FUTURIOM
THE FUTURE OF TECH

Technology Research
June, 2017

ANALYSIS OF ADVANCED TECHNOLOGY MARKETS

Endpoint Security and SysSecOps

The growing trend to build a more secure enterprise

Key Findings

- Endpoint security integration and organizational coordination are key to building a SysSecOps approach to enterprise security
- Many of the major hacks of the past five years could have been prevented with better organizational response and integration of security tools
- Half of the respondents to the 2017 Futuriom security survey of believe security technology integration is a major challenge in securing endpoints
- Integrating security tools is a major goal of SysSecOps, which can have beneficial effects in securing the enterprise, according to Futuriom research
- Many systems and security operations staff say they are challenged by time and resources, meaning further security automation would be welcome
- Conflicting security goals within the same organization can be a barrier to securing endpoints and systems
- Many current endpoint security tools are inadequate, lacking integration with other security components
- Malware and phishing remain major threats to enterprise security, requiring integrated system monitoring and endpoint protection

Table of Contents

Introduction: The Quest for More Holistic Security 3

Industry Needs: Coordinated Visibility and Control 6

- A Review of Recent Breaches: What to Learn? 6
- Creating an Intelligence Platform 10
- Creating Control and a Responsive Organization 11

Trends in Integrating the SysSecOps Ecosystem 13

- Integrating the Category Killers 13
- SysSecOps is Driving New Requirements 17
- The Evolution of Full Visibility Security Stacks 17

Endpoint Visibility for SysSecOps: What Users Want 19

- IT roles of survey participants 19
- Top organizational challenges 20
- Most hopeful approaches to improving security 22
- Top security goals 23
- Success rates in endpoint security 24

Conclusion: Leading the SysSecOps Future 25

Introduction: The Quest for More Holistic Security

Visibility into Information Technology (IT) systems has never been more important. Managers of IT systems as well as security operations professionals are charged with installing, monitoring, maintaining, and securing a vast array of corporate IT assets. However, as demonstrated by the recent impact of major security breaches, this responsibility extends up the corporate ladder to CxOs, including the CEO – as well as the corporate boardroom. The stakes have never been higher.

Let's look at some examples of the risks to your enterprise. It's already estimated that the recent WannaCry ransomware virus will likely cause more than $4 billion in economic damage, according to USA today.[1] In the breaches at Target and Home Depot in 2014, the collective cost was $500 million, according to Digital Transactions. 2 Target CEO Gregg Steinhafel was forced to resign in the aftermath of the exposure of 40 million credit and debit card accounts, along with personal information on 70 million customers. Home Depot reached a legal settlement to pay a total of $160 million in compensation to consortiums made up of Visa, MasterCard, and various banks. That doesn't take into account the brand damage and settlements with customers.

Monitoring the myriad IT systems means dealing with more complexity than ever. Virtualization, cloud services, extensive remote workers, and ever-increasing endpoints – including those connected to customers, partners, and employees -- means that systems are no longer contained within corporate boundaries. Chances are, at any time, many employees and network endpoints are accessing data all over the world, from a variety of cloud services. At the same time, the threats to IT resources are scaling on a global level, with prominent cybersecurity attacks occurring

[1] "North Korea May Be Linked to WannaCry Cyberattack, US News, May 16,2-17; https://www.usnews.com/news/national-news/articles/2017-05-16/north-korea-may-be-linked-to-wannacry-ransomware-cyberattack-experts-say

[2] "Expenses From the Home Depot and Target Data Breaches Surpass $500 Million," Digital Transactions, May 26, 2016 http://www.digitaltransactions.net/news/story/Expenses-From-the-Home-Depot-and-Target-Data-Breaches-Surpass-_500-Million

daily, often resulting in stolen data, corporate financial losses, and violations of privacy.

How does an organization holistically manage risk and security for this infrastructure? It starts at the endpoint. Mature security organizations recognize that preventative endpoint protection platforms can only do so much. Thus, endpoint detection and response (EDR) platforms have become a focus of the security industry.

But how do EDR products and processes integrate with the broader risk management and security tools around them? To secure and protect connected assets, security specialists and IT managers need higher quality insights and visibility from these endpoints, not more siloed solutions. And they need to share that data to establish a single source of truth enabling quicker and more effective security and risk mitigations.

These findings are the result of an extensive survey of a wide range of staff –from IT system administrators, security operations, and executive management. The survey, conducted by Futuriom, found remarkable consistency from the results of this survey, which included responses from 149 systems management and security professionals. The top goals of these professionals are increased integration of IT systems and security operations, both tools and functions – as well as coordination of the associated budgets allocated to these organizations.

Some of the key findings of this report:

- **Integrated security visibility is a top challenge.** Fifty-three percent of the IT and security respondents (including IT system admins, security specialists, hardware specialists, network admins, executive managers, and others), indicated a "challenge in integration of many security tools" as a major challenge of securing their endpoint environments.
- Security starts at the endpoint. Respondents to the survey see endpoint security technology as key, with 55% demanding better protection of endpoints as a top security goal.
- **It's a human problem -- many attacks can be stopped.** A look at the major hacking events of the past five years shows that many breaches were flagged by technology – the failure came with human response.

- **Integrated security visibility is a top challenge.** More than 50% (53%) of the IT and security respondents (including IT system admins, security specialists, hardware specialists, network admins, executive managers, and others), indicated a "Challenge in integration of many security tools" as a major challenge of securing their endpoint environments.
- **Integrating existing tools is a major focus.** When asked, "What would be the most helpful in improving IT security in your organization?", end users selected "Better integration between systems management and security operations tools," as one of the most helpful approaches.
- **Time and resource are a big challenge.** Half (50%) of the survey end users said they lack time and resources to secure the environment. Thus, more efficient and prioritized operations would help.
- **Management isn't always on the same page.** Thirty-seven percent of the survey end users say conflicting IT and security goals prevented them from achieving their goals.
- **Current endpoint tools may still be inadequate.** Many end users say despite the plethora of security and visibility tools at their disposal, better tools are needed.
- **Malware and Phishing remain major threats.** The Verizon Data Breach Investigations Report puts malware and phishing as the cause of 51% of cyberattacks, underscoring the importance of coordinated systems and security operations.

The findings were consistent among IT system managers, security specialists, and network managers – they all want to see improved, more highly coordinated system monitoring and security operations. The need for better integration of system monitoring and security tools and operations is an approach we are defining as "SysSecOps".

The goal of SysSecOps is to give IT and security teams a improved, more holistic view capability in managing the overall risk and security of their endpoint environments. This report outlines the trends in coordinating system and security, specifically EDR, tools to yield a SysSecOps platform for improved visibility and control into the wide array of managed IT systems or endpoints.

Industry Needs: Coordinated Visibility and Control

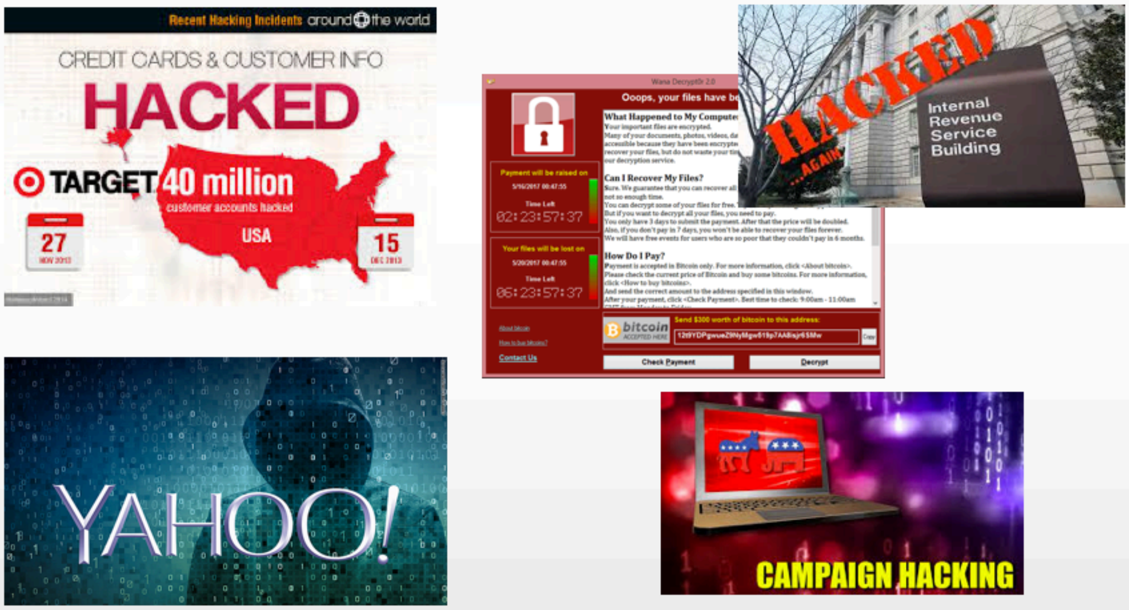
As discussed, the stakes of SysSecOps are rising with the potential economic and reputation risks for individual enterprises, as well as all individual managers and consumers. The pattern of security in the past five years shows that many could have been prevented, or discovered more quickly, with better visibility and alert / response systems.

The risks are clear, on an economic basis. The average total cost of a data breach for 383 companies increased from $3.79 to $4 million, according to the 2016 Data Breach Survey by the Ponemon Institute and IBM.

A Review of Recent Breaches: What to Learn?

It's clear that anxiety is rising in boardrooms, governments, and IT staff rooms around the world, as the number of high-profile headlines about security breaches streams in.

Security Events on the Rise



What Happened to My Compute
Your important files are encrypted.
Many of your documents, photos, videos, da
accessible because they have been encrypte
recover your files, but do not waste your tim
our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all
not so enough time.
You can decrypt some of your files for free.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

It's insightful to take a detailed look at some recent major events to find the root causes and some measures that could have been taken to mitigate or stop the attacks.

Significant security events in just the last few years include:

- **Yahoo Breach, 2013-2014.** A series of disclosure by Web content and service provider Yahoo (now owned by Verizon) has revealed that as many as 1 billion users accounts were compromised in the period of 2013-2014. Data involved included names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions that could be used to reset a password. Yahoo forced all users to change passwords and invalidate security questions. The New York Times reported that one of the challenges at Yahoo was continued clashes between the security team and senior management after the security team sought to implement better security systems. 3

Wh**at could have gone better:** Better resource and budget coordination among staff.

- **Target Breach, 2013.** A Breach of Target Corp. systems in 2013 was launched using malware to steal roughly 40 million credit and debit card records and 70 million customer accounts. The malware was installed on Target' s point-of-sale (POS) machines and was attributed to passwords stolen from Fazio Mechanical Services Inc., a refrigeration vendor for Target Corp. In an evaluation of the attacks, it was clear that Target had trouble tracking the attacks due to the multi-layer nature of the networks and IT systems involved in supporting the POS and financial systems. CEO Greg Steinhafel, a 35-year veteran of the company, was fired in 2014.

What could have gone better: Organizational response time -- and perhaps automation -- to issues flagged by technology.

- **Sony Hack, 2014.** Hackers penetrated Sony networks, then stole and released confidential data belonging to Sony Pictures Entertainment (SPE) on November

[3] "Yahoo Says 1 Billion User Accounts Were Hacked," *New York Times*, December 14, 2016; https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?action=Click&contentCollection=BreakingNews&contentID=64651831&pgtype=Homepage&_r=0

24, 2014. The stolen information included emails between employees, corporate information including salaries of employees at the company, unreleased Sony films, and other information. The hackers claimed to have stolen 100 terabytes of data and later identified themselves as Guardians of Peace. The U.S government accused the North Korean government of being involved in the hack. Some security experts have speculated that the security compromise was underway for as long as a year. After the hack, the hackers installed software known as Wiper on Sony's computer infrastructure, designed to erase data. Sony co-chairperson Amy Pascal announced her resignation in May 2015.

What could have gone better: Better overall endpoint monitoring, threat detection, and coordination between IT and security teams to detect and quickly respond to the hack.

- **Home Depot Attack, 2014.** Home Depot announced in September 2014 that a massive data breach allowed criminals to take data on 56 million credit and debit cards in the United States and Canada. The theft involved the installation of malware installed on self-checkout registers. As in the Target attack, Home Depot said the hackers used a vendor’s stolen log-on credentials to get access to the computer network and install malware. Investigations concluded that many of Home Depot’s executives and security experts may have moved too slowly to alter its security defenses to scan for new threats.

What could have gone better: Home Depot was advised to activate installed endpoint detection capabilities, but did not. Heightened awareness and a quicker response by executives could have mitigated risks.

- **Ebay Hack, 2014.** In 2014, hackers gained access to records for as many as 145 million users, including unauthorized access to a database containing names, addresses, phone numbers, dates of birth, email addresses and encrypted passwords. Ebay said “Cyberattackers compromised a small number of employee log-in credentials, allowing unauthorized access to eBay's corporate network. We are working with law enforcement and leading security experts to aggressively investigate the matter. At this point, we are not disclosing further information.” Ebay had taken standard precautionary measures, such as separating and encrypting customer data, but more advanced techniques could have been used. For example, it could have used behavioral analytics to score transactions and decline ones that seem fraudulent, according to Liron Damri, chief operations officer of security specialist Forter, in an interview in Inc. 4

What could have gone better: Feeding detailed endpoint behavioral data into an analytics engine probably could have identified the attack earlier and prevented further damage.

- **Anthem Healthcare Breach, 2015.** A breach at Anthem Healthcare in 2015 affected up to 80 million Anthem members. Information such as names, birthdates, social security numbers, and other data was exposed in one of the company's databases. The firm hired security firm Mandiant (now owned by Fireye) to evaluate security policies, but those details have not been publicly released. The company disclosed that the data was gained by the compromise of an administrator's account, so encryption would have helped. Security experts have speculated that it could have been an "internal attack," in which an employee used an account, or an outsider phishing the credentials from an employee. Firewalls and other perimeter defenses would have not stopped these types of attacks. Some experts believe that behavioral analysis may have identified anomalies in activity that could have flagged the attack earlier.

What could have gone better: A real-time, automated behavioral analysis of user and system activity, leveraging endpoint data, may have led to the attack being discovered sooner.

- **Democratic National Committee (DNC), 2016.** The DNC in 2016 and 2017 disclosed that it had been hacked by cyberespionage groups. One of these cyber-attackers is believed to have been in the system for a year and had been monitoring internal communications, including email. Another group of hackers is believed to have been in the system for only a and was targeting the DNC's research on then-presidential candidate Donald Trump. The information gained was then leaked on WikiLeaks, including 19,000 emails and 8,000 attachments from the DNC. This story, of course, has become national attention and is

[4] "How the Once Impregnable EBay Fell Victim to Hackers (And You Can too)," Inc.; https://www.inc.com/jeremy-quittner/new-details-emerge-on-ebay-hack-attack.html

subject to an ongoing Federal Bureau of Investigation (FBI) investigation and Congressional inquiries related to who was behind the attack. The cyber-attackers are believed to have links to Russia. Security firm CrowdStrike as well as Fidelis identified the perpetrators as "Cozy Bear" and "Fancy Bear," hackers believed to have strategic connections to the Russian government. The Central Intelligence Agency (CIA) has concluded Russia conducted operations during the 2016 U.S. election to prevent Hillary Clinton from winning the presidency. In the fallout of the first discovered breach during the summer of 2016, representative Debbie Wasserman Schultz of Florida, the chairwoman of the D.N.C., resigned.

What could have gone better: The DNC hack appears to have been launched with a relatively simple phishing operation combined with weak passwords. A combination of technology and practices, such as endpoint detection and response capabilities, employee training, and two-factor authentication, could have resulted in a better outcome for the DNC.

Creating an Intelligence Platform

A large portion of security breaches start at the endpoint. This is why the integration of endpoint security and IT management tools is crucial to gaining visibility into security risks.

A major issue for many IT and security teams is maintaining a "clear picture" of what's happening across their endpoint environment. The review of recent breaches teaches us that most these attacks were aided by the defending organizations lack of clear intelligence – whether it was a lack of data exposing clear vulnerabilities on their systems, a lack of user or system behavioral data indicating abnormal activities, or a lack of threat detection data indicating a clear threat on a system.

More than 51% of data breaches used malware, according to Verizon's 2017 Data Breach Investigation Report (DBIR). In addition, 66% of malware was installed via malicious email attachments. The Verizon DBIR goes on to describe a "triple threat of hacking, malware and social," which it sees trending upward for the last few years.

The Verizon DBIR also highlights the popularity of phishing attacks, whether by email or social networks. These types of attacks are also prevalent in some of the big-name breaches of the past few years, including the now world-famous attack on the DNC. In the end, human behavior, such as clicking on malware-carrying links, is one of the highest security threats. And most of these malware attacks exploit systems with vulnerable, unpatched applications or operating systems. This makes endpoint detection, and the use of endpoint detection data for monitoring and analytics capabilities, a key effort in IT security.

And as noted previously, endpoints are increasingly remote, or disconnected entirely making it challenging to monitor activities and risky end user behaviors. The myriad endpoint monitoring, management, and security tools create silos of data that can conflict with one another, creating incremental issues that teams must reconcile.

Ultimately, this lack of a "clear picture", or the need to piece together data from a variety of systems leaves organizations struggling to understand their risk posture and security state, making it tough for teams to answer some of the most basic risk and security questions like:

- What systems are connected to our network?
- What software is running on those systems?
- Are my systems compliant to our own policies?
- What vulnerabilities exist in our systems?
- Are there clear indicators of threats on my systems – internal or external?
- How did a threat get onto our systems?
- What actions did a threat take once it was in our environment?

The ability to collect and share endpoint intelligence is a clear first step for organizations working to implement coordinated systems and security operations, SysSecOps.

Creating Control and a Responsive Organization

One of the patterns in many of the major data breaches is a lack of human response. Many of the major security breaches of the past five years could have been easily prevented with improved security hygiene, or flagged by existing endpoint security technologies. One of the major struggles is reacting to critical issues and breaches, and quickly reporting incidents up the chain of command.

In some cases, such as Target, the intrusion was flagged by certain systems but did not propagate alerts far enough up the food chain to stem the damage. Or, worse yet, some of the alerts appear to have been ignored. Believe it or not, this is a common problem.

At the DNC, there seems to have been a fundamental misunderstanding of the threat of simple malware and phishing scams – which could be solved with good training, password practices, and endpoint threat detection.

At eBay, endpoint and transactional data could have been fed into an analytics engine to give better visibility into the potential of fraudulent activity.

In many of these situations – the technology existed to stop attacks – and was in fact already in house. Some of it only had to be "turned on" – or listened to. The larger struggle is to structure an organization and their corresponding technologies to clearly recognize issues and to respond to the items at hand – or even to automate a response.

One of the problems may be that the proliferation of security and monitoring alerts has overwhelmed many security professionals. A recent survey by the Enterprise Strategy Group (ESG) found security professionals are inundated with security incidents, averaging 78 investigations per organization in the last year, with 28 percent of those incidents involving actual targeted attacks. And in almost every case, response to any alert, be it vulnerability, compliance or actual breach alerts, requires quick, coordination between both IT and security teams. So, to create endpoint control and a responsive organization requires coordinated systems and security operations, SysSecOps.

These findings were reported in the ESG report, "Tackling Attack Detection and Incident Response" commissioned by Intel Security, which examined organizations' security strategies and incident response challenges.[5]

Because of this challenge in "alert propagation," or what many refer to as "alert fatigue", it makes sense to consolidate the alerting process and further refine it using analytics and automation. This can be useful in filling organization gaps and relying on human responses to alert events.

In the following section, we go into more detail about some of the groups of management and security tools and how SysSecOps trends are emerging to deliver a more robust security monitoring system.

[5] "Tackling Attack Detection and Incident Response," Jon Oltsik, Senior Principal Analyst, McAfee and ESG, April 2015; https://www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf

Trends in Integrating the SysSecOps Ecosystem

One thing is clear from a careful examination of the details of major security breaches as well as feedback from leading experts and end users: There are a vast range of tools and techniques that can be used to manage endpoint risks and contain threats, but the challenge is to implement them and coordinate them in a way that yields the best results.

In addition to gathering end-user data from 147 SysSecOps specialists and executive managers, Futuriom spoke to a half-dozen security experts to get more qualitative feedback on the challenge of SysSecOps. The resounding conclusions was that diverse tools and systems – with a lack of coordination even at the management level – was a barrier to achieving improved visibility and control into the IT systems infrastructure.

Experts say the challenge is not the lack of tools or knowledge, it's integrating existing organizations and their tools into a system of monitoring, control, and automation that can give the best defense.

"There are many smaller technology companies filling in the gaps in security, now you have this need for a best-in-breed architecture," says Anthony Juliano, CTO with Landmark Ventures. "You need to find 5, 15, or 20 different vendors. You need to invest back into that business. It's not the same level of efficiency than if you are going to one provider. How do I integrate those together to create a true protection lifecycle?"

Integrating the Category Killers

Integrating today's best-of-breed tools to enable SysSecOps is no easy matter, but signs are improving. As end users attest to frequently, there is a dizzying array of tools, both in the IT and security infrastructure, that help monitor the health and security of a digital organization. First there are direct, preventative security tools that require no day to day operations involvement that include, but are not limited to:

- Endpoint protection platforms with anti-virus (AV)
- Host based firewall
- Disk encryption
- Virtual private networking (VPN)
- Host intrusion prevention systems (HIPS)

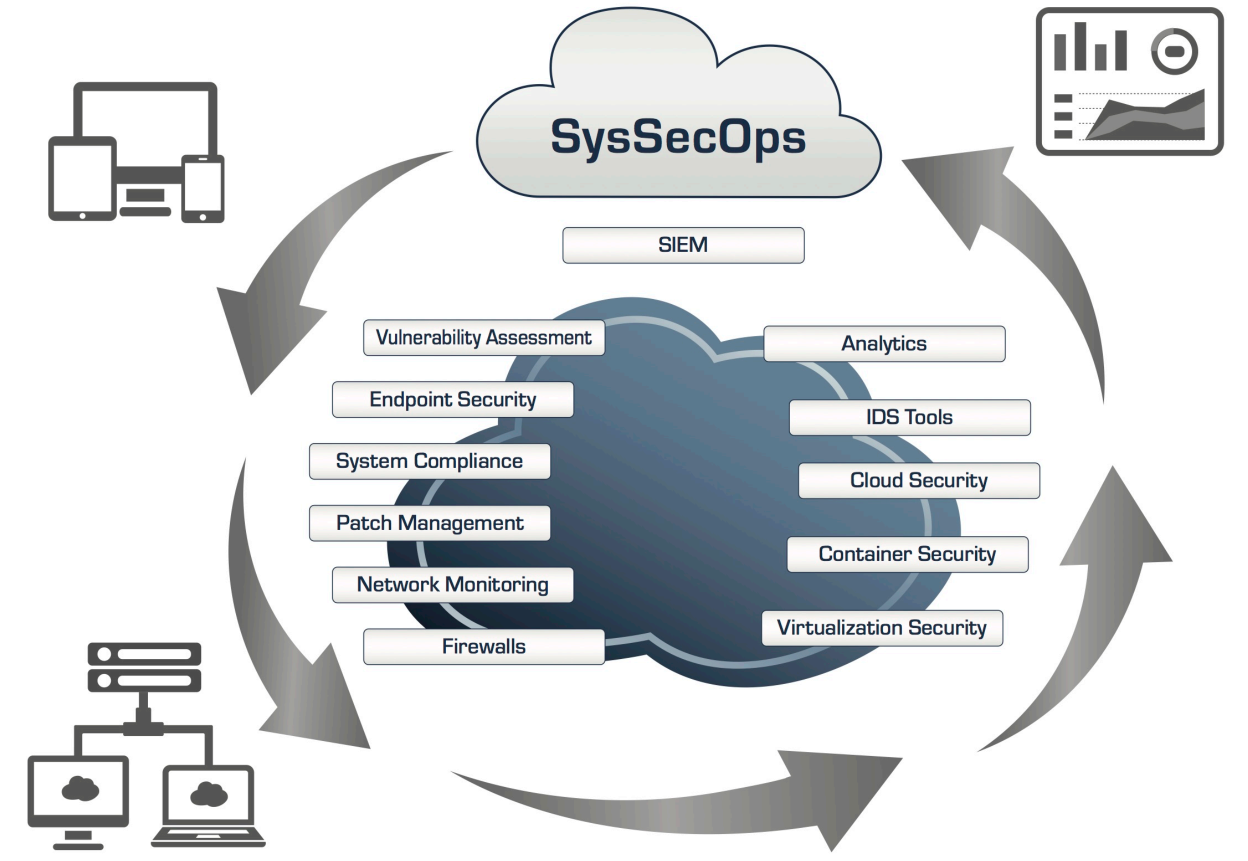
But there are many others used by IT and security teams to monitor and respond to risk and security issues. These tools and capabilities are the ones that require much greater coordination to enable SysSecOps, and include:

- Systems management tools
- Configuration management / system compliance monitoring
- Patch management tools
- Vulnerability assessment (VA)
- User and entity behavior analytics (UEBA)
- Endpoint detection and response
- Malware analysis and sandboxing
- Security information and event management (SIEM) tools

The trend in all of these security niches is further integration, to yield a dynamic ecosystem that works together. The diagram below illustrates how a SysSecOps strategy can tie together many discrete security data and analytics components.

FUTURIOM
THE FUTURE OF TECH

Building SysSecOps



www.futuriom.com

Let’s look at some of the recent trends in some of the most popular categories and how they are evolving to integrate into a best-of-breed SysSecOps solution.

Systems and patch management: Systems management is the process of monitoring and maintaining all the components of an enterprise IT or data center domain. For the purposes of security assessment, this is important for monitoring relevant software and hardware systems to gain visibility into the assets and activity. In addition, patch management is a subset of systems management, to make sure that systems are up to date and include patches that are used to block known security risks, such as updates to operating systems. Configuration management also typically a subset of systems management and delivers a picture of whether systems are configured in a way that complies with organizational policies. This is a natural integration with security functions that can be used to plug known security risks. One example is the recent outbreak of the WannaCry virus, which exploited holes in the Windows operating systems for which there were patches aleady available.

Vulnerability Assessment (VA): Vulnerability assessment provides a critical function in the identification of system risks, but solution capabilities vary when it comes to reporting, analytics, prioritization, and remediation. VA tools go hand in hand with patch management solutions, as patch management is a necessary remediation process that follows the identification of any software vulnerability. From a risk management standpoint, accurate VA intelligence is a requirement for the prevention of most security threats that look to exploit known vulnerabilities in common applications.

User and Entity Behavioral Analytics (UEBA): Endpoint monitoring involves more than looking for vulnerabilities, non-compliant systems, and indicators of infection. More and more it also includes monitoring for abnormal user behaviors or systems behaviors. Insider threats are known to be some of the most dangerous and costly breaches because they are difficult to detect and because legitimate users with data access can often easily exfiltrated sensitive corporate data. Systems behaviors, even performance issues, can often serve as broad or operational indicators of compromise. Thus, integrating UEBA functionality is a critical step in systems and security operations.

Anti-Virus (AV): Everybody has an AV program. These operate by identifying the signatures of known threats and malware — including adware, spyware, phishing attacks, and trojan horses. But the failure of these platforms to stop all threats has ushered the recent growth in endpoint detection and response tools that add to an already crowded endpoint SysSecOps toolkit.

Endpoint Detection and Response (EDR): As stated above, EDR provides detection of threats that manage to evade AV and other preventative security measures. EDR technology should be able to integrate with leading analytics and SIEM products to conduct forensics and provide proactive, automated monitoring, as well as enforcing compliance and examining vulnerability throughout the organization. EDR must provide proactive measures that discover vulnerabilities ahead of time, or at least earlier in the curve.

Malware Analysis and Sandboxing: Sandboxing is a technique that executes untrusted programs or code in a virtualized or segmented software environment to isolate the activity from the host machine. Specific sandboxing tools have been built to analyze malware in an isolated environment. Sandboxing is evolving into a more general technique to virtualize applications so that there is less risk to a host system. For example, in virtualized data centers, entire applications can be run on a sandboxed OS or network segment so that changes don't affect other systems. The integration of these systems with endpoint monitoring can provide timely and enhanced endpoint detection capabilities.

SIEM: Security information and event management (SIEM) systems provide real-time analysis of security alerts generated by network hardware and applications. However, many of these products exist in standalone silos and are not adequately coordinated with other products such as AV, EDR, and firewalls. Integration between security products and SIEM is crucial to getting a complete picture of the entire security footprint. The SIEM, however, is seen by many experts as the natural consolidation point for a wide variety of security-related data – it can be used to build an analytics engine to aggregate and analyze data from all of the systems described below.

"Here's the thing when it comes down to it, the inability to tie security stacks together," says Anthony Cochenour of Hoplite Industries, a security firm that works with Fortune 500 companies and the federal government. "If you are a CIO or a CSO, you might have a variety of security tools such as Proofpoint, QRadar, and FireEye, but they might not log all events the way they need it. All of them need to be rolled up to report into a SIEM."

If one were to summarize the trends in all the security categories described – it's to find ways to connect data feeds and analytics so that all of the tools can be used in synchronicity, to monitor potential problems, analyze data, and eventually become tools for predictive and automated responses to security threats. This is especially true when it comes to systems risk and security management that crosses multiple IT teams and a variety of tools.

SysSecOps is Driving New Requirements

The delivery of a holistic SysSecOps approach requires several capabilities not always present in existing toolsets. One requires a touchpoint to end users devices as well as machines connected to the network, where massive amounts of data about users, systems, applications and network connectivity can be gathered. This data access should be optimized to support a full suite of near real-time risk and security management functions and control. And, as we have outlined, feeding this data into a centralized SIEM and other analytics tools to enhance the value of incumbent tools is key to building a more preventative and detective SysSecOps environment.

Traditional AV is pretty good… they all do a decent job," says Juliano, with Landmark. "But we need things that are more broadly preventative and detective. This requires forensics, visibility and control -- capturing as much data as possible."

In order to achieve this, tools need the ability to work across the enterprise to collect details from all of the endpoints including, remote worker endpoints, non-connected endpoints, and virtualized endpoints such as virtual machines (VMs) in a private data center or public cloud.

The Evolution of Full Visibility Security Stacks

As you can see, one of the key problems among these sets of security tools is they aren't always integrated, and security and IT professionals must choose from an array of screens to watch, rather than being able to monitor the health of IT systems from a "single pain of glass."

"Information security is in crisis and the popular approach to improve this situation is to move to a risk-based model," Jeff Northrop, CTO at the International Association of Privacy Professionals, told Cyber Security Intelligence. "Currently, we have business intelligence tools, data integration tools, data discovery tools, data encryption tools, compliance tools, and SIEM tools. All require that foundation for a data security intelligence tool; that is, an understanding of what data is collected; where it's located; how it's structured, categorized, and used; and who has access to it," Northrop says. "Most vendors operate in one or two of these areas; but a few companies have recognized a need for better information on the data they're responsible for protecting; therefore, taking advantage of their platform to extend their products to meet this need."[6]

[6] Top Security Tools to Fight Against Cybercrime, Cyber Security Intelligence, May 5, 2015; https://www.cybersecurityintelligence.com/blog/top-security-tools-to-fight-against-cybercrime-315.html

It makes sense to have a focal point for this data integration. Integrated endpoint data in a SysSecOps enabled tool is a perfect first step. Tools that provide a single view of systems operational and security intelligence are new to the market, but growing quickly. Companies like 1E, Ivanti, Micro Focus, Tanium, Ziften, and others are rapidly growing solutions that address the requisite SysSecOps visibility, control and integrations capabilities.

Traditional EDR vendors are well positioned to take advantage of this SysSecOps trend. But most focus solely on threat detection and have not incorporated the need to integrate / coordinate both risk management and threat detection operations.

Integrating endpoint data from these SysSecOps tools into the SIEMs provides an even higher layer of integration looking universally across both systems security, and network security. It can also serve as a single point for aggregating all systems or endpoint risk and security alerts for coordinated IT and security incident response.

In our survey of end users and executive managers, integration was flagged as a major barrier to solving important security challenges. For example, asked, "What would be the most helpful in improving IT security in your organization? (choose as many as two)," 31% of responses cited "Better integration between systems management and security operations tools."

This desire has been confirmed in many other places. In the ESG report, "Tackling Attack Detection and Incident Response," nearly 80 percent of the respondents believe the lack of integration and communication between security tools creates bottlenecks and interferes with their capability to detect and respond to security threats.

Security and IT management specialists we interviewed, in addition to the data we gathered from our end-user survey, indicate that integration of reporting, visibility, and logging features is crucial to a high-performance security system.

There are key features and capabilities to look for in technology products to figure out whether they will solve the SysSecOps challenge. Here are some examples:

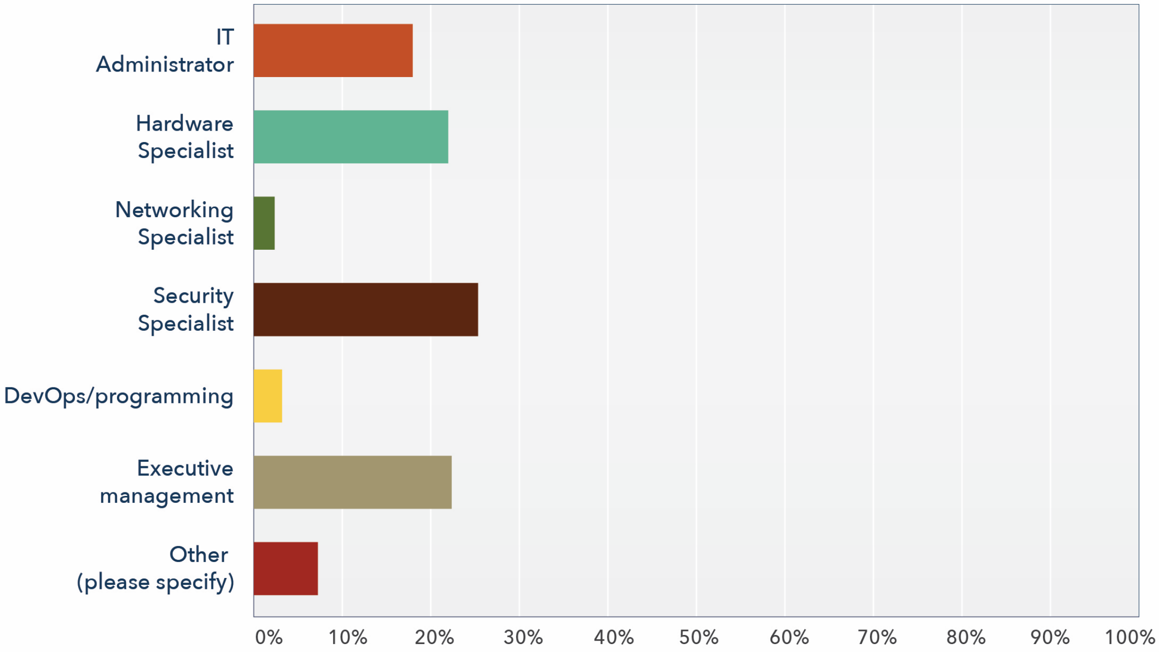
- Do the products share their data and integrate with data analytics platforms or the SIEM?
- Do the products support the coordination of IT and security teams in managing endpoint risk and security?
- Do the tools work across all operating systems: Mac, Linux, and Windows, both on and off network?
- How do the products help provide context to alerts from network and applications monitoring tools – or vice versa?

Endpoint Visibility for SysSecOps: What Users Want

To get a better vision of what is needed to drive better data collection and analytics to produce a stronger SysSecOps toolkit, Futuriom reached out to end users and executive management to gauge their perception of security challenges and potential solutions.

End-users, including IT administrators, hardware specialists, networking specialists, security specialists, DevOps staff, and executive staff were targeted via social media and email outreach. The survey gathered results on five questions from 149 participants. The breakdown of the audience was such:24.8% security specialists; 22.8% executive management; 22% hardware specialists; 18% IT administrator; 3.4% devops/programming staff; 2.7% networking specialist; 6% other.

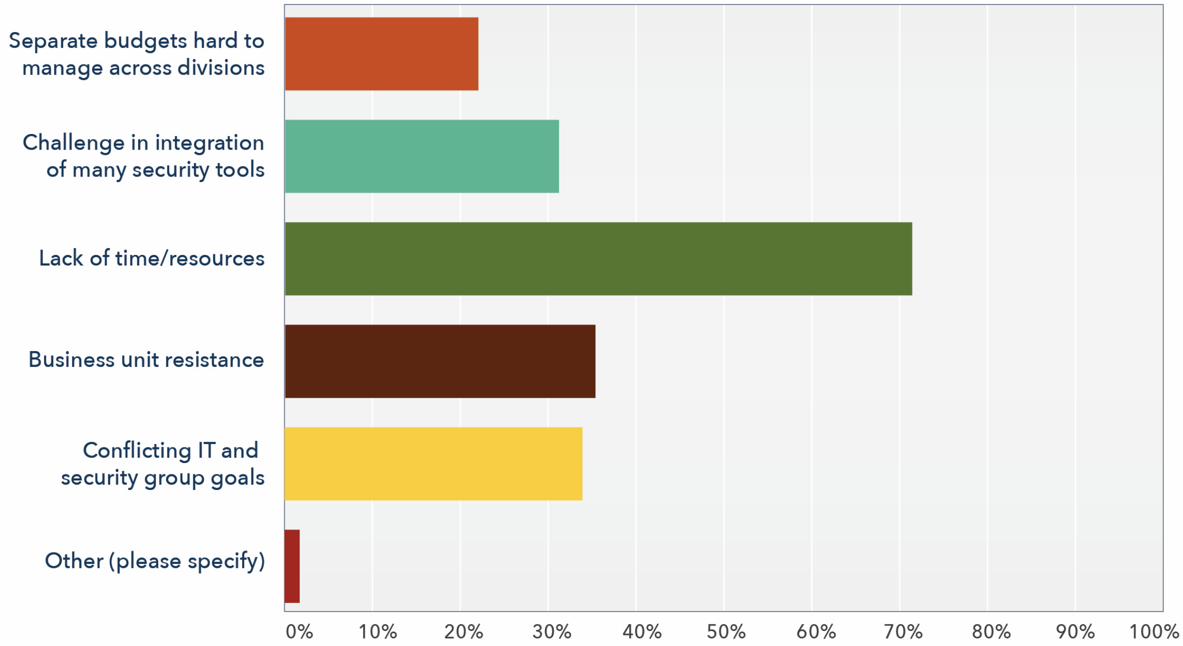
Q1: Which of the following best describes your IT role?



Answer Choices	Responses	
IT Administrator	18.12%	27
Hardware Specialist	22.15%	33
Networking Specialist	2.68%	4
Security Specialist	24.83%	37
DevOps/programming	3.36%	5
Executive management	22.82%	34
Other (please specify)	6.04%	9
Total		149

Respondents were asked about the top challenge to creating an integrated security strategy across the organization. This is what we found:

Q2: What are the top challenges to creating an integrated security strategy across the organization?

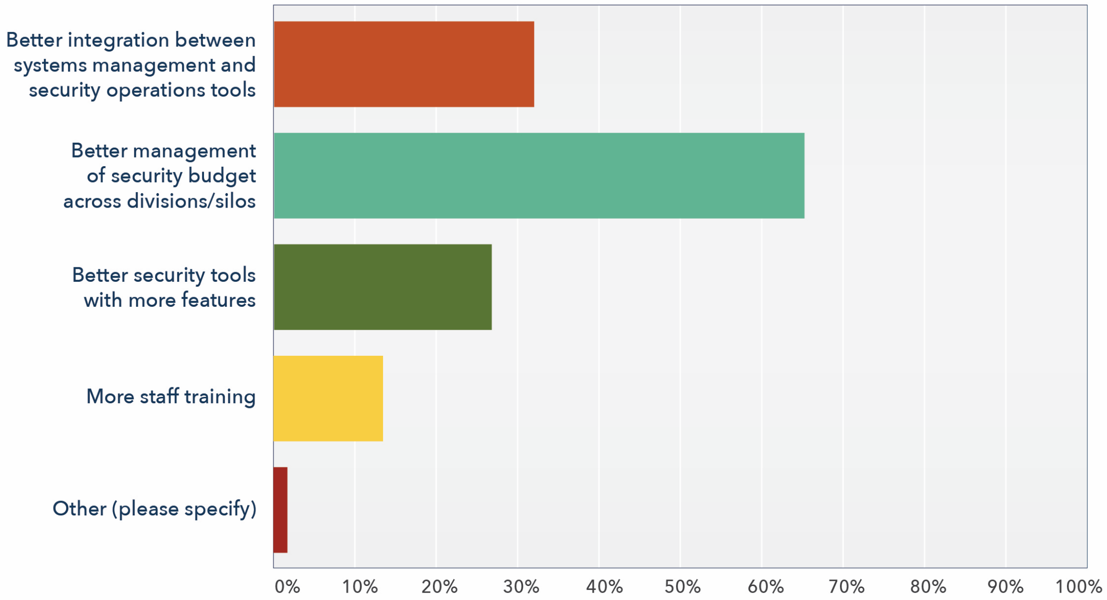


Answer Choices	Responses	
Separate budgets hard to manage across divisions	22.76%	33
Challenge in integration of many security tools	31.03%	45
Lack of time/resources	71.03%	103
Business unit resistance	35.17%	51
Conflicting IT and security group goals	33.79%	49
Other (please specify)	2.07%	3
Total Respondents: 145		

Survey respondents were asked to pick up to two responses, giving more depth to our understanding. As you can see, many challenges overlapped, but not surprisingly the lack of time/resources was cited as the #1 challenge, with 71% of respondents selecting. The next three most popular choices were "business unit resistance" (35%); conflicting IT and security group goals (34%), and "challenge in integration of many security tools" (31%). The selections were rounded out by "separate budgets hard to manage across divisions (23%) and other (2%).

The next question is how to solve some of these challenges? In Question 3, we asked what the most helpful approaches to improving security would be.

Q3: What would be the most helpful in improving IT security in your organization?



Answer Choices	Responses	
Better integration between systems management and security operations tools	31.03%	45
Better management of security budget across divisions/silos	64.83%	94
Better security tools with more features	26.90%	39
More staff training	13.10%	19
Other (please specify)	1.38%	2
Total Respondents: 145		

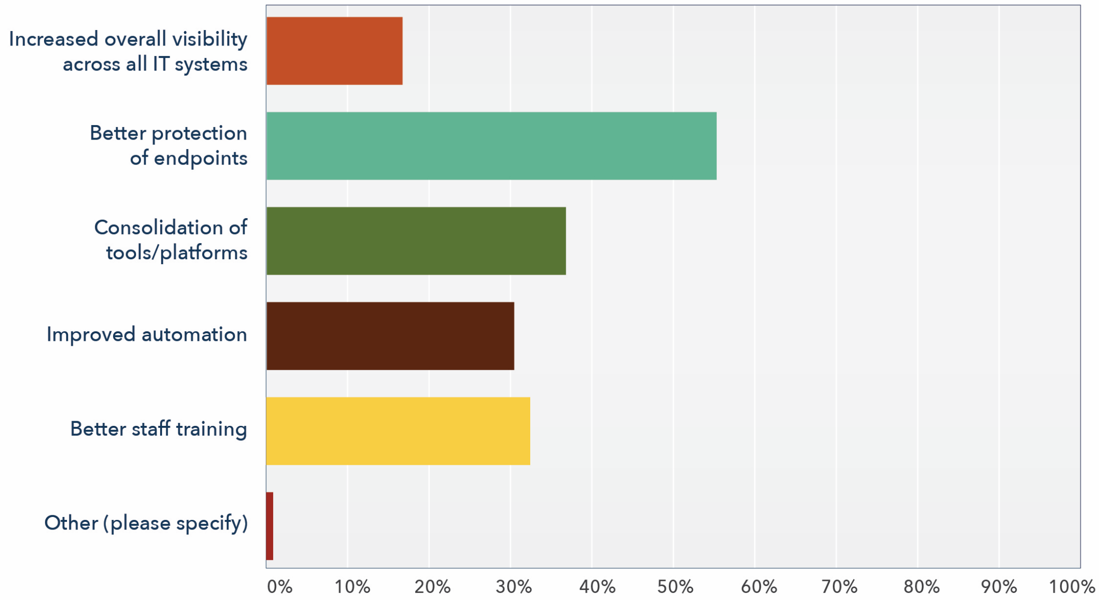
In an interesting result, respondents made it clear that managing budgets across organizations was a challenge. This is because organizations are challenged by often have separate IT and security management budgets that aren't always coordinated. A broad majority, or 64.83% of survey respondents, chose "Better management of security budget across divisions/silos" as one of the top goals in improving security infrastructure. Next in line was "Better integration between systems management and security operations tools," at 31.03%; "Better security tools with more features," 26.90%; and more staff training 13.10%.

What's notable about these responses is that the budgets and integration of tools are related. One of the key trends in security is an increased need to integrate data into a central repository so that activity can be analyzed and automated. Converging

SysSecOps capabilities allows IT and security teams to benefit for the same tools for endpoint protection. But today's fragmented budgets often result in the purchase of narrowly focused, siloed tools for monitoring, management and security. Therefore, it's going to be more important over time for organizations to coordinate their IT and security budgets to address the SysSecOps integration need.

The next question, Question 4, is useful for identifying the overall goals.

Q4: Which of the following are among your top security goals? (results on following page)

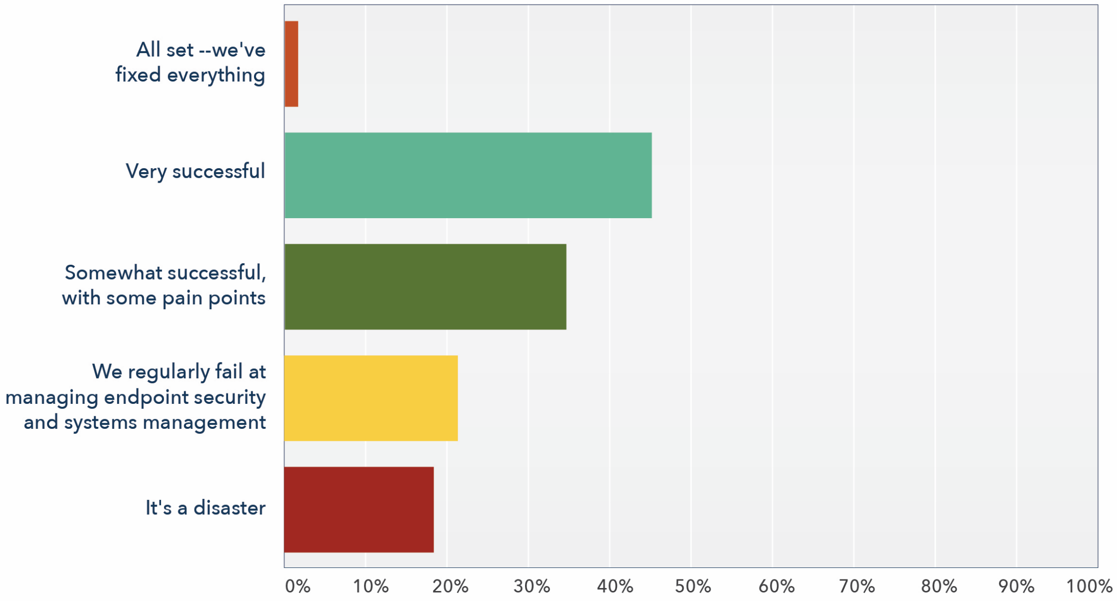


Answer Choices	Responses	
Increased overall visibility across all IT systems	16.44%	24
Better protection of endpoints	54.79%	80
Consolidation of tools/platforms	37.67%	55
Improved automation	30.14%	44
Better staff training	32.88%	48
Other (please specify)	.68%	1
Total Respondents: 146		

The number one goal cited by respondents is "Better protection of endpoints" cited by 55% of respondents (multiple response allowed). This indicates that even though respondents have made clear their desire for integration, they see endpoint security as a key area in the security portfolio. This makes sense as endpoints are natural places to collect and observe data on network and applications activity and can be used to assess and monitor risks. The next most oft-cited goals are "consolidation of tools/platforms" at 38%; and "Better staff training," at 33%. These results are in line with the themes of the responses to other questions which stress organization and technological integration and consolidation of the SysSecOps tools.

Finally, it's useful to see how organizations view their success in managing security and moving to an integrated SysSecOps approach. It's clear that more progress is needed, because only 3% of respondents replied that they have "fixed everything." The largest group, 44.53% of the respondents, characterized their mission as "very successful," and 34% said they are "somewhat successful, with some pain points." Twenty-one percent said they "regularly fail at managing endpoint security and systems management." And finally, a not-so-small number of respondents -- 18%! -- described the mission to provide overall endpoint/systems management as a "complete disaster." Clearly there is more work to do!

Q5: How successful do you consider your organization at overall endpoint / systems management?



Answer Choices	Responses	
All set -- we've fixed everything!	2.92%	4
Very successful	44.53%	61
Somewhat successful, with some pain points	34.31%	47
We regularly fail at managing endpoint security and systems management	21.17%	29
It's a disaster	18.25%	25
Total Respondents: 137		

Conclusion: Leading the SysSecOps Future

Our investigation into the needs for SysSecOps have revealed many interesting trends, among them the requirement to integrate existing systems management and security tools, coordinate budgeting and planning across organizational boundaries, and focus on using endpoint visibility data to drive analytics improvements for building predictive detection of security and system risks.

But how does one do that? It's clear from a look at the major security and systems failures of the past few years that such an approach requires strong leadership across the organization, driven from the executive and board level of the organization. If the leadership of the organization does not realize these critical goals, a SysSecOps approach cannot emerge and thrive .

Some key elements of a SysSecOps strategy include:

- IT and security professionals are asking for better integration of tools, which requires coordination of organizational budgets and planning
- To achieve SysSecOps integration, systems management and security budgets need to be coordinated across organizational boundaries to plan for the required technology components.
- The emphasis on technology should be toward building coordinated data-collection and analytics engines.
- SysSecOps for endpoints is built on a foundation of endpoint visibility, control and integration within a broader security ecosystem.
- Finally, an integrated SysSecOps strategy needs to be developed and coordinated within the organization – across divisional boundaries including systems management, and security – and driven from the highest levels of the organization.

Coordinated SysSecOps visibility has already proven its worth in helping organizations assess, analyze, and prevent significant risks to the IT systems and endpoints. If these goals are pursued, the security and management risks to an IT system can be greatly diminished.