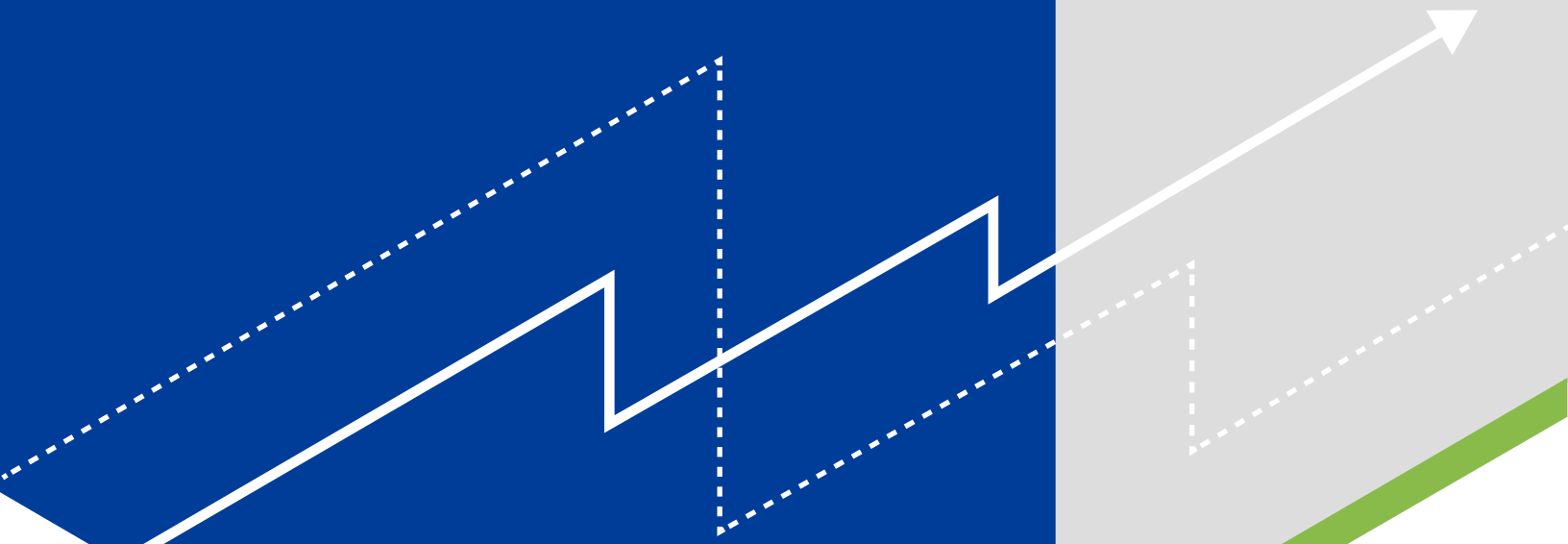
A Forrester Consulting
Thought Leadership Paper
Commissioned By Endgame

July 2017

Achieve Complete Breach Intolerance Through SOC Transformation

Simplify Operations And Empower Your Staff To Fight Targeted Attacks



FORRESTER®

Table Of Contents

Project Director:
Sarah Brinks,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Nearly 40% of organizations experienced three or more types of attacks in the last year

Ninety-one percent of survey respondents said that achieving complete breach intolerance was important to their company.

Executive Summary

Successful, targeted attacks, such as the "WannaCry" malware attack in May 2017 or the "Petya" ransomware attack in April 2017, are happening with alarming frequency. Yet organizations are not moving with equal speed to secure their systems and data. It is time for organizations to not only catch up or keep up but to plan against future attacks. Having a fully staffed security operations center (SOC) that is equipped with the right tools and backed up by a strictly followed set of processes to stop targeted attacks is critical.

In May 2017, Endgame commissioned Forrester Consulting to evaluate whether and how enterprises are transforming their SOCs as they face a new generation of attacks, and explore the opportunity to invest in a comprehensive endpoint security platform to overcome their challenges while preventing future attacks. Forrester conducted an online survey with 156 respondents and three interviews with security decision makers from large US enterprises in technology, financial services, oil and gas, and energy industries. Forrester found that companies are encountering many types of breaches as often as every day. Organizations fear the high costs associated with severe breaches as well as the potential damage to their brand and reputation. It is clear that enterprise security teams must make fundamental changes to their staff's skillsets, processes, and tools to achieve complete breach intolerance.

KEY FINDINGS

- **Breach elimination is key to companies.** Ninety-one percent of survey respondents said that achieving complete breach intolerance was important to their company. Complete breach intolerance was defined in the survey as: stopping all attacks before there is damage to systems or data loss. In order to try to stop all breaches before they result in damage or data loss, organizations are investing in endpoint security software, automation, employee training, and compliance mandates.
- **Staff without the right skills or training leave a gap.** Most SOCs are not fully staffed; only 44% of organizations have an analyst at the tier 1 level or higher (an incident responder and first-line support to advanced support). Another 44% of survey respondents agree that they need to improve their staff's technical skills around endpoint security in order to achieve complete breach intolerance. Many categorize their staff's proficiency as only competent on a scale from beginner to expert. Companies are looking for ways to add skills to their SOC team with automation and training to fill the gap.
- **The cost of severe breaches is too high to accept.** Companies fear a severe attack that results in damage and data loss. Today, SOC teams are using many tools to stop threats, but current strategies fail to prevent these targeted attacks. Improving workflows and lowering false positives can lead to key benefits such as rapid identification and remediation of threats.

Organizations Are Treading Water To Stay Afloat In A Sea Of Attacks And Breaches

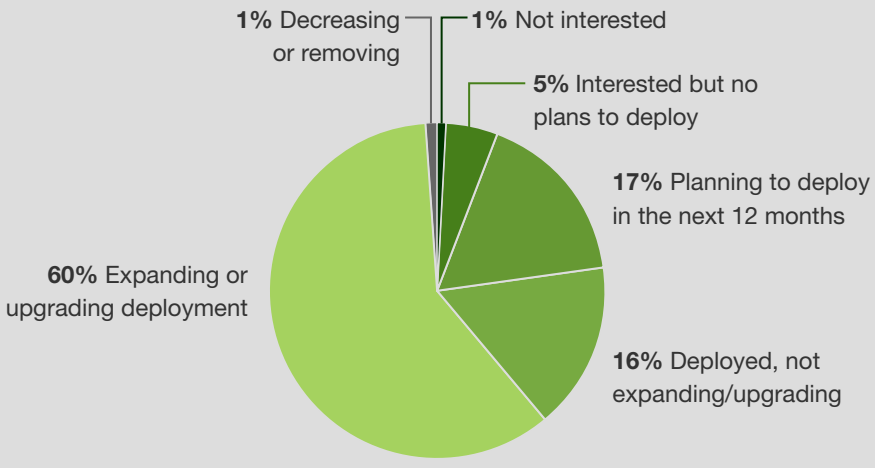
Security operations centers are a key part of enterprise security environments. According to our survey of 156 security professionals, 60% of organizations are expanding or upgrading their current SOC deployment (see Figure 1). These organizations need their SOCs to be working at peak performance, as nearly 40% of survey respondents experienced three or more types of attacks (such as: phishing, malware, and targeted attacks) in the last year, and many experience those attacks on a daily basis.

Our study showed:

› **Companies prioritize the most common and dangerous attacks.** As companies address their daily attacks, they have to concentrate on the most severe threats to their business. Forty-six percent of survey respondents have experienced phishing attacks in the past year, and 44% have experienced a targeted endpoint attack. For example, one of our executive interviewees, a chief information security officer (CISO) of a US banking company, is most concerned about targeted attacks and phishing. Despite the fact that about 93% of the company's email gets blocked, some phishing still gets through. The CISO of a global energy company has different concerns. He is most focused on third- and fourth-party breaches and organized crime. Organizations based out of China and Russia attempt to extort, steal, or blackmail them to get money. Similar to what happened in the 2013 major retail chain breach, this energy company fears that a breach of vulnerable third and fourth parties with security weaknesses could reach their systems.

Figure 1

"What are your organization's plans when it comes to security operations center transformation?"



Base: 156 US-based application IT security decision makers at companies with 1,000+ employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Endgame, May 2017

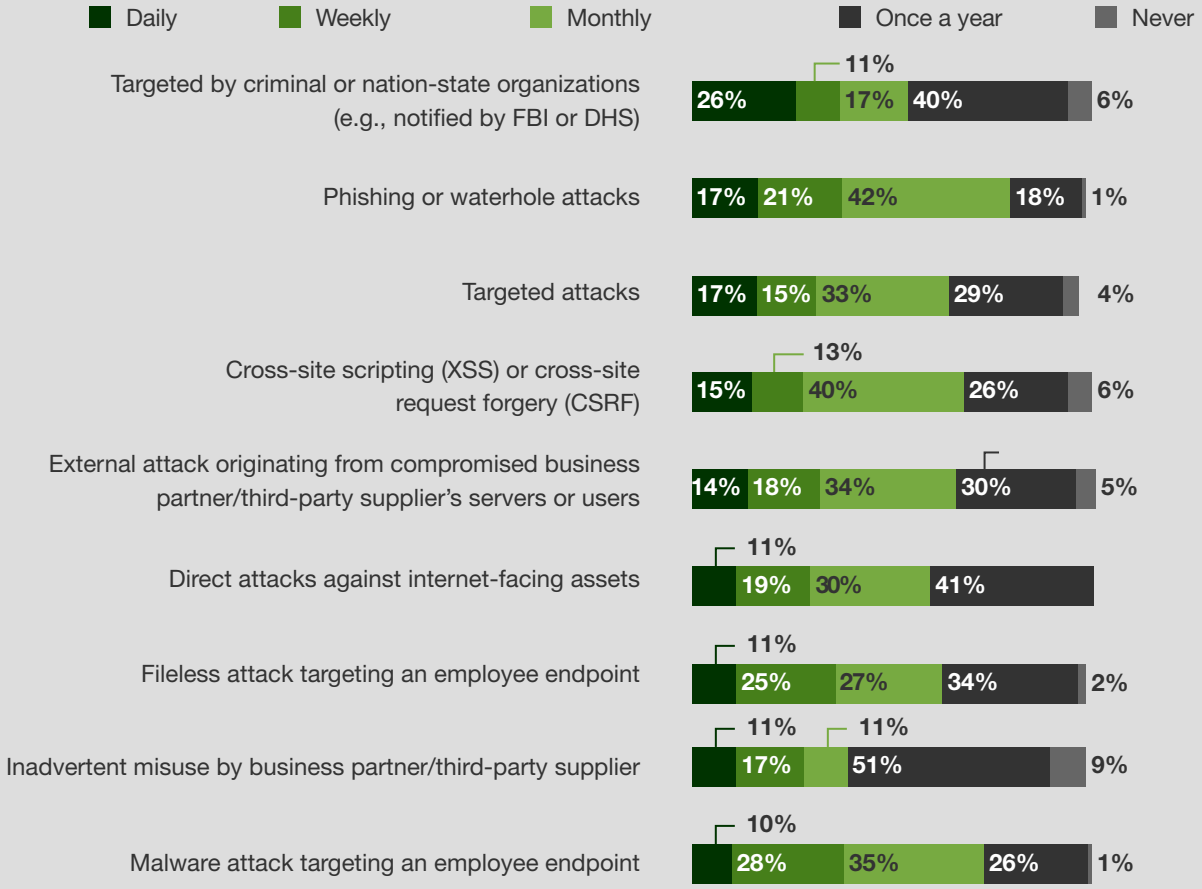
FORRESTER®

› **Targeted attacks continue to hit organizations.** Over a quarter of survey respondents are targeted daily by criminal or nation-state organizations. The CISO of a global energy company experiences hundreds of phishing attacks daily. Almost all organizations surveyed experience malware attacks targeting an employee endpoint, and nearly three-quarters experience them at least monthly (see Figure 2). Organizations are taking different steps to confront these daily attacks. Over half of the organizations surveyed are investing in tools to detect and block ongoing endpoint attacks, and 45% are investing in software/tools to discover and reduce network vulnerabilities. An information security officer (ISO) at a US-based energy company believes that active penetration testing is the key to stopping attacks. During our interviews, this ISO told Forrester: "If we are not doing pen testing and actually generating those activities the attacker is hunting for, how are we going to know how to find them? You won't know what they look like, and if you do the pen testing, you'll know what's really behind it. You'll know what the attacker's intent was, because you'll remember what your intent was behind the test. It's training your team to think like an attacker."

› **The threat is real.** Ninety-two percent of survey respondents have experienced at least one successful attack or data breach that put their organization at risk in the past year. Nearly a third of organizations experienced 20 or more successful attacks (see Figure 3). The type of attack that organizations are most concerned about ranges from phishing to spyware to the exploitation of OS vulnerabilities. Organizations have real concerns about their ability to keep their systems and data secure. For example, 66% agree that their current visibility into endpoint behavior is lacking the depth and breadth required to detect zero-day malware/targeted threats. Seventy-three percent of respondents agreed that though they are interested in acquiring deeper visibility into endpoint behavior, they lack the staffing expertise to respond to detected events. The CISO of a US banking company is concerned about how long it takes to stop a breach once malicious behavior has been detected. Combined with the high volume of alerts they receive, it is hard to keep up.

Figure 2

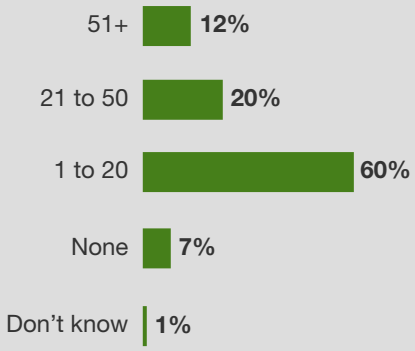
"How often do the following types of breaches occur at your organization?"



Base: 156 US-based application IT security decision makers at companies with 1,000+ employees
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Endgame, May 2017

Figure 3

"How many security incidents (e.g., successful attacks, data breaches, etc.) have put your organization at risk (whether publicly announced or not) in the past 12 months?"



Base: 156 US-based application IT security decision makers at companies with 1,000+ employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Endgame, May 2017

FORRESTER®

Complete Breach Intolerance Is Key To Stopping Damage And Loss

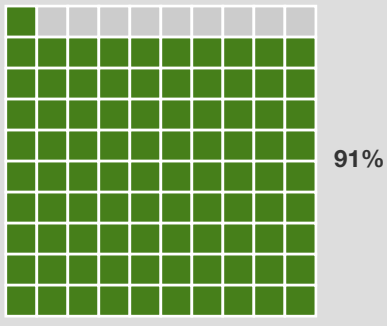
Ninety-one percent of organizations feel that reaching complete breach intolerance at their organization is important. Though the majority of organizations have a goal of complete breach intolerance. When they are asked to rate their tools, staff, and processes their level of tolerance for breaches increased. Organizations are most willing to accept breaches that come from their tools (see Figure 4). Fifty-seven percent of organizations have high to moderate tolerance for breaches from tools, and 48% have high to moderate tolerance for breaches from processes or personnel. (High tolerance was defined as: "We accept that breaches will occur since we are unprepared to stop them." Moderate tolerance was defined as: "We are actively trying to reduce breaches while recognizing more can be done to stop them.")

Our survey and interview results revealed:

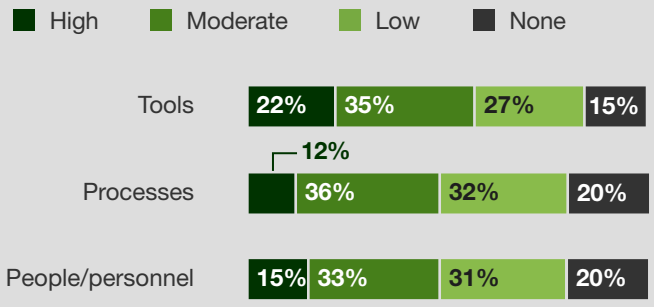
- **The existential nature of attacks is well known.** Sixty-four percent of the companies surveyed are concerned that the next breach or attack they experience could be somewhat to significantly severe. That fear is coupled with the fact that many IT security decision makers do not know the system or the vector that will likely be attacked next. Seventeen percent of survey respondents feel the system or vector is not predictable at all.
- **Weakenesses in tools, processes, and people hinder complete breach intolerance.** Figure 4 shows tools are where organizations have the lowest breach intolerance. But they feel that their processes are the least qualified aspect of their organization to achieve complete breach intolerance. Fifty-two percent of organizations have low to zero tolerance for breaches coming from their processes. Aware that this was an opportunity for growth, the CISO of a US banking company told Forrester: "This year we're focusing our energy on the processes. I'm

Figure 4

"How important is reaching complete breach intolerance to your organization?"
(Somewhat to very important)



"Thinking about your organization's current tolerance for security breaches, how would rate that tolerance within the following areas of your organization?"



Base: 156 US-based application IT security decision makers at companies with 1,000+ employees
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Endgame, May 2017

talking about optimizing our tools, so we feel we have adequate tools in place. Other processes that we've continued to work on are vulnerability management and task management." While the CISO of a global energy company was focused on staff and tools, "It's definitely difficult to get the right people in the right positions without having to train them yourselves. I'm not overly excited about our technology. There's an over-complexification of security tools that I'm trying to drive out. Put simply, complexity breeds insecurity."

- **There is uncertainty around the severity of the next attack and its consequences.** To say IT security professionals live in a state of fear may not be as hyperbolic as it seems. Sixty-four percent of survey respondents believe that the next security breach/attack on their organization could be somewhat to significantly severe. Only 8% said they believe that the next security breach/attack on their organization could not be at all severe. The consequences of a severe breach can be costly, as we saw with the WannaCry attack. IT decision makers fear a loss of revenue and damage to their company's brand and reputation as a result of a successful breach. The CISO of a US banking company told Forrester: "We have a large presence in our community; if we had a major breach, it would really be detrimental to our brand. Our reputation would be ruined for the most part."
- **Organizations are focusing on improving their prevention capabilities.** Survey respondents are taking steps to counter attacks that threaten damage to systems and loss of data. Over half of the survey respondents who fear the next security breach/attack on their organization could be somewhat to significantly severe are looking to improve their endpoint threat prevention capabilities. Other steps include initiating vulnerability assessments, making technology improvements, and training/hiring staff with sufficient skills (see Figure 5).

> "If you look at security holistically, and you have a strong endpoint protection and you have a strong security infrastructure . . . the next piece of the puzzle is access control. Making sure the right person has access to the right data at the right time. If you have all the protections in the world and a bad guy assumes your identity, none of it matters."
>
> *CISO of a global energy company*

Figure 4

"You said you believe the next attack on your organization could be somewhat to significantly severe. What steps are you taking to counter the attacks?"

Base: 99 US-based application IT security decision makers at companies with 1,000+ employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Endgame, May 2017

FORRESTER®

Find The Right Tools And Staff

A consistent theme that emerged in the online survey and telephone interviews is that IT decision makers are struggling to fully staff their SOC with qualified people and select the right tools without succumbing to over-complicated processes and alert fatigue.

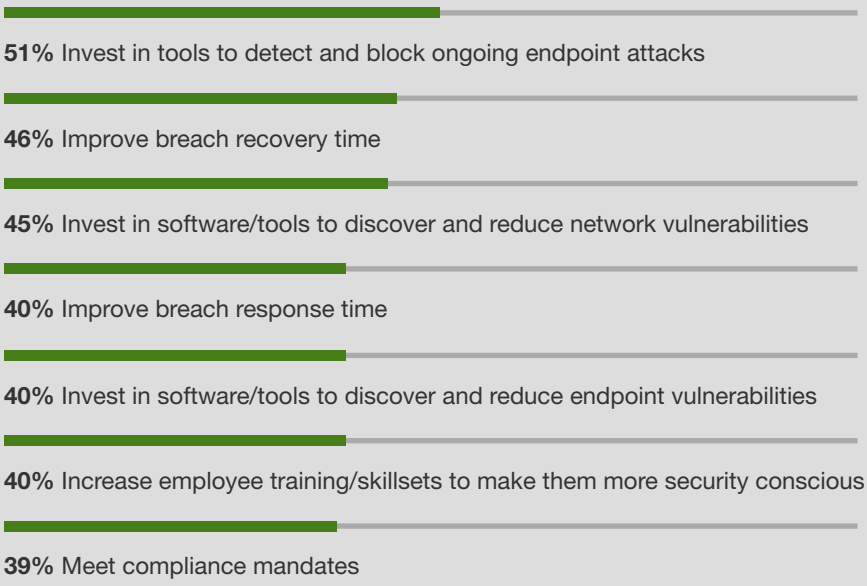
FIND UNIFIED TOOLS TO REDUCE COMPLEXITY

Our research shows:

› **Companies struggle with inadequate tools and unnecessary complexity.** When survey respondents were asked where they were most willing to accept breaches from they said their tools, fifty-seven percent of organizations accept that breaches will occur as a result of the tools they use. Only 15% of organizations said they have no tolerance for breaches from their tools (meaning they have zero tolerance for breaches and have done everything possible to prevent them), and 27% said their tolerance was low (meaning they are trying to prevent all breaches from occurring while recognizing a determined adversary may still get past their defenses). This is compounded by the fact that 71% are using five or more technologies in their SOC and a third of respondents are using eight or more technologies. The CISO of a global energy company said: "What I'd like to do is reduce the overall risk footprint, thus being able to reduce the number of tools. There's a lot of work that we're doing to try to reduce overlap of tools." Organizations are looking for the right tools to help them prevent, detect, and respond to ongoing endpoint attacks as well as discover and reduce their network vulnerabilities (see Figure 6).

Figure 6

"What are your organization's goals to achieve complete breach intolerance?"



Base: 141 US-based application IT security decision makers at companies with 1,000+ employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Endgame, May 2017

FORRESTER®

› **Reducing complexity saves time and money.** IT decision makers want to reduce their SOC complexity, allowing their staff to focus on genuine security work rather than chasing down a lot of unnecessary alerts and software malfunctions. The CISO of a global energy company said: "It is hard to cut through all that fog and try to find the gems in all the stones. That's one of the reasons why I'm trying to push this to the cloud." The CISO of a US banking company said that one of their SOC's biggest challenges is the number of alerts they get every day, noting: "My staff is pulled in all different directions. The SOC may not be a full-time job for them. It primarily is, but they get pulled on to other things that they're having to deal with those, too. They're supposed to be watching alerts, but they are also managing the tools as well."

FIND THE RIGHT STAFF WITH THE RIGHT SKILLS

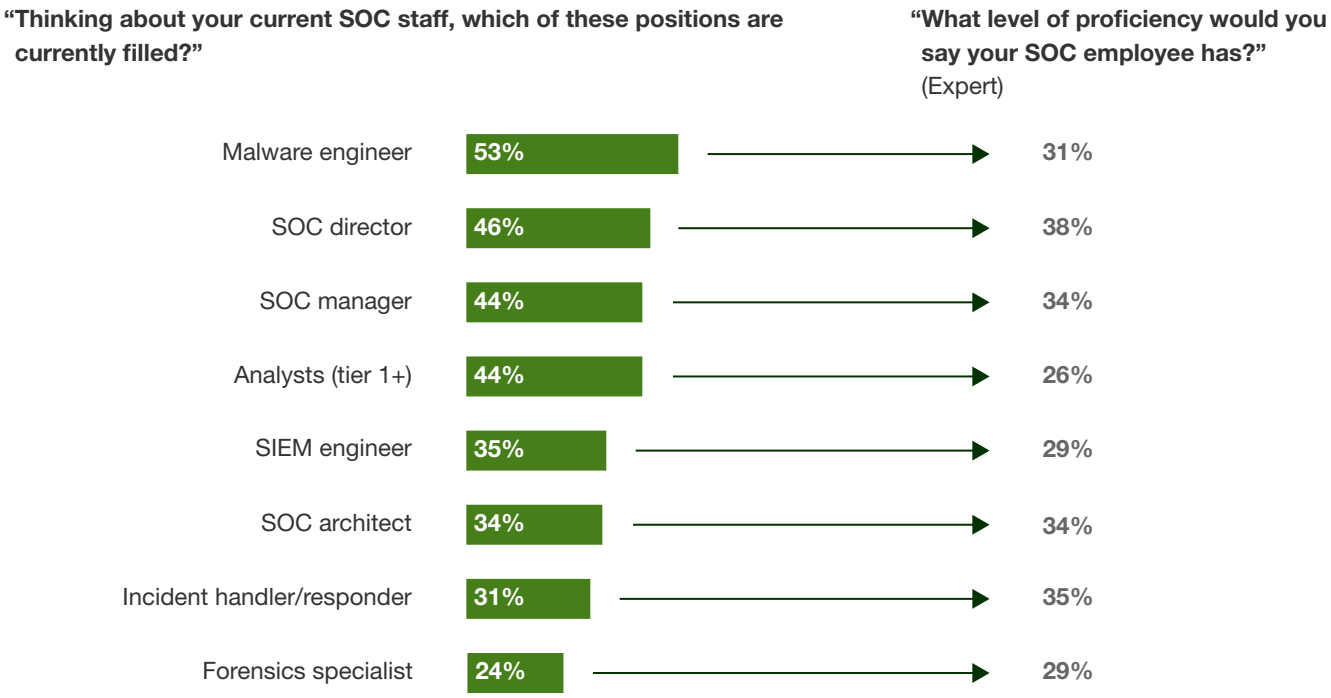
› **Improved endpoint security and threat intelligence skills are crucial.** Forty-two percent of respondents listed employee skillset improvement as their top option to help their organization limit security breaches. Specifically, they are looking to grow their staff's endpoint security technical skills to achieve their desired level of complete breach intolerance.

› **A competitive market makes hiring staff with the right skills challenging.** Our survey and interviews show that organizations are struggling to hire fully qualified staff for their SOCs. It often isn't a matter of salaries or incentives; there is simply a draught of qualified security staff available (see Figure 7). The ISO at a US-based energy company is taking a new approach: "I'm doing something that I didn't think I would do last year in that the staff that I have right now and the staff that I'm going to be hiring have six months' experience or less in security. Before I was trying to go for the upper end. The more expensive 10-year, 15-year veterans. What I was finding in them, for lack of a better word, is they were content. Less experienced employees want to learn and grow." The CISO of a US banking organization who earlier lamented his staff not being able to solely focus on security work also said: "A bigger staff would help my team do their jobs better. They get a lot of drive-bys, where people come by and ask for help. That distracts them from what they really need to be doing. Because we're short staffed, that keeps us from optimizing some of the tools that they need to optimize." This sentiment was also echoed by the CISO of a global energy company: "I think the biggest challenge that we've been facing is trying to get the right level of expertise. Let's start with the people first, getting the right people in the right positions and getting them trained. It's very, very hard for us to find people that are experts in the field to come in and work with us."

"What I've found most organizations do very poorly and that makes it hard to find staff is they combine the job with other responsibilities. What they should be is a threat hunter and a threat responder. But they also give them the job of compliance person and then also give them the responsibility of project manager. They're spending 90% of their time doing nonsecurity work. We're funded well, so my staff only have to do security. I just have to find people that can hunt and respond to incidents. They don't have to wear all these other hats and they don't have to get burnt out with all these other jobs."

Information security officer at a US-based energy company

Figure 7



Base: 156 US-based application IT security decision makers at companies with 1,000+ employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Endgame, May 2017

Achieve Complete Breach Intolerance

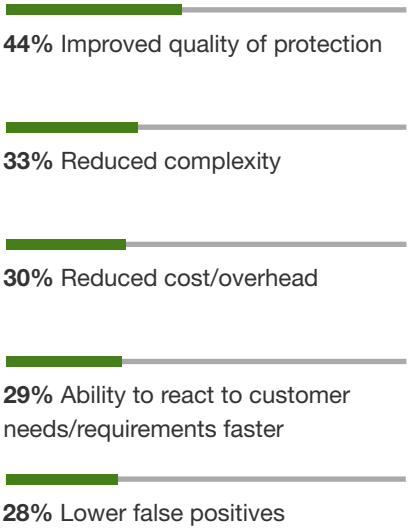
It is critical for security decisions makers to make sure their staff, tools, and process can stop targeted attacks today. It is necessary to equip the SOC team with the right tools and skills. The right tool is one that focuses on complete attack life-cycle protection as well as automates investigation and triage to empower SOCs to respond before any system damage or data loss occurs. Having an SOC performing at peak efficiency has benefits for the business, not just security (see Figure 8).

Our survey respondents agree:

- **Improving endpoint security strategy helps resolve attacks without losing vital data.** Forty-four percent of survey respondents agree that they need to improve their staff's technical skills around endpoint security to achieve complete breach intolerance. Organizations are looking to reduce their vulnerabilities as well as build more automation between endpoint prevention, detection, and response capabilities, and they are using continuous monitoring to stop advance threats. Other ways they are improving their strategy is by integrating endpoint security with network security for reduced operational friction.
- **Targeted attacks are sophisticated and must be dealt with aggressively to stop system damage and data loss.** Organizations are experiencing targeted attacks with alarming frequency, yet they delay the necessary steps to meet those attacks head on. Organizations agree that achieving complete breach intolerance is very important, but are they doing enough? The CISO of a global energy company works hard to create a security-aware culture within the organization: "Everyone in the company has to pass the user awareness test every year. We change the questions on it every two years to keep it fresh. We write a lot of articles and we publish them throughout the company, we put them in the company magazine, we put them in the seat backs of the company jet, we have them up on the monitors that are in the hallway, we create poster boards, put them up on easels next to the elevators, and we do training." A reduction in the number of tools the CISO of a US-based banking company uses would allow his staff to be more strategic: "Reducing complexity of our environment would free the staff up to work on some segmentation projects that we might need to do, so we could segment our network a little better. It would also allow us to shift our team to a more strategic approach of things instead of even just on a day-to-day basis. They could think more strategically instead of just big architecture planning. They can explore how this affects the day-to-day work they're doing, then affect the strategy, and what they should then do to change that strategic objective or the strategy moving forward."

Figure 8

"What benefits have you achieved/would you expect to achieve as a result of partnering with a security vendor to run or augment your security operations?"



Base: 156 US-based application IT security decision makers
Source: A commissioned stat companies with 1,000+ employees conducted by Forrester Consulting on behalf of Endgame, May 2017

› **Simplification cuts back on nonsecurity work.** The information security officer at a US-based energy company agreed: “Lowering our false positives lowers our head count because we don’t need as many people watching. That saves us money.” Twenty-eight percent of survey respondents achieved lower false positives because of partnering with a security vendor to run or augment their security operations (see Figure 8). The CISO of a US-based banking company feels, “Alert fatigue is a challenge. If my staff had time to take a look at our architecture, we would be able to reduce the number of tools that we had, or number of providers we had, and really look at things from a holistic approach and not a point solution-type approach. We would reduce the number of vendors we’re using, which then in turn would reduce the alerts or reduce that fatigue.”

Enterprises are transforming their SOCs to block targeted attacks. They must seek out tools that not only provide endpoint security and block vulnerable systems but also build their staff’s skills and grow their expertise, while reducing complexity and maximizing efficiency. Organizations must find the right mix of prevention, detection, and remediation of threats to achieve complete breach intolerance.

Key Recommendations

Forrester's in-depth survey of IT security decision makers about security operations centers' challenges and barriers yielded several important recommendations:

Strive for complete breach intolerance with a strong prevention-first strategy. Targeted attacks continue to plague organizations, and these intrusions damage the brand, customer loyalty, and margins. Preparing for and responding to these attacks requires a focused and resolute strategy of complete breach intolerance to stop system damage and data loss. While detection technologies are very popular today, the best way to efficiently achieve complete breach intolerance is to build a strong layer of prevention-focused controls to lower your organization's attack surface in the first place. This will lower the number of incidents that your SOC staff need to deal with and reduce the "noise" seen by detection-focused tools. Finally, ensure your leadership understands the risk a single breach can have on your business and that your goal is to ultimately build resiliency to quickly respond to and recover from targeted attacks.

Reduce your internal friction through integrated endpoint prevention, detection, and remediation. Many organizations invest in point products for each core endpoint requirement (threat prevention, detection, and response), with little integration or automation between the three. If you don't establish a solid foundation of automation and orchestration, blind investments in prevention and detection likely won't have the intended effect and will leave you more vulnerable. To get the most value from your endpoint security purchases and lessen the burden on IT and security ops teams, prioritize vendors offering integrated threat prevention, detection, and response technologies.

Look to expand your detection capabilities beyond static IOC (indicators of compromise) identification. Given the prevalence of fileless attacks and novel attack methods utilizing legitimate software, your detection capabilities must go beyond malicious file and process detection. Signatures and IOCs are generally only useful for file-based threats that have already been seen, and with all the variations of malware due to metamorphic and polymorphic malware, your detection capabilities must cast a much wider net. Prioritize tools that include behavior-based detection from a process and user perspective.

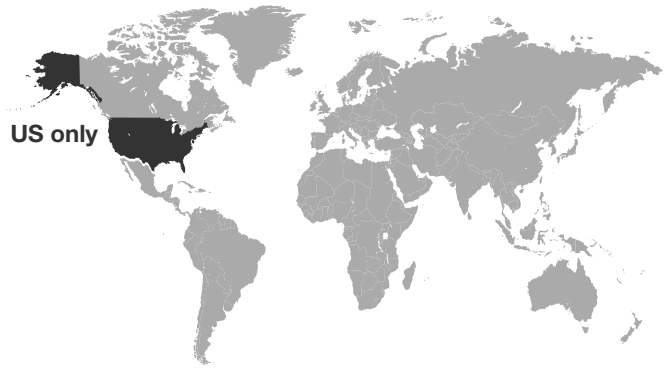
Build up employee skillsets through automation and training. Automation is key to alleviating SOC staff struggles, as it allows for more agility, flexibility, and rapid responses to threats. While technology is not a substitute for people, you can only maximize it when you have staffed your team appropriately with skilled and trained resources. Send your staff to leading incident response conferences like the SANS Digital Forensics and Incident Response (DFIR) Summit or the Forum of Incident Response and Security Teams (FIRST). Consider rotationships between your red and blue teams for skill cross-pollination. Remember, attackers learn new techniques and methodologies for compromising your environment; your defenders should be learning as well.

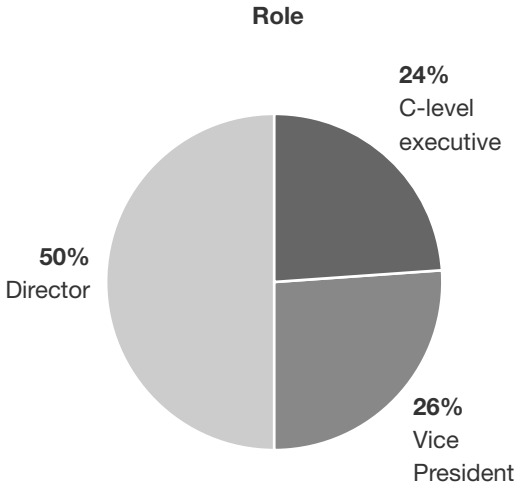
FORRESTER®

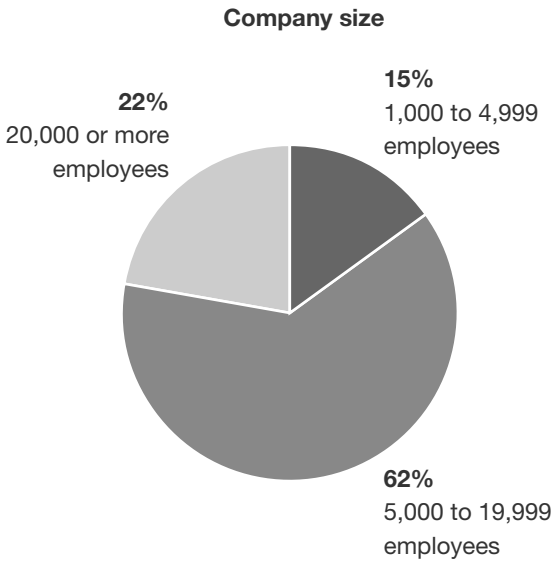
Appendix A: Methodology

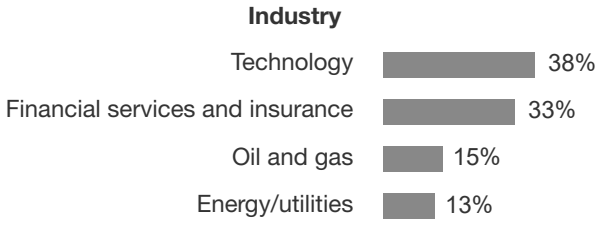
In this study, Forrester interviewed three security decision makers and conducted an online survey of 156 security decision makers in the US to evaluate security operations centers challenges and barriers. Survey participants included decision makers in director or higher roles. Questions provided to the participants asked about their security breaches, tolerance around breaches, and their current SOC offering and staff. The study took place in May 2017.

Appendix B: Demographics/Data









Base: 156 US-based application IT security decision makers at companies with 1,000+ employees
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Endgame, May 2017

FORRESTER®