayed a note saying that only the attackers' decryption service could restore access to the files.

In return they demanded $300 in Bitcoin be sent to an address within three days.

Don't pay within a week, and the files would be deleted.

The WannaCry threat didn't last long. The security community reacted quickly, and within days a kill switch was discovered and activated, essentially rendering the malware toothless by ensuring that it couldn't decrypt files on systems it was attacking.

That doesn't mean it's still not out there.

There are still about 2.3 million devices with the Windows SMBv1 (Server Message Block) exposed to the Internet, the primary avenue WannaCry took into the systems, according to Juniper Threat Labs. And in March, a Boeing aircraft plant was hit by a cyberattack that appeared to be related to WannaCry. (See WannaCry Ransomware Hits Boeing, but Company Claims It's Contained.)

At the same time, the industry is still feeling the effects of WannaCry a year later. Ransomware remains a problem, though some researchers are seeing a decline in instances, and creators of newer malware took the lessons learned from WannaCry to create such threats as NotPetya, BadRabbit and Olympic Destroyer. The ransomware also put a spotlight on the need for such capabilities as segmentation and advanced endpoint security, and the reasons researchers urge organizations to reduce the exposure of their systems. (See Ransomware: Still a Security Threat & Still Evolving.)

WannaCry may have been effectively neutralized, but the repercussions continue.

THE RISE OF WANNACRY

"At a really high level, the reason why WannaCry was so effective what that it was the first time someone had combined a ransomware payload with a network vector," Craig Williams senior threat researcher and global outreach manager for Cisco Talos, told Security Now. "In this particular case, the network vector was what we call EternalBlue. It was an exploit leaked out of the Shadow Brokers release."

Bringing together the WannaCry encrypting malware with the EternalBlue exploit enabled the ransomware to spread rapidly in worm-like fashion. It targeted vulnerable PCs with the Internet-facing SMBv1 ports and, once inside, searched for and spread to machines with similar vulnerabilities that were part of the network.

"WannaCry was a big deal because the victims numbered in the millions and the effects were devastating," Mounir Hahad, head of Juniper Threat Labs, told Security Now in an email. "Technically speaking, it also dawned an era where ransomware can now cross network boundaries and jump countries. It was an effective combination of crypto-ransomware and worm capabilities."

Before WannaCry, ransomware typically needed someone to do something -- opening up an email or going to a website, thus unintentionally letting the malware into the system. This made it difficult for the ransomware to cross network boundaries, Williams said.

In 2016, the SamSam malware became the first to use a network vector, but it wasn't automatic. It still required the attacker to spread the malware around. However, it showed researchers the impending threat of criminals making a piece of malware into an automated worm that could spread rapidly. The WannaCry creators did just that.

It also was the first major new worm seen in the past 10 years, since the days of Conficker and Slammer, putting the industry on notice that worms were still around.

DECONSTRUCTING WANNACRY

However, WannaCry, for all the chaos it caused and anxiety it produced, wasn't the best piece of malware. There were problems with it. For one, it couldn't correlate who paid the ransom and who didn't, so not everyone who paid received the decryption key. It also wasn't stealthy, it spread across the Internet in a haphazard fashion and it had a broken scanning algorithm, which meant it didn't spread as fast as it could have, Williams said. It also had a narrow attack surface, targeting only certain versions of Windows.

And it also had the kill switch.

"The worst piece from a malware standpoint was the idea of the kill switch, which really doesn't make any sense from any security perspective," Williams said. "Effectively what it let people do was turn off the malware which is what happened. So, from a practical standpoint, WannaCry was not super successful. WannaCry was more of a proof-of-concept of what may be possible as far as combining data destruction malware with network vectors."

That said, there was pain. Dan Wiley, head of incident response at Check Point, told Security Now that it didn't hit a large number of organizations, so it wasn't as large a problem as many may think. However, "the damage that it did do to the 10 or 20 major corporations that were hit with it was pretty dramatic," Wiley said.

THE LASTING EFFECTS OF WANNACRY

Despite the malware's weaknesses, WannaCry's influence can be seen throughout the industry a year later. That influence can be seen in the ransomware that has come since. Ransomware like NotPetya and Olympic Destroyer took was WannaCry was doing and improved on it.

"WannaCry took what was supposed to be a precision ammunition, namely EternalBlue, and turned it into a weapon of mass infection," Juniper Threat Labs' Hahad said. "Seeing how effectively it spread, several other malware, such as NotPetya and BadRabbit, followed suit using similar techniques to infect as many hosts as possible. NotPetya, for instance, expanded on those techniques by also incorporating EternalRomance as a method of spreading to other computers."

NotPetya "came out a month later and it used multi-vectors and a lot of really evasive techniques," Williams said, adding:

It used probably one of the most advanced scanning mechanisms we've ever seen. It combined a supply-chain attack of the initial vectors so it spread almost invisibly across the world and then all at once it wiped systems all over the world. WannaCry was a wakeup call. But it happened so quickly and it shut down so quickly, a lot of people thought maybe they got lucky. But then a month later when NotPetya hit, people realized that these were not going to stop. This is the first worm vulnerability in a long time and it continues to be used today for different types of malware.

This newer generation of ransomware also is less noisy and more targeted than WannaCry, Check Point's Wiley said. WannaCry made headlines around the world, researchers attacked it and very quickly they figured it out and neutralized it. The ransomware attackers who came after that looked to keep out of the spotlight to keep the money coming in.

"You want to be just right under the threshold of pain," he said, noting that companies are still paying tens or hundreds of thousands of dollars in ransomware extortion. "Sure, it's a lot of pain per company and globally it has an impact, but it doesn't get anyone's attention because it's right under the threshold for a lot of the law enforcement agencies to get involved."

WHAT'S NEXT

Cybercriminals also are being more selective. Rather than a scattershot across the world, they're being more targeted in their efforts.

"For attackers, it's becoming much more intimate," Wiley said. "They're choosing their victims very carefully, profiling them a lot more carefully, and definitely targeting them one at a time ... the financial effectiveness of [WannaCry] is not as lucrative as targeting a particular corporation, extorting them to the maximum and then moving on to the next victim."

WannaCry also has highlighted the ways organizations can better protect themselves against ransomware threats, including segmenting machines if they can't be patched to reduce the amount of damage done. In addition, companies need to shut down the vulnerabilities that allow WannaCry and other ransomware to get into the systems. SMB should never be exposed to the Internet. The same goes for Remote Desktop Protocol, Wiley said. If it's exposed to the Internet and isn't protected against brute-force login attacks or by two-factor authentication, it needs to be shut down.

And that highlights the key problem. Despite the warnings, there are still millions of machines with SMBv1 still exposed to the Internet.

"Many companies have learned from the major attack, but there will always be a big enough trailing crowd that is unable to change its security posture," Hahad said. "One year later and we are still seeing about 2.3 [million] devices with SMBv1 still exposed to the Internet ... This is often a result of having understaffed security teams that are bogged down by manual processes and complex policies, creating fertile ground for future attacks. For example, it is reported that every day in Q1 2018, an average of 20,000 systems scan the Internet looking for still-open SMB ports, which are the ports used in the WannaCry campaign through the Eternal Blue exploit."

JEFFREY BURT IS A LONG-TIME TECH JOURNALIST WHOSE WORK HAS APPEARED IN SUCH PUBLICATIONS AS EWEEK, THE NEXT PLATFORM AND CHANNELNOMICS.

When you're under assault, fight back.

IBM **BigFix**

Every day you're under attack from unscrupulous cyber criminals intent on exposing and exploiting any vulnerability they can find. They're not working alone. And neither should you. Learn how you can ward off their unrelenting attacks. The IBM BigFix® endpoint management and security platform can help you integrate other key security and operations applications to keep your systems safe from those who wish to do you harm.

Gather intel.
Read our informative piece, ***CISOs Investigate Endpoint Security***, and see first-hand what endpoint security issues are top of mind with 13 security leaders across industries.

Read our paper

Put together a team strategy.
Our blog, ***Why collaborative defense is the future of endpoint management***, presents how IBM Security is expanding its endpoint ecosystem with application integrations that include both IBM and third-party solutions.

Read our blog

Listen to the experts
Attend our webinar, ***How collaboration (or lack of) affects your endpoints***. Learn how the BigFix ecosystem works and how your business can take advantage of it. You can also see specific use cases regarding BigFix integrations with IBM QRadar®, IBM Resilient®, ForeScout and Carbon Black.

Attend our webinar

Steal good ideas
Attend our webinar, ***Gartner and IBM BigFix Talk Endpoint Hygiene Basics and Collaboration***, and hear why endpoint hygiene is critical and what to look for in solutions. We also discuss why patching isn't getting done, and offer ideas for better collaboration.

Attend our webinar

© Copyright IBM Corporation 2018. IBM, the IBM logo, ibm.com and BigFix are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.

IBM