WHITE PAPER

Affordable Tools and Shared Responsibilities Define Midmarket IT Security Trends

Sponsored by: SolarWinds | March 2019

Analyst Jay Bretzmann

solarwinds

Research and Analysis by IDC

IDC ANALYZE THE FUTURE

IDC Opinion

Midmarket companies face considerable business challenges as they adopt and embrace technology that will help them grow into the enterprises of tomorrow. Corporate and IT management teams know they can't do it all, and therefore focus their resources on the "must-do's" while strategically partnering for as many of the "should-do's" that funding allows. By-and-large, security teams understand the challenge and are looking for affordable tools that serve as force multipliers. The right intelligence and automation can help even a part-time resource significantly reduce an organization's attack surface.

IDC conducted a survey sponsored by SolarWinds that was designed to discover the challenges companies face in terms of cybersecurity. Companies have deployed numerous technologies to help them both monitor the environment and document who's doing what for compliance purposes. They're spending less on prevention activities and luckily, few have experienced a devastating attack. The more immediate exposure stems from internal user mistakes and technology deployment misconfigurations that effectively leave the front door — or at least a ground-floor window — wide open.

It's also clear that talent is in short supply. Midmarket companies are necessarily seeking outside help in the form of education, hosting, monitoring, threat intelligence and incident response. For many industries, that help is increasingly being capped by a fixed percentage creating opportunity for those technology providers that offer affordable solutions.

Methodology

The results presented in this study are derived from a survey link sent to both IT and non-IT respondents who declared themselves to be either knowledgeable or very knowledgeable about their organization's cybersecurity practices. All results were collected from a survey website during February 2019.

Of all the respondents, 66% were based in North America, 17% were from the United Kingdom, and 17% were from Germany, Austria, and Switzerland. Regarding company size, 56% of respondents were from midmarket organizations (100 to 1,000 employees), 24% of respondents were from large-scale organizations (1,000+ employees), and 20% of respondents were from small businesses (under 100 employees).

Introduction

This paper explores how midmarket companies in particular are deploying and using security technology. For midmarket organizations, it's a hybrid IT infrastructure world managed by a combination of in-house expertise and specialized service providers. Some IT practices are deeply ingrained within these organizations, while others need more focus, education — and likely — more service resources. A specific effort was made in the survey to understand both the insider risk that exists within these organizations and what insider incidents occurred in 2018. For the most part, detection or monitoring tools are in place, yet it's the protective practices that need some additional focus. For many organizations, time will tell if an ounce of cybersecurity prevention delivers pound(s) of cybercrime cure.

What's otherwise surprising from the survey is the consistency of the answers to most questions given the diversity of the sample organizations. Yes, threats exist, but most survey respondents believe the greatest exposure comes from self-inflicted conditions. If proper configurations are too hard to decipher, they'll probably deploy the default configuration and revisit questionable risk decisions later. Regrettably, patching and endpoint management tasks are traditionally viewed as overly time-consuming, so security teams get to them as schedules allow — which means basic cyberhygiene practices are often forgotten. Detecting an intruder is one thing, but leaving the door open for the intruder is another.

Midmarket teams clearly report the need for effective and affordable tools to help them reduce deliberate and malicious attacks and avoid accidental configurations.

SITUATION OVERVIEW

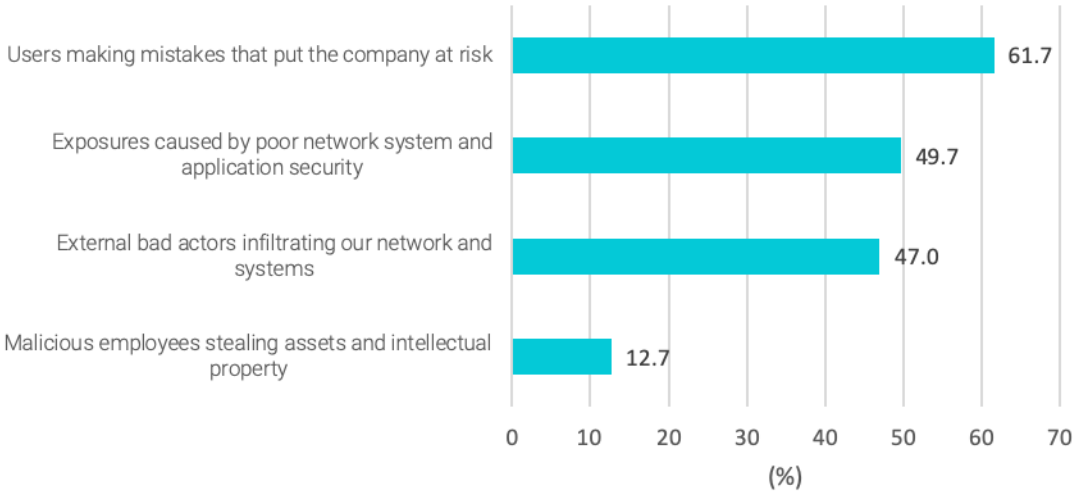
For cybersecurity teams, there's never any shortage of things to do, and for every data breach that gets reported, there are likely another three that organizations just don't talk about. The cybercrime industry has turned into a machine, offering would-be attackers a cornucopia of ready-made exploit kits backed by professional service and support. It's never been easier for cybercriminals to conduct both random and focused attacks.

Properly conducted, a risk analysis will help cybersecurity teams prioritize their use of defensive resources. Job one is to reduce the attack surface around an organization's most valuable assets. Smaller companies often approach the task — out of necessity — with a finger-in-the-dam approach, and they run out of fingers pretty quickly. These companies know they need

help. Most currently support hybrid IT infrastructure environments which add complexity to the basic challenge, and most also outsource whatever security services they can pursuant to industry or governmental regulations and their own sense of comfort.

Figure 1. It's Mistakes/Misuse More than External Attackers

Q: In 2018, which of the following types of cybersecurity threats led to incidents within the company?



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

Protecting against external attacks occupies the attention and consumes the majority of the cybersecurity budgets of most CISOs. The board and C-Suite want to know shields that shields are up against the threats on the web they hear about. But more savvy practitioners know that an equal and more impending threat can come from within, driven by maliciousness, laziness, or just plain ignorance (See Figure 1). The survey results also confirm that cybersecurity teams need to spend more time using powerful, affordable tools to batten-down all the hatches before trouble ensues.

Looking at survey results, the cold reality is that most problems and exposures are self-inflicted. Organizations mistakenly configure something with an open port or someone among the end user community clicks on a bad link despite efforts to train end users about such threats or attacks. Astute security teams may discover these problems before they lead to data loss or mandate compliance reporting efforts, but only if they deploy enough security tools to scan and assess the environment.

Figure 2. Regular Employees Pose Largest (Mistakes) Risk

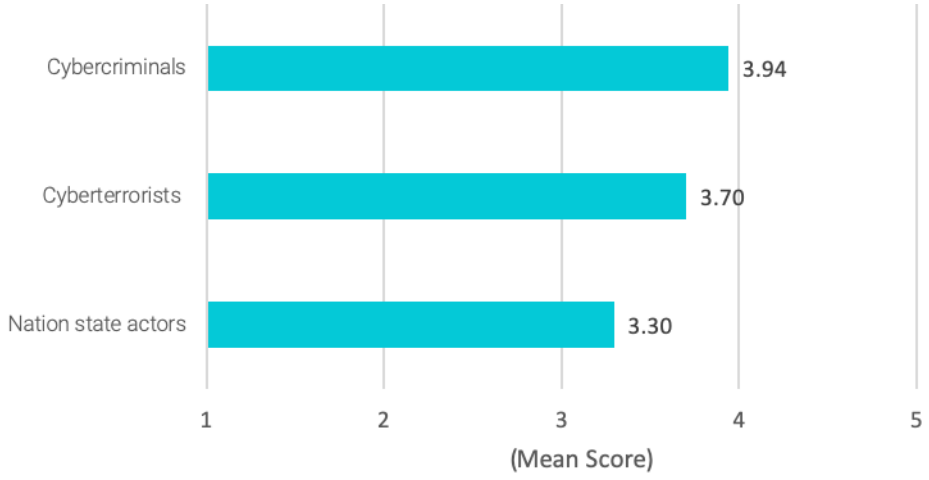
Q: Which of the following users pose the biggest risk for insider abuse/misuse?

N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

Despite a heightened sense of security awareness, traditional challenges still plague organizations with few dedicated resources. Most have employed both internal monitoring and managed (third party) services to defend the environment against possible cybersecurity threats; what these monitoring activities are seeing is that regular employees pose the largest source of insider threat (see Figure 2).

Figure 3. External Threat Focus

Q: . How concerned are you now about the following outsiders?



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

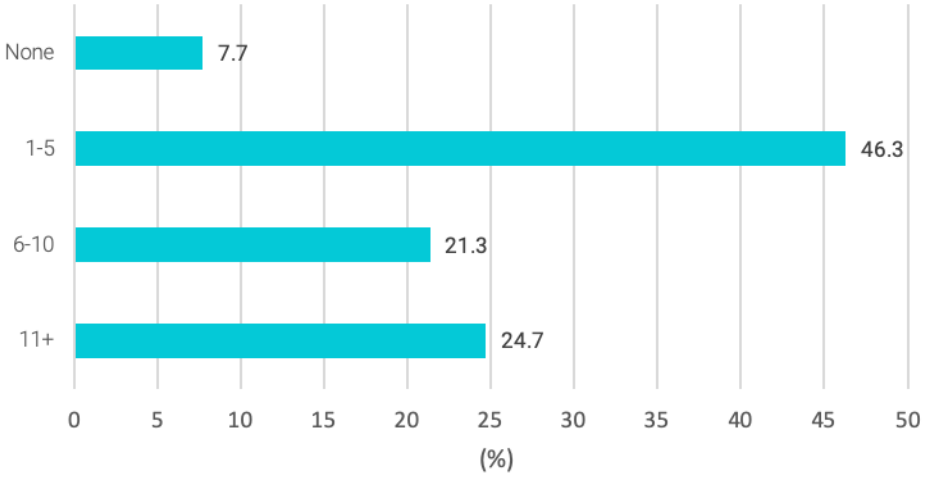
About half (47%) of respondents did experience some sort of incident based on the activities of bad external actors. Survey respondents rated their concern about outsiders on a five-point scale (with 1=not concerned, and 5=extremely concerned). Midmarket security teams are concerned about cyberterrorists and even nation state actors (see Figure 3), but the most likely encounter with these groups would be a result of a fast spreading malware possibly taking advantage of vulnerabilities identified or developed by bodies like the U.S. National Security Agency and leaked to the Dark Web. Midmarket organizations are much more likely to be attacked by smaller criminal organizations targeting specific data to either be exfiltrated and sold, or encrypted and held for ransom.

SECURITY SPECIFICS

Here's how cybersecurity teams we surveyed are aligning their resources to defend their organizations. Findings cover staffing, infrastructure hosting and the division of day-to-day management responsibilities.

Figure 4. Most Organizations Have Limited Staff

Q: . How many dedicated full-time cybersecurity personnel do you have on staff at your company?

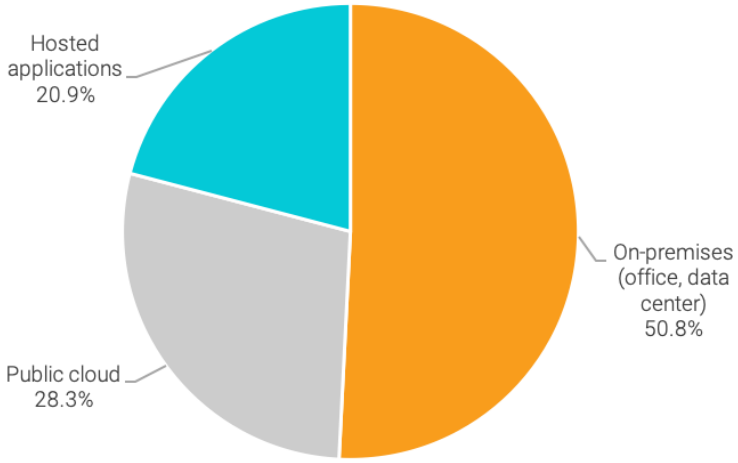


N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

Figure 4 shows the largest segment (46%) of survey respondents employed between 1-5 dedicated, fulltime security people. Almost 8% had zero security employees, and the larger organizations had six or more employed in these roles, which are especially prevelant within finance, manufacturing, and healthcare vertical industries.

Figure 5. Where Infrastructure Runs

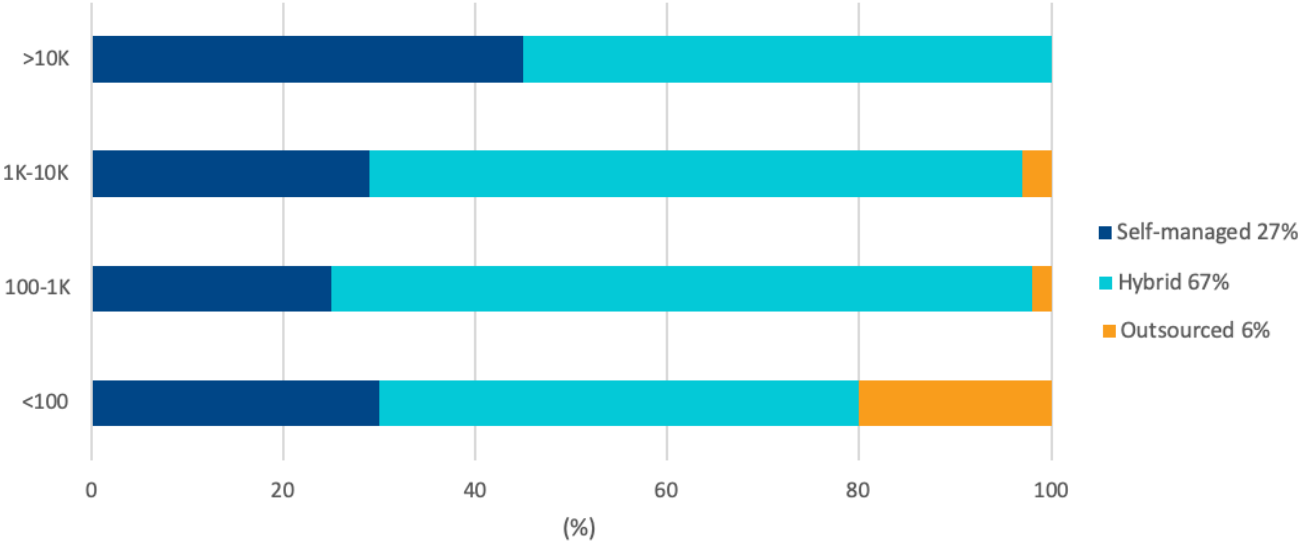
Q: What percentage of your infrastructure is running on-premises, in the public cloud, or via hosted applications?



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

Most of these teams are also working with the majority (51%) of their infrastructure running on-site although nearly every respondent has some percentage of public cloud and hosted applications in the mix (see Figure 5). Few respondents reported issues with the cloud infrastructure or apps in terms of being the source for an insider incident. Indeed 69% said elements like Microsoft Azure® and Office 365® were unproblematic.

Figure 6. Security Management by Organization Size



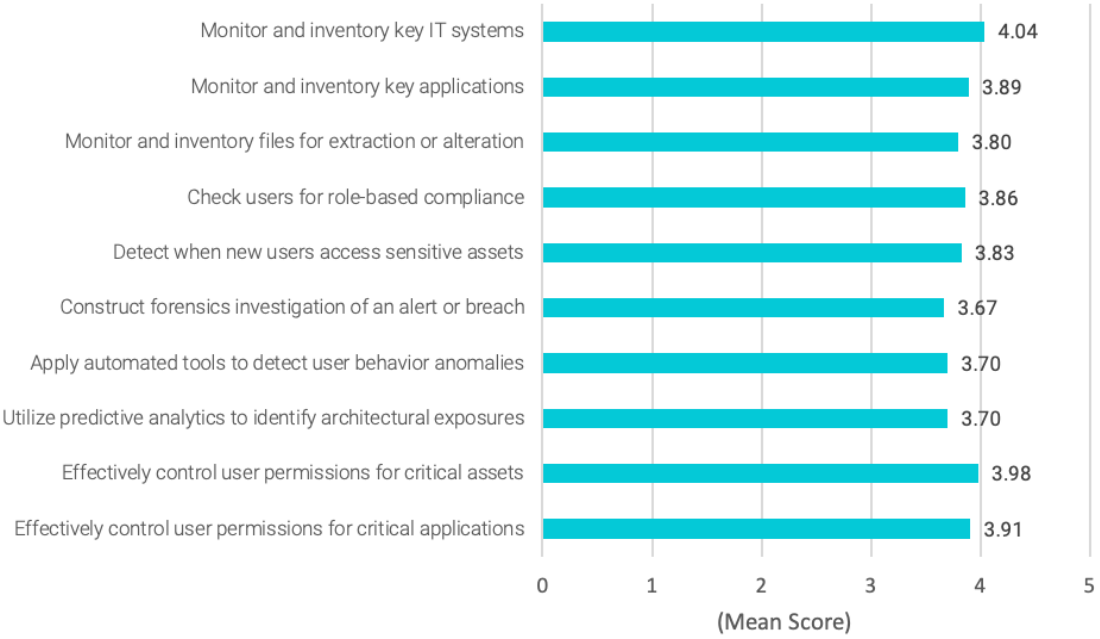
N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

And despite the large percentage of on-premises technology, Figure 6 shows that midmarket companies rely heavily on third parties to help them manage their environments. Availability of skills has been a problem for almost every company; hence it's critical to bring in outside talent. Also, having a partner that can keep copies of an organization's data off-site or "air gapped"

from the operational network is one of the first and biggest recommendations for security best practices developed by the National Institute of Standards and Technology (NIST), the National Cybersecurity and Communications Integration Center (NCCIC), the Federal Bureau of Investigation (FBI) and others to combat ransomware attacks.

Figure 7. Security Teams Are Pretty Confident

Q: With the tools you have on-premises today, how confident are you in your ability to do each of the following?



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

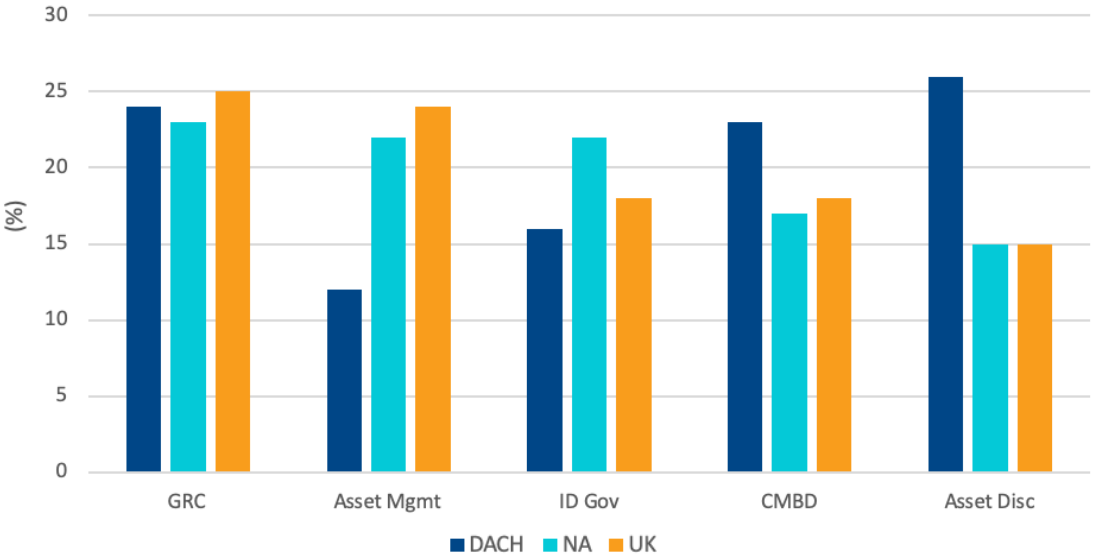
Respondents were asked to gauge their confidence levels about a number of security-related tasks (see Figure 7). Overall, respondents are fairly confident in their abilities – which can present dangers in that some people likely don't know what they don't know. To mitigate overconfidence, more training and exposure to threat intelligence best practices is recommended.

Also, the skills ratings didn't significantly change when the location of the tools was said to be in a public cloud (vs. on-premises) environment introducing a little more doubt into the responses. There are no shortage of internet posts describing misconfigured cloud storage "buckets," and identity management just gets more complicated across a mix of on-prem, hybrid and hosted application resources.

DEPLOYED DEFENSES

Unsurprisingly, the leading solutions deployed by survey respondents for identifying and managing risk have to do with governance and compliance. The explosive growth of digitally stored data means there's just more sensitive and personally identifiable data being collected by companies of all sizes.

Figure 8. Identify and Manage Risk by Region

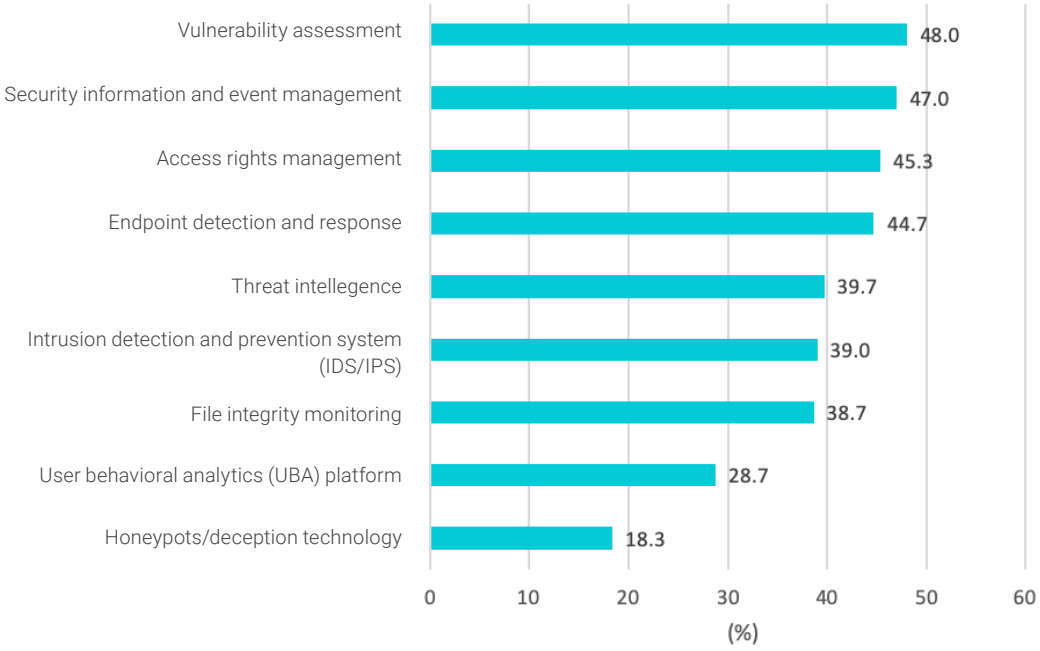


N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

The General Data Protection Regulation (GDPR) ushered in a new standard for compliance reporting and the potential for significant fines. Similarly, the New York State Department of Financial Services defined 23 NYCCR 500 introducing new data protections and requirements that began rolling out in 2017, and The California Consumer Privacy Act (CCPA) will come into effect in 2020. So, it's not terribly surprising that all regions in this study took governance, risk and compliance (GRC) very seriously as the top risk management activity — compliance is rarely optional and it is getting harder to document with each passing year (see Figure 8).

Figure 9. Vulnerability Edges Out SIEM for Detection

Q: Which of the following does your company use to detect compromises and malicious/suspicious behavior?

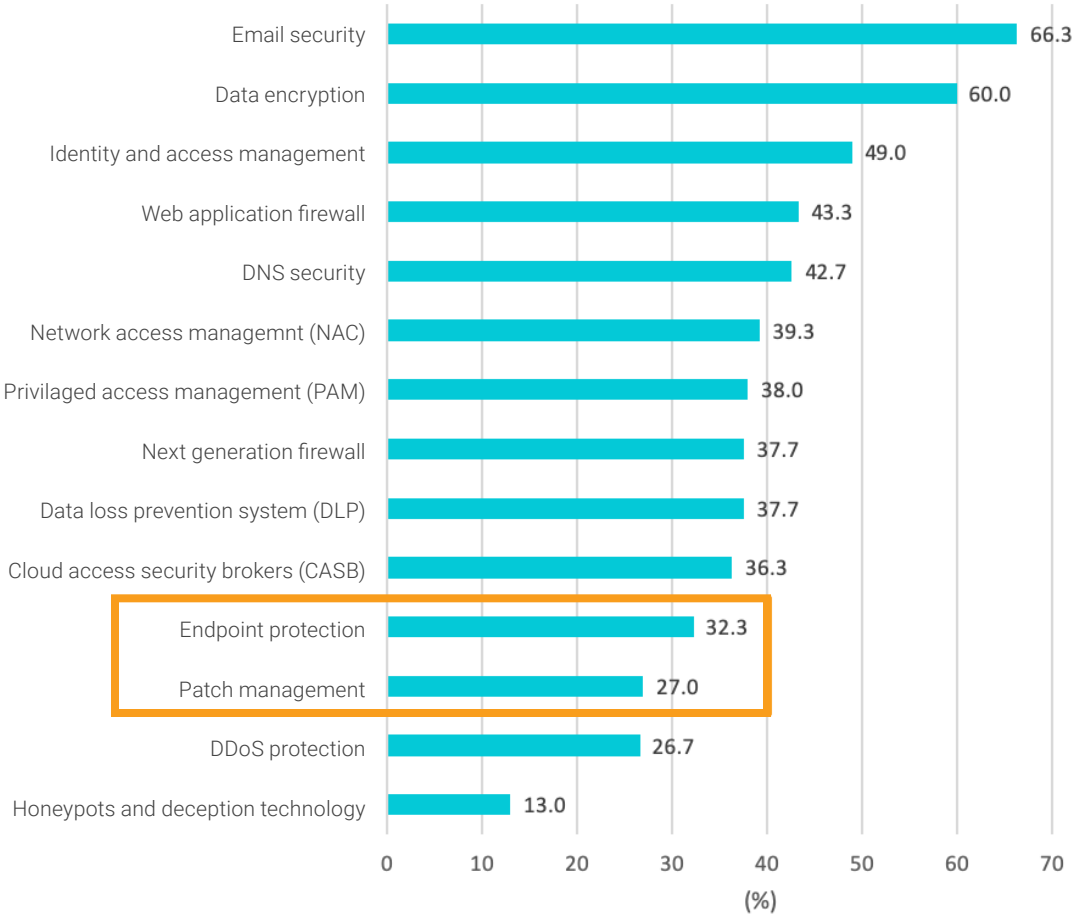


N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

As for detection technology, survey respondents said they viewed vulnerability scanning (48%) as the leading activity, but only slightly ahead of SIEM adoption (47%), as shown in Figure 9. Multiple technologies are deployed, and security teams generally feel like they can view and query areas of the network to discover suspicious activity. Furthermore, many teams are beginning to use threat intelligence in whatever form to adjust configurations or search for vulnerable situations.

Figure 10. Lack of Focus on Patching

Q: Which of the following does your company use to protect the organization from external and internal threats?

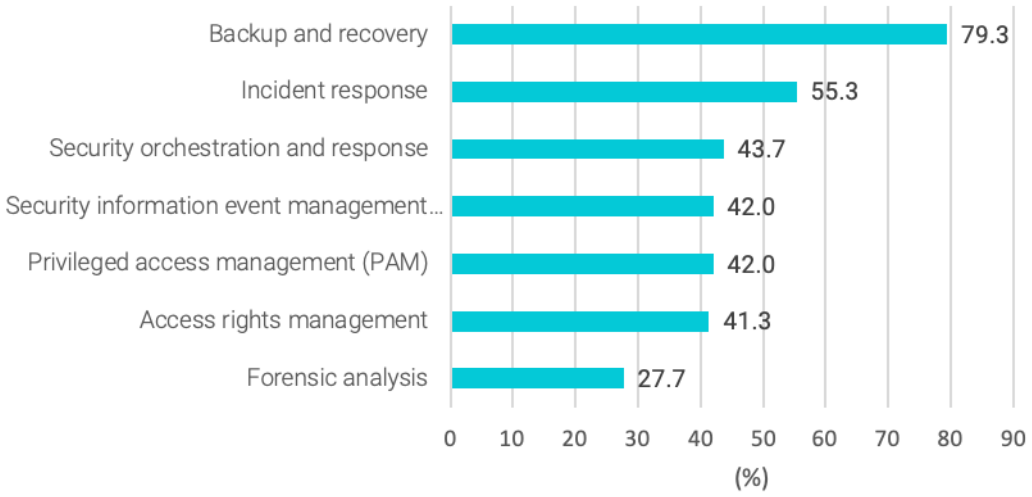


N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

One of the most concerning findings is a lack of patch management activities and a reduced focus on network endpoints (see Figure 10). On the protection front, these basic cyberhygiene best practices need to be combined with detection to help ensure that the "front door" isn't left wide open.

Figure 11. Backup and Recovery Dominates Response

Q: Which of the following does your company use to respond to and recover from an incident?



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

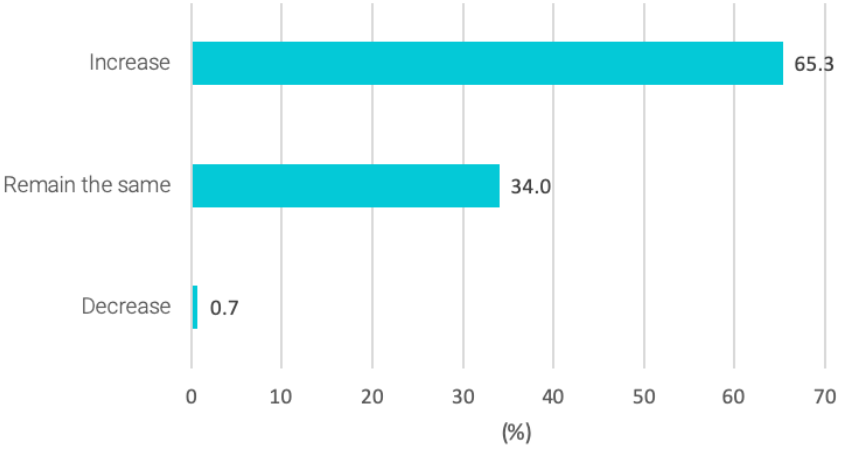
How do you respond and recover from a cyberattack that compromises your data? Somewhat in the same way you respond and recover from a network asset failure. Figure 11 shows that backup and recovery practices focused primarily on getting data back are widespread and well understood from a configuration, deployment and practice standpoint. However, businesses rely on more than data. As this survey shows, the more mature process of full incident recovery, including forensic analysis, is not understood.

2019 SPENDING

After years of playing catch-up, growth in cybersecurity budgets is beginning to moderate. Everyone agrees there's a limit to how much an organization can spend defending itself, it's just hard at times to accurately define that limit. Emergencies aside, cybersecurity is becoming a line-item expense with a fixed allocation. Organizations must spend dollars, euros, pounds, and so forth wisely.

Figure 12. Security Tools Spending for 2019

Q: How do you expect your spend on security tools and services in 2019 will change compared to 2018?

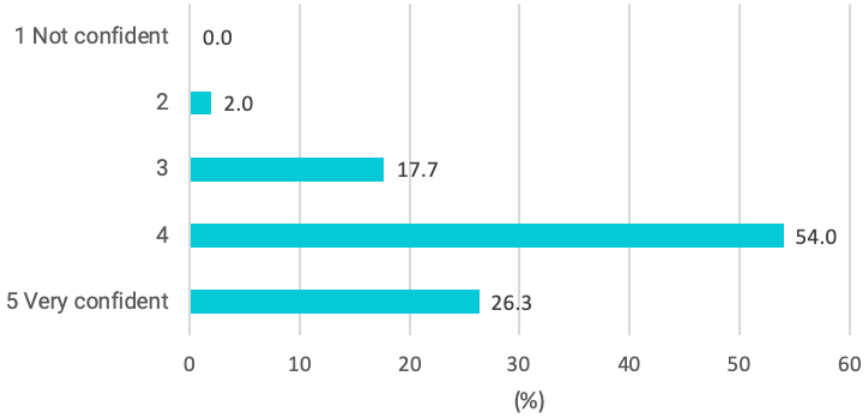


N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

For 65% of respondents, spending on security tools is expected to increase in 2019. Such a finding is not all that surprising, but the percentages seem to be moderating a bit; 34% of the sample plan to spend the same, while fewer than 1% expect their funds to decrease (see Figure 12).

Figure 13. Security Technology Expense Still a Major Factor

Q: . If cybersecurity solutions were more affordable, how confident would you be in your ability to improve your cybersecurity posture?



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

Figure 13 confirms that midmarket companies are still price conscious when it comes to security investments. A sweet spot for them seems to be the acquisition of an automation capability. Whether doing their own management or using partners, one could speculate that they desire the ability to search for risky conditions more than rapidly respond to active attacks. Fear is in the unknown; a couple of well-written queries might identify potential threats and help midmarket companies remediate trouble before any real bad actors discover a completely unrelated system vulnerability. Such a view is at least consistent with the idea that nation states, cyberterrorists, and even smaller cybercriminals do not comprise primary threats to the midmarket.

Conclusion

Cybersecurity is a big challenge for most organizations, and as this survey suggests, midmarket companies are doing all they can, using what they know, and spending whatever resources they have to defend against both external and internal attacks. Most respondents had some experience with an external attack in 2018, but even more were affected by internal vulnerabilities.

The biggest problem reported was that end user mistakes contributed to the largest attack exposures, and that regular employees — not privileged users — were the leading culprits. On the bright side, most situations were not malicious in nature. More education and training are needed.

Cybersecurity has become a budgeted organizational expense rather than a proposal for funding. Most organizations have limited staff and know what they're getting. They see where the problems lie and who's creating them, but they're behind on doing the more mundane work. Patching just isn't exciting. An automated solution is needed.

Amid defending their on-premises assets, most organizations surveyed were also running tools or acquiring services to defend hybrid infrastructure resources. Cloud dynamics and outsourced applications are attractive alternatives for standard IT services, but many are based on a shared responsibility model leaving organizations responsible for data security. Hybrid tools are needed.

With initiatives like the GDPR going into effect, organizations in all three regions surveyed received the message about improving GRC capabilities. Other U.S., and global regulations recently passed also included new privacy rights for data owners. New data tracking and access capabilities are needed.

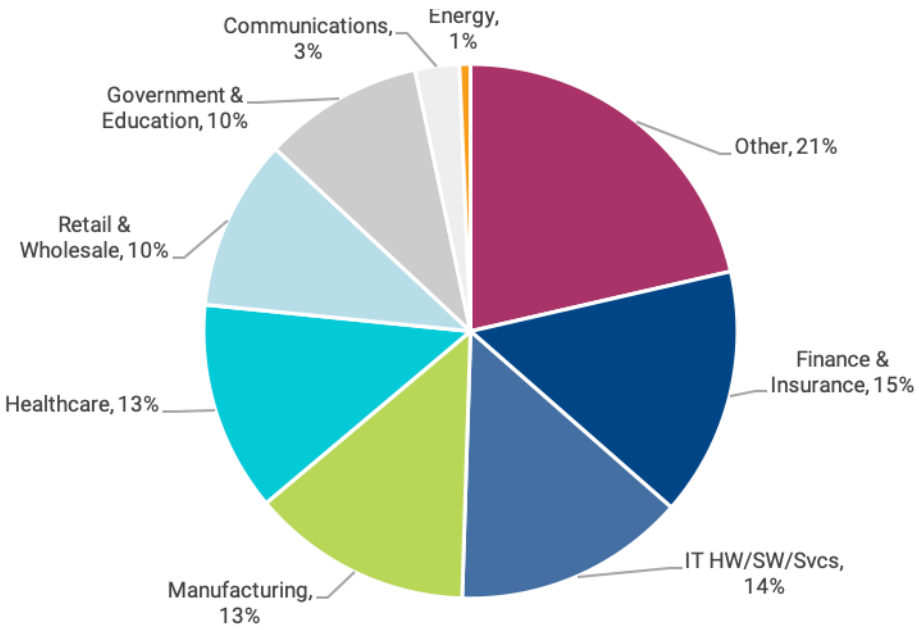
Some of these needs will be met in 2019 and some won't. Some organizations will lose data, but more won't. The threats are real, but associated attacks don't often occur. It's these conditions that can cause midmarket cybersecurity teams to become complacent, developing a disastrous sense of false security. If an attack does occur, the primary recovery tactic is to restore the environment from a backup. The midmarket isn't yet in a position to fund or conduct extensive forensic analysis activities leading to any patient-zero identifications.

Funding for 2019 is in place and cybersecurity solutions spending will meet or slightly exceed what survey participants invested in 2018.

Appendix

SURVEY PARTICIPANT INSIGHTS

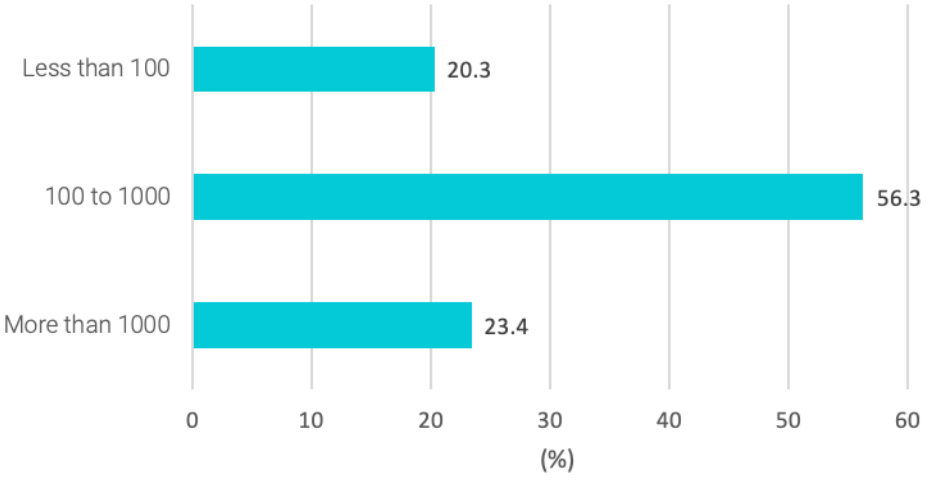
Figure 14. Broad Industry Representation



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

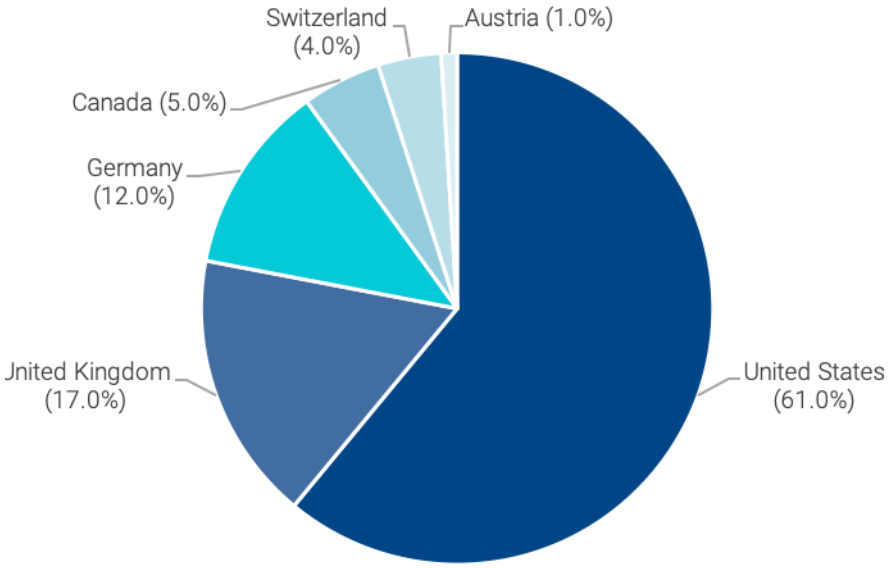
Figure 15. High Participation of Midmarket Organizations

Q: Approximately how many employees does your organization have, across ALL locations?



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

Figure 16. Geographic Sample Representation



N=300, February 2019, IDC's Insider/External Threats Survey, Sponsored by SolarWinds

About SolarWinds

SolarWinds provides powerful and affordable hybrid IT infrastructure management software to customers worldwide from Fortune 500® enterprises to small businesses, government agencies and educational institutions. We are committed to focusing exclusively on IT Pros, and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address all key areas of the infrastructure from on-premises to the Cloud. Our solutions are rooted in our deep connection to our user base, which interacts in our THWACK® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at http://www.SolarWinds.com/.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx