CSO
FROM IDG

WHITE PAPER | SPONSORED CONTENT

THE SECURITY GAME SHOULD BE STRATEGIC, BUT SEEMS ONE OF CHANCE

Study finds continuing tool sprawl, lack of meaningful metrics, and strategic misalignments hinder progress

Market Pulse 2021

IDG MarketPulse Research:
Impacts of IT Security Tech Sprawl

Sponsored by

RELIAQUEST

IN THIS REPORT

INTRODUCTION

Even as organizations prioritize and invest in cybersecurity, progress seems elusive. In some ways, it's the perfect storm: the junction of on-going tool sprawl, a continuing skill set shortage, and lack of strategic metrics that can't solve the problem at hand. And in certain cases, the situation is further complicated by misalignment between executives and those in charge of security operations.

Too often, what should be a game of strategy ends up being a game of chance.

START WITH SWIRLING TOOL SPRAWL. On average, enterprises maintain 19 different security tools, according to a new survey of 400 IT leaders by IDG and ReliaQuest. IT security teams continue to invest in tools and search for better alternatives while at the same time eliminating the old, the survey found.

On an average, enterprises activate six tools while deactivating seven in a 12-month period. Unfortunately, many tools—old or new—are perceived to deliver dubious return on investment (ROI). Couple this with a shortage of in-house expertise for managing an expanding set of tools that do not play well together, and enterprises are playing a game of security carousel that appears to lack strategic intent.

"The growing sprawl of security tools, each addressing a different security challenge, continues to get worse year after year," says Bob Bragdon, SVP/managing director of CSO worldwide at IDG.

LAYER IN A GROWING SKILL SHORTAGE: 70% of security professionals report negative impacts on their organizations from a cybersecurity skills gap, according to research from the Information Systems Security Association (ISSA). What's more, workloads are increasing while most budgets stay flat. "Like everybody else these days, we have to do much more work with no expanding budget," wrote one respondent to the IDG/ReliaQuest survey.

NOW ADD IN THE PROBLEM WITH METRICS. The survey also revealed that that security teams simply aren't collecting the right metrics. They are often focused on technical metrics such as measuring number of vulnerabilities or tool functionality instead of more holistic ones tied to business outcomes.

FACTOR IN MISALIGNMENT ON OBJECTIVES AND TACTICS. In some cases, the survey found, security teams at the top view investment and direction differently than those charged with execution. This is not a surprise. Executives at the CISO and VP level have their eye on strategic business goals and ROI. Directors and their staff, on the other hand, are typically faced with putting out fires, spending a growing amount of time managing tools, and manually piecing together data from across these tools to identify threats, among other things.

BUT THERE IS LIGHT AT THE END OF THE TUNNEL. Organizations that can gain singular insight into their security tools, optimize the use of automation to help solve the resource issue, and focus on metrics that evaluate progress and extend ROI can win at enterprise IT security. Underpinning this: A focused, strategic approach that connects the business and all levels of the security team.

This report examines the IDG/ReliaQuest survey findings in detail and offers best-practice advice and considerations for IT security leaders.

ABOUT THE SURVEY

In November and December 2020, IDG and ReliaQuest surveyed 400 IT and security leaders to better understand their security tool and technology deployments. Respondents worked at enterprises with 1,000+ employees in the US.

Respondents came from a wide range of industries, with 15% representing each of the top four verticals:

- Financial services
- Manufacturing, production, and distribution
- Retail
- Technology

THE REALITY OF TOOL SPRAWL & SUB-OPTIMAL RESULTS

The issue of tool sprawl, the questionable value of these tools, and their associated management complexity, is very real, according to the survey results.

On average, enterprises maintain 19 different security tools

A mere 22% of IT security tools (on average) are vital to primary security objectives

Only 47% of existing IT security tools are used daily; 28% are used less than quarterly

85% of participants are adding technologies faster than they can productively use them

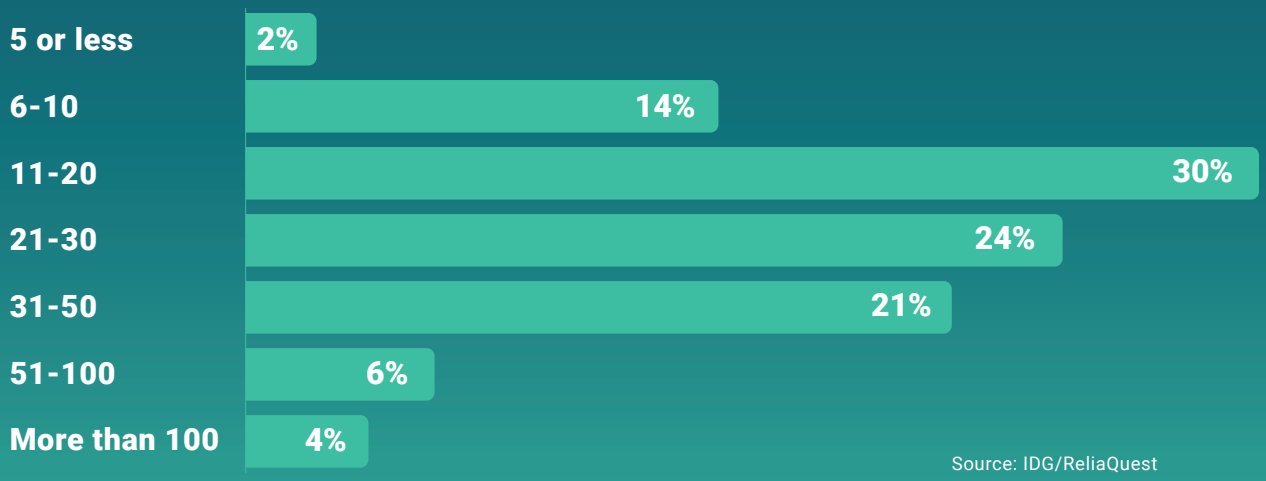
Respondents who admit most existing tools are underutilized: 71%

Those reporting the number of tools prevents them from deriving optimal value from each: 70%

71% said the increasing amount of time they spend managing tools inhibits their ability to effectively defend against threats

And yet, in spite of all this, 87% of survey respondents expect the number of security tools to increase in the next 12 months, the survey found.

FIGURE 1: IT SECURITY TOOLS/TECHNOLOGIES IN PLACE TODAY



Source: IDG/ReliaQuest

FIGURE 2: SECURITY TOOLS: VOLUME AND UTILIZATION IN TODAY'S ENTERPRISE

Source: IDG/ReliaQuest

MORE TOOLS, MORE PROBLEMS

Even with plenty of security firepower at their disposal, companies aren't meeting their security objectives. In fact, 62% of respondents say that there are more security technologies deployed than they need.

"The number of tools isn't necessarily the problem," says CSO's Bragdon. "The real problems are the difficulty in getting actionable intelligence from those systems, making sure that they are properly resourced, and, when they no longer perceived to deliver value, they are replaced or otherwise eliminated."

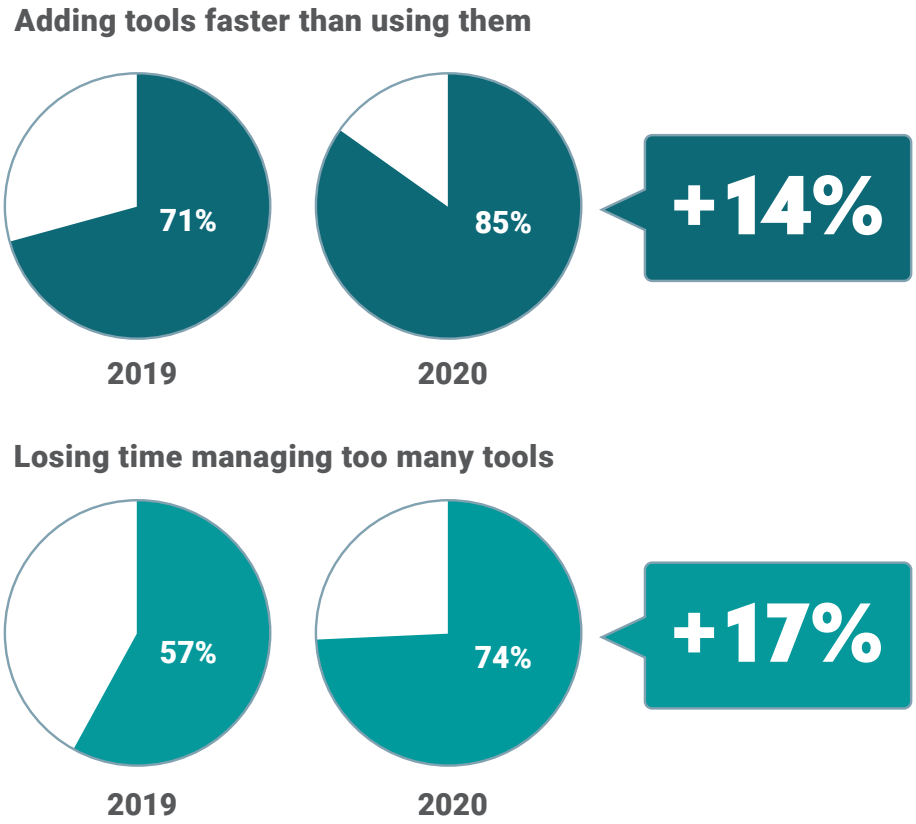
As a company's portfolio of security tools grows, the level of complexity in the security organization can grow, leading to missteps.

The majority of survey respondents (92%) agree there's a tipping point where the number of security tools in place negatively impacts security. Seventy-eight percent said they've reached this tipping point.

And nearly three-quarters (74%) said their organization's security team loses time managing a growing number of security tools, in turn hindering their ability to effectively defend against threats.

According to Joe Partlow, chief technology officer at ReliaQuest, one problem is that companies often purchase tools without a clear understanding of what their security teams actually need. "All too often, unfortunately, we see people go out and buy whatever the new shiny tool is. And maybe it really doesn't provide much of the protection or risk mitigation the business needs," he says.

FIGURE 3: THE GROWING SECURITY TOOL PROBLEM



Source: 2020 IDG Marketpulse Research: *Impacts of IT Security Tech Sprawl*; 2019 ReliaQuest Security Technology Sprawl Report.

As one survey respondent said, "I believe that security teams now spend more time managing security tools than defending effectively against threats."

Complexity also leads to other problems. As another respondent said, "If the system is too large and complex, it will inevitably lead to security loopholes. If the malicious code is not found and repaired in time, the data may be damaged, lost, or tampered with maliciously, causing great losses."

MISSING THE FOREST FOR THE TREES

As cyber threats grow ever-more sophisticated, the temptation is to throw money at the problem in the form of more security tools, Partlow says. And that's the wrong approach. "People buy advanced tools for very niche problems, and they're missing the bigger picture to focus on specialized threats."

"In other words, missing the forest for the trees causes problems," he continues. "You end up with tools for something that's not that big of a risk. Unfortunately, a lot of times, that comes at the expense of just getting the basics covered." Basics include ensuring cyber hygiene such as mapping security controls to risk, patching known vulnerabilities, and maximizing visibility.

With all the clutter of specialized tools, it's no wonder that in the present survey, 90% of respondents said there's been a negative impact on operations from the high number of security tools in use.

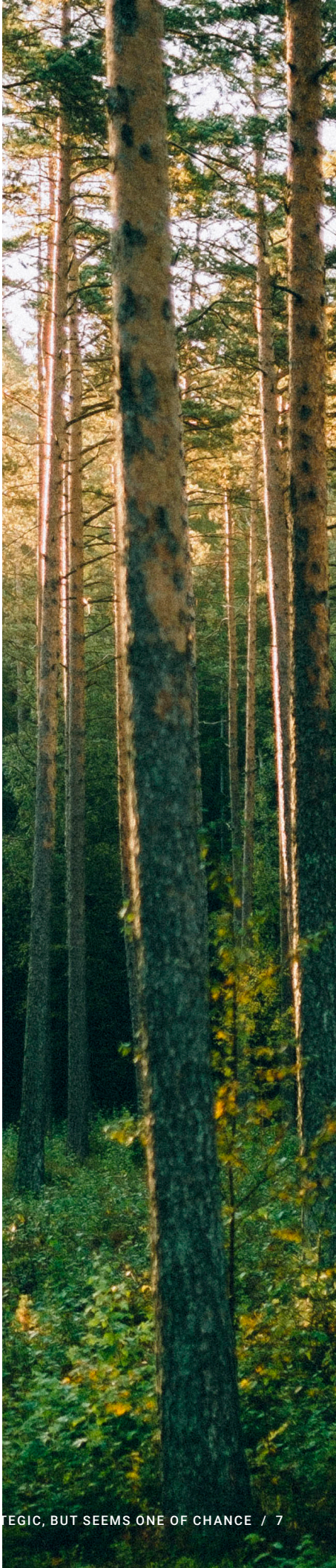
Survey respondents said they added an average of six security tools in the previous 12 months. They've also deactivated an average of seven technologies over the same period. The primary reasons for eliminating tools: replacing the tool with better alternatives, lack of ROI and integration capabilities, a general dissatisfaction with the tool, and tools adding to the chaos.

"Threats are evolving, the bad actors are getting better," Larry Trittschuh, CISO of HealthEquity acknowledges. "To keep up with them, you have to continuously evolve all aspects of security. But that doesn't necessarily mean you always have to buy the latest technology that promises to solve your problems. What's needed is clear visibility across your environment to ensure you have consistent awareness around your organization's coverage."

In fact, less than half—only 42%—of survey respondents say they're getting better visibility as a result of implementing multiple security technologies. Two-thirds (66%) of respondents say they are unable to integrate the technologies together, leading to a swivel-chair approach to security practices.

"Tool sprawl can get expensive as each additional solution is added," one survey respondent said.

Compounding the problem of tech sprawl is insufficient training, Partlow notes. "Having good training on a product will help shift the perception that tools aren't working and new ones are needed. Knowing what you have and knowing how to use it is more beneficial than throwing money at a new tool."



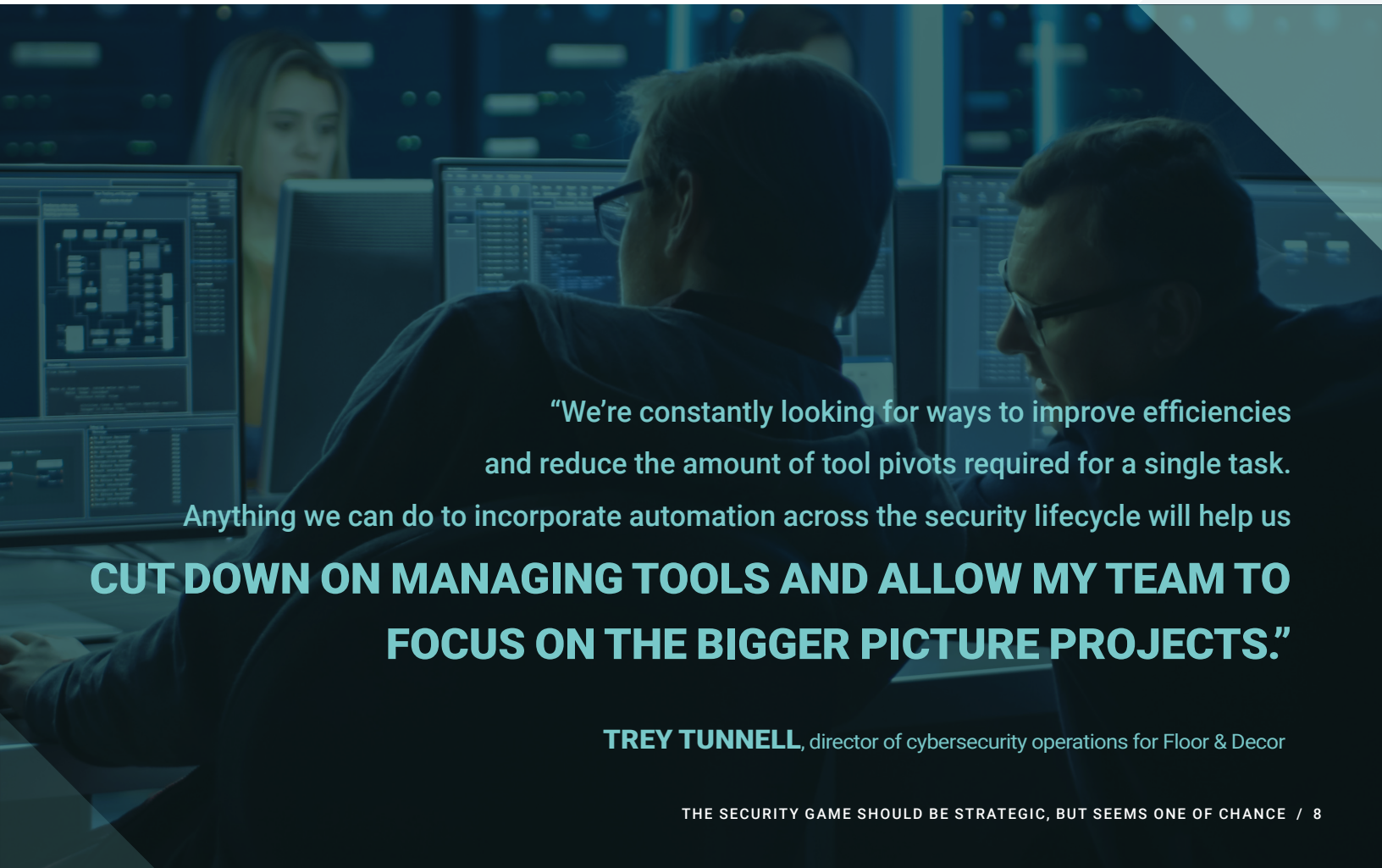
THE REALITY OF STAFFING ISSUES

According to ISSA's research, 70% of security professionals say the cybersecurity skills gap has negative effects.

The IDG/ReliaQuest survey confirmed that staffing shortages are causing headaches. More than half of the respondents (51%) said their security headcount has stayed flat over the past 12 months. At the same time, workloads are increasing.

The picture isn't likely to change over the coming year; 52% of IT security leaders said they expect the rate of new hiring to remain stagnant over the next 12 months. Nevertheless, the need for more help is real, despite increased investment in security tools.

In other words, even as enterprises keep adding new security tools, there aren't enough people to manage them—let alone dive into the features and capabilities of each.



"We're constantly looking for ways to improve efficiencies and reduce the amount of tool pivots required for a single task. Anything we can do to incorporate automation across the security lifecycle will help us **CUT DOWN ON MANAGING TOOLS AND ALLOW MY TEAM TO FOCUS ON THE BIGGER PICTURE PROJECTS."**

TREY TUNNELL, director of cybersecurity operations for Floor & Decor

SECURITY TOOLS ELUDE ROI

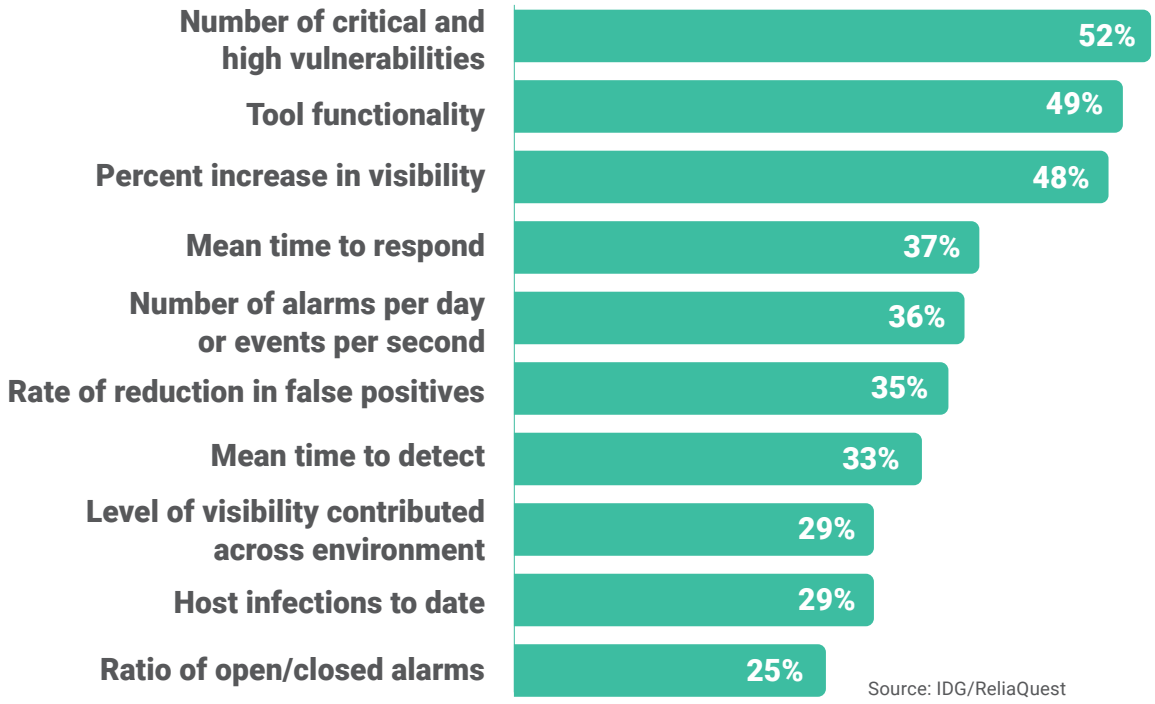
At the same time, a dearth of strategic metrics hinders meaningful progress.

Most enterprises struggle to measure ROI for security tools, the survey found. Respondents most often measure their investments using these three metrics: the number of critical vulnerabilities identified (52%), tool functionality (49%), and the percentage increase in visibility (48%).

Only 29% of respondents said they measure the level of visibility contributed by tools across the environment, and only 33% look at how fast they can detect and respond to threats (Figure 4).

Instead of focusing on technical metrics, it is important that security teams measure visibility, tool efficacy, and team performance. These metrics allow them to gauge how well their investments are doing. This focus shift also helps with distilling complex measurements into simple, meaningful metrics for use outside the security team.

FIGURE 4: CALCULATING THE ROI OF SECURITY TOOL/TECHNOLOGY INVESTMENTS



Source: IDG/ReliaQuest

Furthermore, 93% agree that better visibility would strengthen the security team's position with the company's board and help gain company-wide support for their initiatives. This visibility would also help demonstrate the value of new security technologies to executives or the board, respondents noted.

MISALIGNMENT ON OBJECTIVES AND TACTICS

At some organizations, tool sprawl, skill gaps, and lack of strategic metrics are further complicated by varying views of the security solutions at hand.

While respondents agree on many things, the survey results also show that in some organizations, upper management (VP and above) has a different perspective versus operations managers (director and below) around the impact of security tool sprawl and the tactics for handling it. The survey revealed the following differences:

WHEN TO REPLACE TOOLS

53% OF UPPER MANAGEMENT said a tool should be removed if it doesn't provide sufficient ROI for its stated purpose. In contrast, only **21% OF OPERATIONS-LEVEL RESPONDENTS** saw insufficient ROI as a key reason for tool replacement.

HOW TO MANAGE NEW TECHNOLOGIES

FORTY-ONE PERCENT (41%) OF UPPER MANAGEMENT said their organization lacks the necessary expertise, versus **20% OF THEIR OPERATIONS-LEVEL RESPONDENTS.** Furthermore, **46%** said their organization's security team has more difficulty determining the source of security incidents due to a large number of tools compared to **25% OF OPERATIONS-LEVEL RESPONDENTS.**

WHEN TO ADD NEW TOOLS

96% OF UPPER MANAGEMENT said their organizations add security technologies faster than they can use them, but only **67% OF OPERATIONS** agree with that assessment.

WHAT'S THE RIGHT NUMBER OF TOOLS

While **91% OF UPPER LEVEL MANAGEMENT** feel there's a point at which the number of security technologies in use increases their organization's level of risk, only **56% OF OPERATIONS LEADERS** agree.

HOW TO COMMUNICATE TOOL VALUE

63% OF OPERATIONAL MANAGERS don't think the board understands the value of new security technologies, versus only **41% OF UPPER MANAGEMENT.** And while **MORE THAN HALF (53%) OF OPERATIONS-LEVEL** respondents said it's difficult to report security ROI to the board, **JUST OVER ONE-THIRD (34%) OF UPPER MANAGEMENT** share that sentiment.

SOLVING THE CHALLENGES: BEST-PRACTICE ADVICE

What's the answer to securing the enterprise? Although the winning formula is easier said than done, there is a formula for success. Strategy is critical, as is overcoming tool sprawl and skill gaps, using the right metrics, and aligning the team around common goals and tactics.

But where should you start? What's the first step? ReliaQuest's Partlow outlines the following key considerations.

- **UNDERSTAND YOUR RISK EXPOSURE.** ***Make a clear assessment of the risks to a particular business. This includes defining the outcomes you want to see, and the metrics you want to measure.***

The assessment requires the IT or dedicated security team to align with business leaders to determine the actual business needs for risk management. "If you ask the business leaders what their biggest fears and risks are, their answers may not align with what the security team thinks," Partlow notes. That means getting agreement on basics such as what systems are most vital to the enterprise.

- **EVALUATE YOUR TOOLS.** ***"Once you define the business needs, then you can determine whether you already have the tools that will give you visibility into and protect against threats," he continues. If it turns out you're missing the necessary tools or that your organization has purchased the wrong ones, then you can rebalance your security portfolio from a knowledgeable position.***

Getting aligned on what needs protecting (and from what threats) will also help security teams make the business case for security investments. "At some point, a business is going to say, 'What are you spending all this money on, and what did it get us?' If you don't have a good answer for that, it's probably not going to be good for you," Partlow says.

- **ANSWER THE PRESSING QUESTIONS.** ***With a clear risk assessment that considers business needs in hand, Partlow suggests answering three crucial questions:***

    1. ***Will your tools help you get a better handle on your critical risks?***
    2. ***Will your tools help you balance your risk profile?***
    3. ***Will your tools help you fill gaps in visibility?***

- **CONSIDER THE IMPACT OF M&A.** ***For certain organizations, one of the best places to start tackling tool sprawl is by assessing the ramifications of mergers and acquisitions.***

"With a lot of mergers and acquisitions, you've got different business units tacked together that may have different tools running across different gear," Partlow says. Investigate what's there with a view to eliminating duplicate functionality. For example, are there redundant endpoint tools? Security information and event management systems (SIEMs)? Firewalls?

- **ESTABLISH A REGULAR EVALUATION SCHEDULE.** ***Depending on the size of your organization and/or the M&A activity going on, Partlow suggests setting a regular schedule for re-evaluating your strategy and tactics. This could be as frequently as once a month or just 2-3 times a year.***

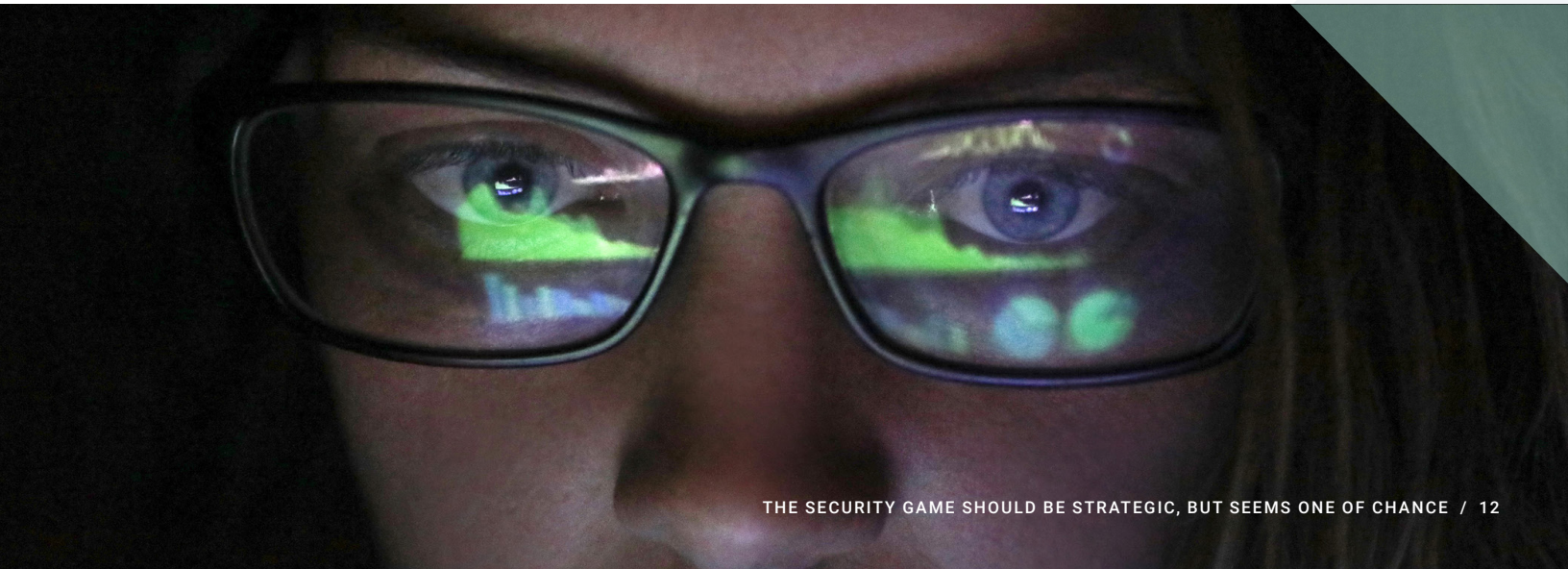
This evaluation isn't just a one-time process. Tools and technology evolve over time, as does the IT environment, both at the enterprise level and across the security landscape. IT leaders must evaluate if any new security gaps have emerged, for example. One way to understand gaps in coverage is by mapping against established frameworks such as the MITRE ATT&CK® or Cyber Kill Chain® constructs.

A regular evaluation can also help answer the following types of questions: *Should older tools be replaced with newer ones? Are our tools and strategy tracking to business needs? Are all the key stakeholders involved in the decisions?*

- **USE AUTOMATION AND INTEGRATION TO OVERCOME RESOURCE ISSUES.** ***The resource and skills shortage problem is not going away soon, and enterprises have to consider ways to force-multiply their existing teams so they can focus on critical objectives.***

Automation across the security lifecycle can eliminate tedious and repetitive tasks and focus analysts on high-priority work. Managed tool integrations is another way to relieve staff from non-security chores.

- **ANALYZE AND EMPLOY THE RIGHT METRICS.** ***Last but not least, security teams should focus on the metrics that help illustrate the value and ROI of both specific tools and their overall security approach.***



Instead of delivering metrics that don't demonstrate business value, teams must focus on "metrics that matter"—ones that span people, processes, and technology. Measurements such as visibility across security controls, or the efficacy of system performance, can provide context to help business leaders better understand the state of their security program and how to improve it.

Visibility and tighter integration across tools and the entire security stack can go a long way toward meeting security objectives, Partlow says. It's essential to determine which tools are the most and least effective—this will help IT security leaders better manage costs while ensuring optimal security coverage and risk management.

"Security is a team sport," he says. "If you've got a partner that can stitch all those elements together, allowing you to get that bigger picture, and then working with you to make sure that you're moving in a positive direction, then you've got an orchestrator or a quarterback to help you produce the outcomes you want."

LEARN HOW TO DRIVE SINGULAR VISIBILITY FOR PROACTIVE SECURITY BY OPTIMIZING TOOLS AND REDUCING COMPLEXITY, AT RELIAQUEST.COM.

ABOUT RELIAQUEST

ReliaQuest is a global leader in cybersecurity focused on helping organizations achieve successful security outcomes by reducing complexity. GreyMatter, ReliaQuest's unified detection, investigation, and response platform, combines in-house expertise with relevant technologies to help optimize security operations. It delivers singular visibility across your security tools with continually updated security, intelligence, and ready-to-use detection content.

Purpose-built automation capabilities across the security lifecycle—from detection to investigation to response—combined with artificial intelligence can help IT leaders focus scarce resources on security priorities, in turn reducing alert fatigue while improving efficacies. Hundreds of security leaders trust ReliaQuest to improve business resilience, reduce risk, and improve security confidence. For more information, visit www.reliaquest.com.

RELIAQUEST

ADDITIONAL READING

THE CISO's GUIDE TO METRICS THAT MATTER IN 2021

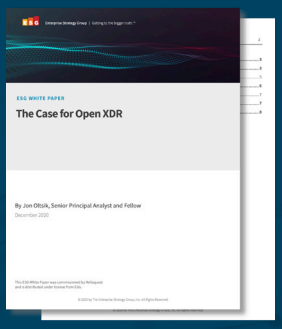
The security metrics that teams traditionally use lack context and fail to provide insights needed to make strategic decisions, leaving CISOs struggling to show ROI, identify gaps, and gain support across the organization. This can leave security teams with a false sense of confidence and a less-than-optimal budget, all while risk increases. By applying the security metrics that matter, CISOs can mature their security programs and articulate value to boards, peers, and technical team members.

READ NOW

SECURITY AUTOMATION FUNDAMENTALS: SIX STEPS TO FASTER DETECTION AND RESPONSE

Too many tools, too little integration, and more noise than a team can effectively analyze all add up to less visibility into threats and less efficient security teams. Automation is supposed to solve the "tool fatigue" problem, surfacing the most critical issues by running playbooks against common threats and freeing up valuable resources for other tasks. Learn how to apply automation across the security lifecycle for faster detection and response.

READ NOW



ENTERPRISE STRATEGY GROUP: THE CASE FOR OPEN XDR

The latest magic bullet security vendors are offering to address the challenges around a sprawling set of tools with eXtended or cross-platform detection and response (XDR)—but does XDR really have the best interests of the customer at heart, or is this just the latest fad vendors are pushing out to market? In this paper, ESG Senior Principal Analyst and Fellow, Jon Oltsik, shares his view of the market, what organizations truly need to get ahead, and why an *Open XDR approach* is likely to help organizations realize their security outcomes and a faster time to value.

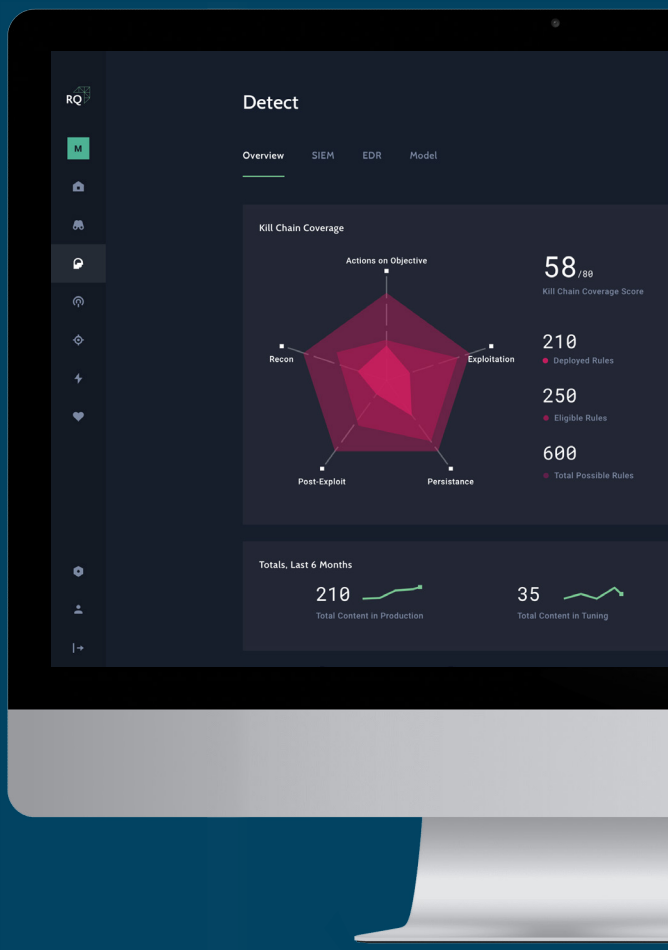
READ NOW

HOW RELIAQUEST GREYMATTER REDUCES COMPLEXITY AND DRIVES PROACTIVE SECURITY

ReliaQuest is a global leader in cybersecurity, focused on helping organizations achieve successful security outcomes by reducing complexity and force multiplying security teams. GreyMatter, ReliaQuest's vendor-agnostic Open XDR platform, unifies detection, investigation, and response capabilities to deliver singular visibility across your security tools by integrating them and driving optimizations with continually updated threat research, intelligence, and ready-to-use detection content. Purpose-built automation capabilities across the security lifecycle—from detection to investigation to response, help focus scarce resources on security priorities, in turn reducing alert fatigue while improving efficacies. GreyMatter helps improve efficacies and performance by enabling teams to measure security practices against easy to understand and actionable metrics that matter.

GreyMatter is the first SaaS solution that spans your enterprise and integrates across any deployment—on-premises, cloud, or hybrid. Hundreds of security leaders trust ReliaQuest to improve business resilience, reduce risk, and improve security confidence.

FOR MORE INFORMATION VISIT RELIAQUEST.COM



> **Before ReliaQuest, we lacked visibility in our tools and a unified view of current threats. ReliaQuest helped us achieve quick response, tool efficacy and data driven results. With the efficiencies we are now able to focus on business growth and not worry about having to scale our team.**
>
> – Mike Novak
> CISO + VP of IT Security, Seminole Hard Rock Casinos

RELIAQUEST

Make Security Possible™

(800) 925-2159 www.reliaquest.com info@reliaquest.com