RELIAQUEST

2019 ReliaQuest Security Technology Sprawl Report

How the Rapid Growth of Security Tools is Impacting the Overall Risk Level, Effectiveness and ROI of Enterprise Cybersecurity

OVERVIEW

A rapidly growing number of security tools has arisen to help organizations better secure their environments and actively protect important data, from Security Information and Event Management (SIEM) to Endpoint Detection and Response (EDR), Security Orchestration, Automation and Response (SOAR) and more. In response, many organizations are purchasing more tools than they can effectively manage as they struggle to stay protected against the latest security threats. This "vendor sprawl" is a result of security professionals buying best-of-breed technologies, typically from standalone vendors, according to a 2019 Forrester report.

This has created major challenges for enterprise cybersecurity leaders. Security teams now struggle to manage numerous disparate products that often have overlapping functions and don't integrate. "Security pros suffer from vendor fatigue" and "the problem of too many different technologies that don't talk to each other," a Forrester blog post from earlier this year says. To better understand the strategic, financial and operational impacts of these challenges, and how security leaders are reacting to them, ReliaQuest surveyed more than 400 enterprise IT and security professionals in the United States who are involved in making decisions about their organization's security technology.

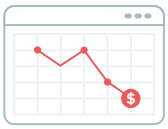
Enterprises have reached a "security tool tipping point," where a growing suite of tools actually *increases* organizational risk levels and *decreases* security teams' ability to respond effectively to threats. How did they get there? Root causes include underutilized technology, ineffective use of valuable security resources and overwhelmed teams that spend more time trying to manage tools than proactively defending their enterprises against threats.

Enterprises have reached a "security tool tipping point," where a growing suite of tools actually *increases* organizational risk levels and *decreases* security teams' ability to respond effectively to threats.

KEY FINDINGS

Enterprises continue to buy new security technologies at a rapid pace... Seventy percent of respondents say they've invested in more than five new technologies in the last year alone, including 19% who say they've invested in more than 20 new tools.

... but can't use them effectively. Seventy-one percent report they are adding security technologies faster than they are adding the capacity to productively use them.



The resulting shelfware is decreasing expected ROI. Sixty percent say that most of their security technologies are underutilized.

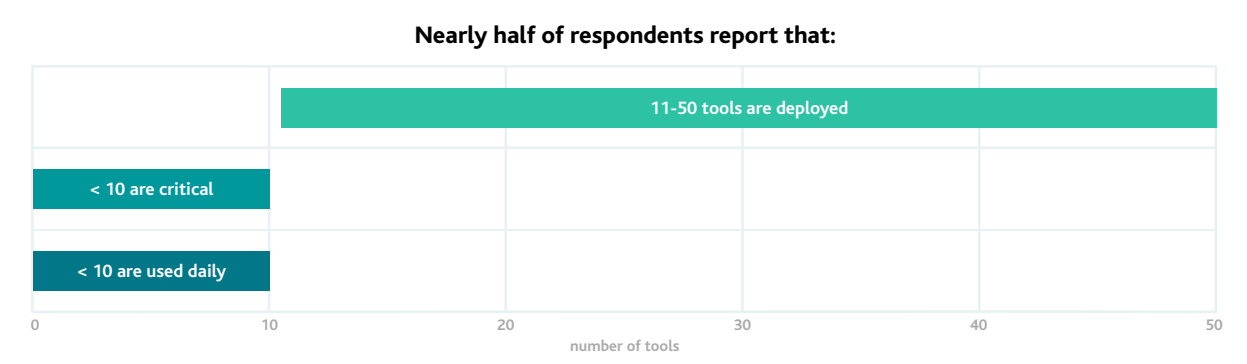
The burden of tool management compromises threat response. Sixty-nine percent report their security team currently spends more time managing security tools than effectively defending against threats.

A majority of enterprises are less secure today as a result of tool sprawl. Fifty-three percent say their security team has reached a tipping point where the number of security tools in place is so burdensome that it adversely impacts security posture and increases risk.

Security Teams Are Buying and Deploying More Tools Than Ever

Security teams are investing in and deploying a large number of new security technologies each year. Seventy percent of respondents say they've invested in more than five new technologies in the last year, including 19% who say they've invested in more than 20. A sizeable portion of respondents (15%) say they currently deploy more than 50 technologies.

But despite this significant investment in new technology, the survey data shows that not all of these tools are being used regularly and only a fraction have become mission-critical. Forty seven percent of respondents report they currently have between 11-50 security technologies deployed, 48% say that 10 or fewer are considered mission-critical to the business and 47% say 10 or fewer are used on a daily basis.



It's no surprise, then, that many tools end up being deactivated after they are purchased. Eighty-three percent of respondents report having deactivated security technology in the last year, including almost one quarter (23%) who say they've deactivated more than 10 tools in that time.

The Business Impact of Vendor Sprawl: Decreased Financial and Operational Efficiency

Enterprises purchase and implement a growing number of security technologies, and the result is vendor sprawl: a proliferation of disparate tools that no longer deliver on their original purpose, individually or collectively. Sixty-three percent of respondents say there are currently more security technologies deployed at their organization than are needed.

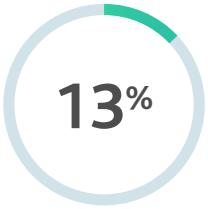
The results:

1. TOOLS BECOME SHELFWARE, UNDERMINING INTENDED ROI

One major consequence of vendor sprawl is that a majority of security teams are spending valuable resources on technology only to have it end up as "shelfware" — instead of being used to strengthen security posture, these products are left sitting on the shelf after being purchased. Indeed, few respondents are able to say that their existing security technologies are used:

of all tools are used on an ongoing basis

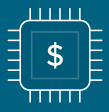
of all tools are used to their full potential



of all tools are used in their intended manner

These tools are either added too quickly to be productively implemented or do not function properly because they haven't been effectively maintained, preventing the achievement of intended ROI. Sixty percent of respondents characterize most of their organization's security technologies as "underutilized," and that same number (60%) say their teams are not currently getting the highest possible value from their investment in security tools.

Respondents report that the top three security technology pain points are:



Technology costs

Time to implement

Lack of integration with other technologies

2. OPERATIONAL EFFICIENCY SUFFERS AS TEAMS STRUGGLE TO KEEP UP

Vendor sprawl exacerbates a simple math problem within enterprise security organizations: the growing requirements of new technologies outstrip the organizational infrastructure available to operationalize them. Seventy-one percent of respondents say they are adding security technologies faster than they are adding the organizational capacity to productively use them. Meanwhile, over half (57%) believe their team loses productivity when new technologies are implemented and one-quarter (25%) say that their organization's security team does not have the necessary training and expertise required to manage new technologies.

There are a few different factors that can contribute to this inefficiency. Sometimes, the team member who purchased and championed a new technology has left, while no one else knows

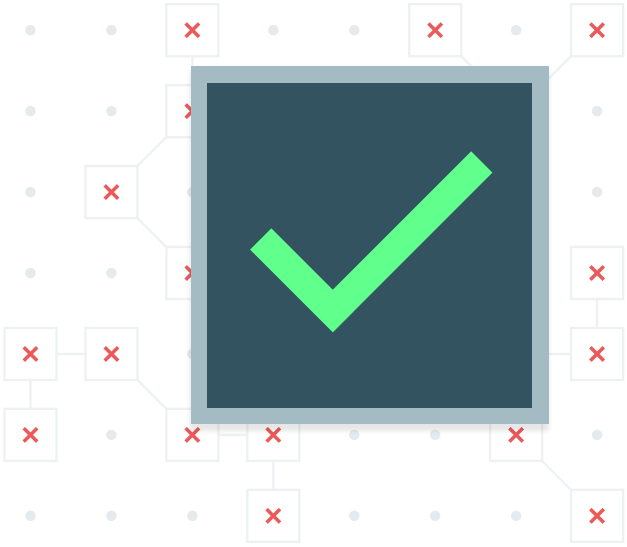
how to properly use it. Other times, companies purchase a tool they think they need, but security teams are too busy or lack the training to implement it correctly. The tool may end up performing only one of the many functions it was purchased for. Tool maintenance is also a factor. Even if a security tool is implemented correctly at the beginning, it needs to be updated as a company's security environment and attack surface expand.

The Long-Term Consequences: More Tools Result in More, Not Less, Exposure to Security Threats

On a macro level, the vendor sprawl challenge is having a concerning impact on organizations' overall security posture. The survey found that a large number of disparate tools is negatively impacting organizations' ability to successfully manage threats. Nearly seven-in-ten respondents (69%) report their security team now spends more time managing security tools than effectively defending against threats. Sixty-six percent of respondents report that the sprawl of security technology makes it harder for their organization's security teams to do their jobs.

THE BOTTOM LINE: ORGANIZATIONS HAVE REACHED A SECURITY TOOL TIPPING POINT

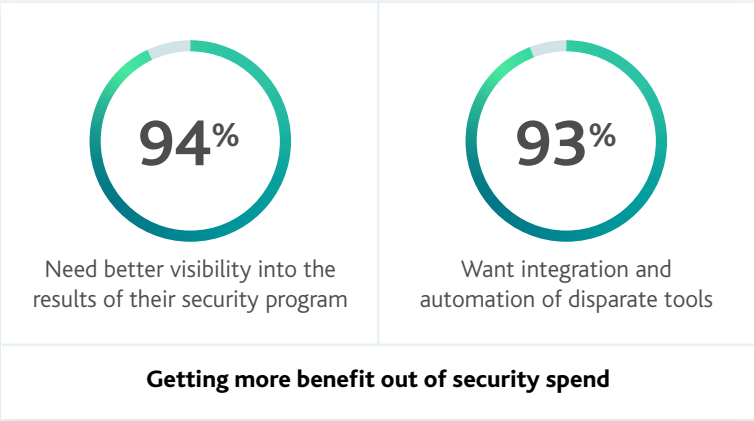
Three-quarters (76%) agree that there is a tipping point where the number of security tools in place is so burdensome that it adversely impacts security posture and increases risk, and 53% say their security team has reached that tipping point. Interestingly, respondents say the average number of tools that make up that tipping point is 22.



One of the major risks of vendor sprawl is that security teams think they have "checked the box" and put necessary protections in place, but in reality those protections aren't being fully managed, monitored or analyzed. This false sense of security leaves organizations vulnerable. They may not realize a tool isn't working properly until it's too late. In other cases, the number of false positives generated by poorly utilized tools can cause the security team to miss the alerts that truly matter.

Overwhelmed Security Teams Urgently Need a New Approach

CISOs see the need to address vendor sprawl before it adds further risk to their organizations. Their ultimate goal: nearly all respondents say that better visibility into the results of their security program (94%) or integration and automation of disparate tools (93%) would allow them to get more benefit out of their security spend. But how do they get there?

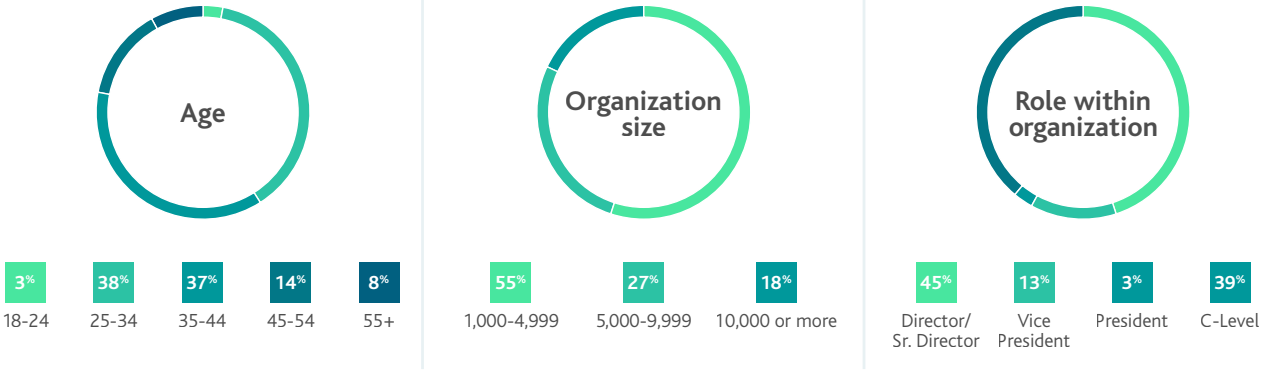


There are a few ways security leaders can restore their security posture, rebalance investments and increase the efficiency of their teams.

- **Focus on optimization.** Instead of acquiring new tools to fill gaps in their security environment, CISOs can take a pause and focus on understanding what they already have. Take time off from buying incremental new products and use resources to get the most out of what has already been purchased.
- **Take inventory.** Security teams should take steps to fully implement the tools at their disposal, which starts by taking an inventory of current capabilities. CISOs should map out each tool and ask themselves how both capabilities and use have evolved since first being purchased. Is the tool still doing what it was originally intended to do? Can it now do more, better?
- **Identify gaps or overlap.** After examining the current tech stack, CISOs can better assess where functions are being duplicated and what areas may be left unprotected to truly merit new tools.
- **Reexamine the internal team.** As an organization grows, the security team's internal capabilities often change. CISOs should revisit whether their tools and staff still match up. Each tool should have resources that understand how to best use and maintain it. If that doesn't exist, either the team needs to be realigned or the value of the tool reassessed.
- **Anchor around current business goals.** It can be helpful to reexamine what larger business goals the security team and its suite of tools are supporting today and whether purchased tools still align. Is the organization's primary goal digital transformation? Building customer trust to better compete in the market? Revisit the KPIs that support these efforts and then organize the technology stack around them.
- **Connect the siloes.** As part of rationalizing their technologies, people and process, security leaders can turn attention to improving connectivity across their organization to avoid siloes while improving both visibility and response capabilities.

Ultimately, the growth and evolution of security technologies helps enterprises stay a step ahead of rapidly evolving threats. However, as their profiles grow in many organizations, CISOs and their teams have an opportunity to be more strategic in the purchase and management of their tools. Vendor sprawl and the financial and operational pains it causes are avoidable. Before that next six- or seven-figure purchase, leaders can reassess overarching business goals, align the specific security initiatives that enable them and then recalibrate the growing amount of technology, process and people to optimally deliver.

Demographics



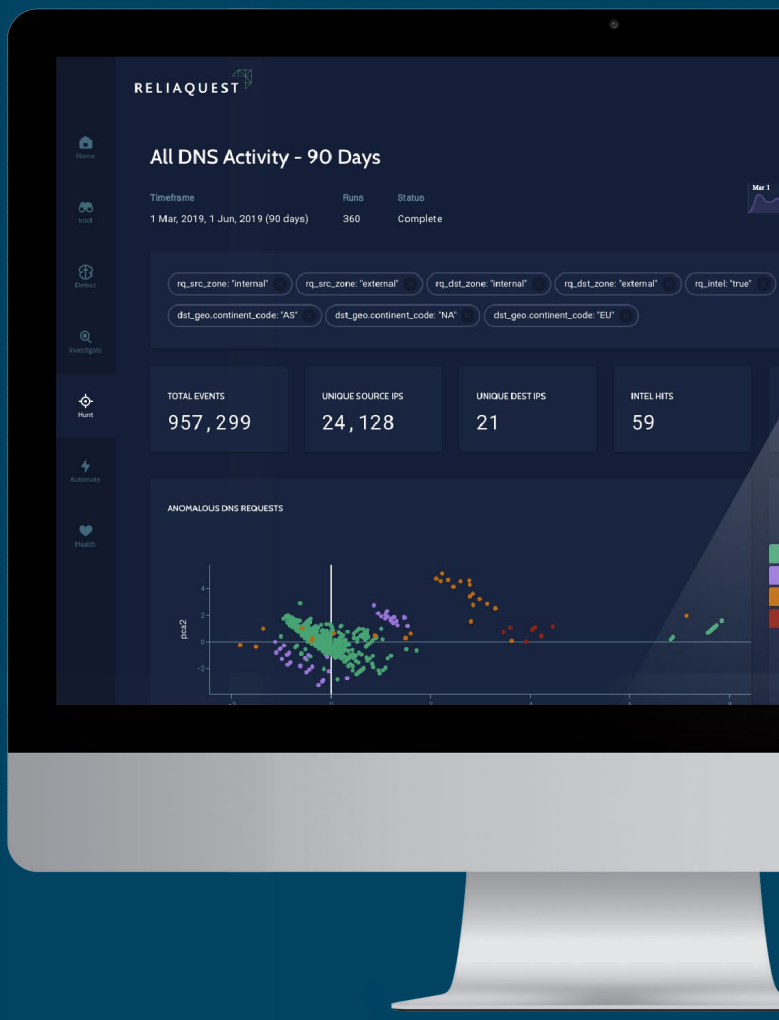
Methodology

ReliaQuest commissioned Market Cube to conduct a survey of 400 enterprise IT and security professionals in the United States who are involved in making decisions about their organization's security technology. The survey was conducted online November 4-11, 2019. The margin of error is plus or minus 4.9 percentage points.

About ReliaQuest

ReliaQuest fortifies the world's most trusted brands against cyber threats with GreyMatter, its SaaS platform for increasing enterprise visibility while automating threat detection and response. It does this by unifying and integrating existing SIEM, EDR, multi-cloud, and third-party apps, to deliver a centralized, transparent view across the environment. The platform's analytics provide actionable reporting and metrics that measure ongoing improvement of the security program to improve the effectiveness of security investments while better enabling the business.

More than 250 Global 2000 enterprises rely on ReliaQuest to achieve security confidence. ReliaQuest is a private company headquartered in Tampa, Fla., with locations worldwide, visit www.reliaquest.com



ReliaQuest GreyMatter, the SaaS security platform, delivers visibility across SIEM, EDR and multi-cloud environments to speed detection and response, while maturing security investments to deliver security confidence.

LEARN MORE ABOUT RELIAQUEST

RELIAQUEST

Make Security Possible™

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