The State of Security 2021

Global research uncovers IT security leaders' key strategies for cloud complexity, remote work and supply chain attacks.

splunk>

Hindsight Is 2020: The Security Hits Keep Coming

The State of Security 2021

2020 started with COVID-19 and a pell-mell shift to remote work, and finished with the gut-punch of a major breach that put hundreds of organizations into frantic assess-and-remediate mode. The year will be seen as one of the most consequential in any security professional's career. For many, there will be a bright line dividing how things were before the pandemic from how they are now, as we hope to rapidly vaccinate our way out of it.

The consequences of the pandemic's rapid shift to work-from-home — and the exponentially faster shift to cloud technology that it helped drive — include less visibility into the security ecosystem, less control of access points, and a larger, more varied attack surface for adversaries to target.

And the consequence of the SolarWinds hacks is a deeper fear of supply chain attacks, and an almost existential question about the vendors every company relies on: *Should we trust our trusted partners?*

Yet the challenges of 2021 are not unfamiliar. They are, broadly: consistency, cost and complexity. To explore the top security challenges facing midmarket and enterprise organizations and to understand emerging strategies, we conducted a global survey of 535 security leaders in nine leading economies across multiple industries with research firm Enterprise Strategy Group. The research was done in February 2021, nearing the one-year anniversary of the pandemic, and two months after the disclosure of the SolarWinds hacks.

When the security and IT decision-makers in our survey identified the prime security challenges of a cloud-native security world, two stood out: 50% of respondents cited maintaining consistency of policies and their enforcement across data centers and cloud, and 42% cited the cost and complexity of using multiple security controls. Overall, our respondents seem to be telling us that cloud complexity, driven by transient workloads, new software development models, and heterogeneous public cloud usage, is the next great security challenge.

78% of companies expect another SolarWinds-style supply chain attack.

88% of orgs are increasing security spending — **35%** say "increasing significantly."

Rising cloud adoption is the top issue driving security investment.

Defining Disruption

Our respondents identified their primary challenge of the pandemic year as a definite increase in cyberattacks. More than four in five suffered at least one security incident, with business email compromise and data breaches being most common.

These incidents consumed significant time and resources for remediation (an impact cited by 42% of respondents), and led to lost productivity (36%) and disruption of business systems (35%). Clearly, these incidents are costly, distracting and potentially devastating.

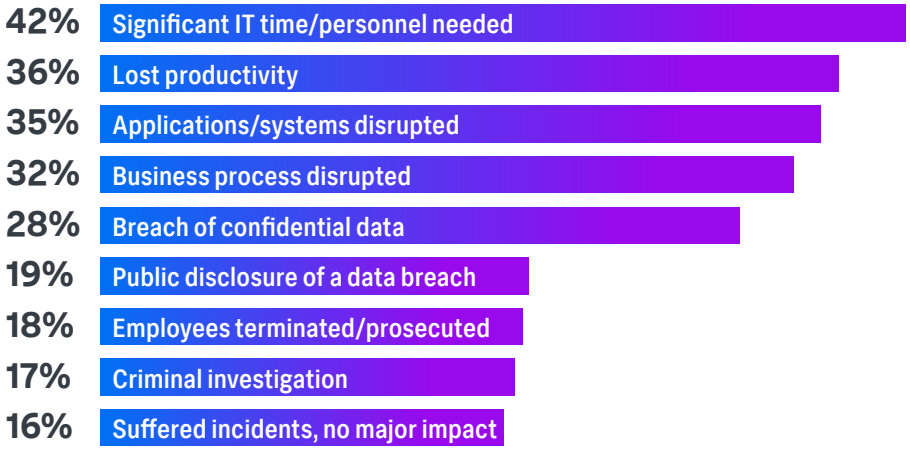
In addition to the difficulties in quickly shifting to remote work and protecting a new, somewhat sprawling perimeter, security teams had to contend with the massive, and massively successful, SolarWinds hacks. Disclosed in December 2020, these attacks caused an extra wave of disruption, leading many organizations to increase their

84% of orgs suffered a significant security incident in the past two years

Top cybersecurity incidents reported by respondents:

The Hidden Costs of Security Incidents

Top impacts of security incidents experienced by respondents:



efforts to fend off future supply chain attacks. To do so, survey respondents claim they will conduct more security controls audits (35%), scan software updates more frequently (30%), increase penetration testing (27%) and ramp up multifactor authentication (26%). While these actions can improve security, they also stretch already limited resources.

On that point: 78% of organizations report one or more challenges related to the cybersecurity team's capabilities or scalability, including the sheer volume of security alerts that redirect efforts from proactive improvement to tactical firefighting, and the drag caused by manual processes. And 78% also voice concern that they could be compromised by an attack like the SolarWinds hacks. Given that we haven't heard the last of the SolarWinds attacks, or even the beginning of other assaults on the supply chain that may come, we wonder: *What were the other 22% thinking?*

Cloud complexity is the next great security challenge.

Executive Highlights

If you want one takeaway, here it is:
Security is a data problem.

Data. It's what you're protecting, it's what tells you when the bad guys come knocking (or are already inside), and it defines the virtual cloud infrastructures in which it lives.

2021's challenges: cloud complexity and the expansion of remote work

Hybrid visibility is difficult enough with one cloud service provider. That may soon seem like the good old days.

- **75%** of cloud infrastructure users are multicloud today.
- **87%** expect to use multiple cloud service providers two years from now.
- **76%** of respondents say that remote workers are harder to secure.
- **53%** say attacks have increased during the pandemic.
  - **12%** call it a significant increase.

SolarWinds attacks: Are we doing enough to protect the supply chain?

- **78%** of security leaders are concerned about more SolarWinds-style attacks in the future.
- Two months after the SolarWinds hacks were disclosed, only **47%** of CISOs had briefed executive leadership or their boards about the implications.
- Only **23%** of organizations have reassessed/changed their policies toward vendor risk management.
- Only **23%** say they've segmented their networks to further limit access to systems and data.
- Yes, overworked security teams have their hands full; nevertheless, the muted response to the SolarWinds situation is concerning.

At least we're investing in solutions

- Nearly all respondents — **88%** — say that their security spending will rise.
- **35%** say it will increase significantly.
- **The takeaway:** Existing security processes and technologies are inadequate, so organizations have no choice but to increase spending and investments.
- See page 19 for respondents' top security investment priorities.

Key recommendations (see page 25)

- **Modernize the security operations center (SOC):**
  - Expand automation and analytics.
  - Adopt the zero trust security model.
  - Improve training and staffing.
- **Continue the one good thing to come out of the pandemic:** closer, timelier collaboration between security, IT and business professionals.

Challenges of the Data Age

Security organizations have always been hard-pressed to keep up with the rising tide of data, the ever-expanding perimeter, and the increasing frequency and sophistication of attacks. Our research confirms the conventional wisdom: It's only getting worse.

The familiar challenges have intensified in the COVID era: Manual processes are slow, cumbersome and widespread. The eternal shortage of skilled security experts is more pronounced. And cloud migration, a trend that goes back a good decade, has become more challenging because of ever-growing complexity, alongside ever-increasing velocity.

Interestingly, the research found that on-premises infrastructure is affected more often than cloud-based infrastructure, but both are vulnerable. The differences are marginal: The most frequent attack, business email compromise, affected on-premises applications and infrastructure 44% of the time, versus 36% for cloud resources. For phishing, mobile malware and insider attacks, the numbers vary by only a few percentage points at most. The key takeaway is that attacks are crossing hybrid infrastructures. Organizations need to prepare to defend against attacks regardless of where they start or end, because the intruder who penetrates an on-premises entry point will attempt to move laterally, including into cloud-based applications and data, and vice versa.

This active extension of the chain of attack from on-premises resources to the cloud underscores the need for visibility across environments. Security teams need to be able to connect dots. But since cloud is all about speed and maximum flexibility, developers are not eager to slow down enough to let the SOC implement controls.

More than one CISO underscored that point with this specific example: They lamented that when their company sends people to Amazon Web Services' Reinvent conference, developers return eager to immediately implement the new features Amazon has rolled out for its cloud service — features the security organization doesn't even know exist, much less have appropriate controls around.

Splunk's CISO, Yassir Abousselham, feels their pain. "In the race to set up remote work, there was a rushed transition to cloud solutions to allow remote employees to do basic tasks, like communicate with videoconferencing and instant messaging," he says. "At many organizations, security practices were sacrificed."

Splunk's CISO, Yassir Abousselham, feels their pain. "In the race to set up remote work, there was a rush to adopt cloud solutions to allow remote employees to do basic tasks, like communicate with videoconferencing and instant messaging," he says. "At many organizations, security practices were sacrificed."

The new security requirements of cloud-based technology, just for the work-from-home transition alone, are challenging, especially when organizations are moving at crisis speed.

"Adoption of cloud-based applications is best secured through single sign-on and multifactor authentication, because you just can't effectively scale account security using passwords alone," Abousselham says. "Converging to a single account per user with single sign-on allows closer control of authorization, stronger authentication and consistent monitoring."

Cloud complexity demands consistency

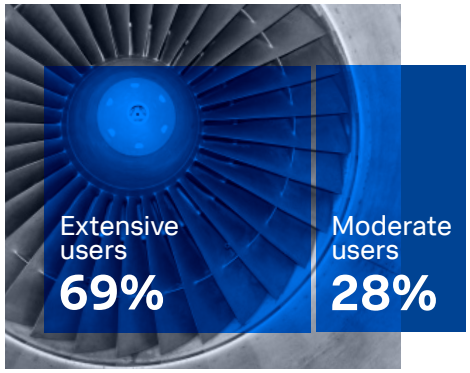
As public cloud usage becomes ubiquitous, security teams need to establish consistent controls around data and visibility into the complexity. Ultimately, organizations need cloud-friendly controls that are agnostic in terms of both architecture and cloud service providers.

Public Cloud Approaches Ubiquity

Percentage of orgs that report moderate to extensive use of public cloud computing

SaaS

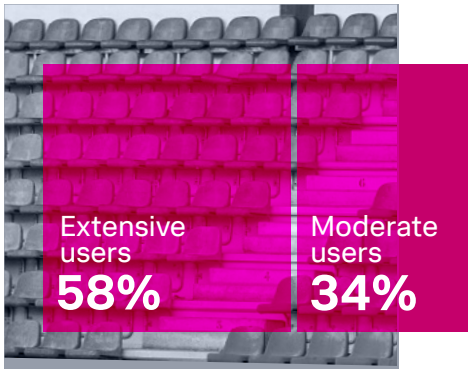
Software as a Service



97% total users

IaaS

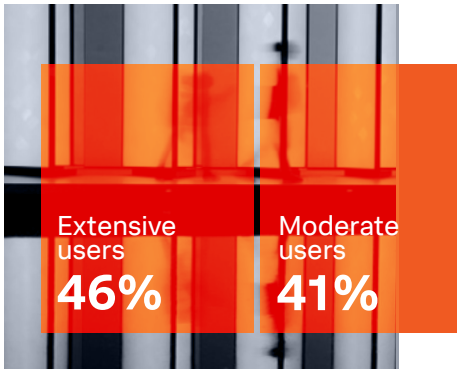
Infrastructure as a Service



92% total users

PaaS

Platform as a Service



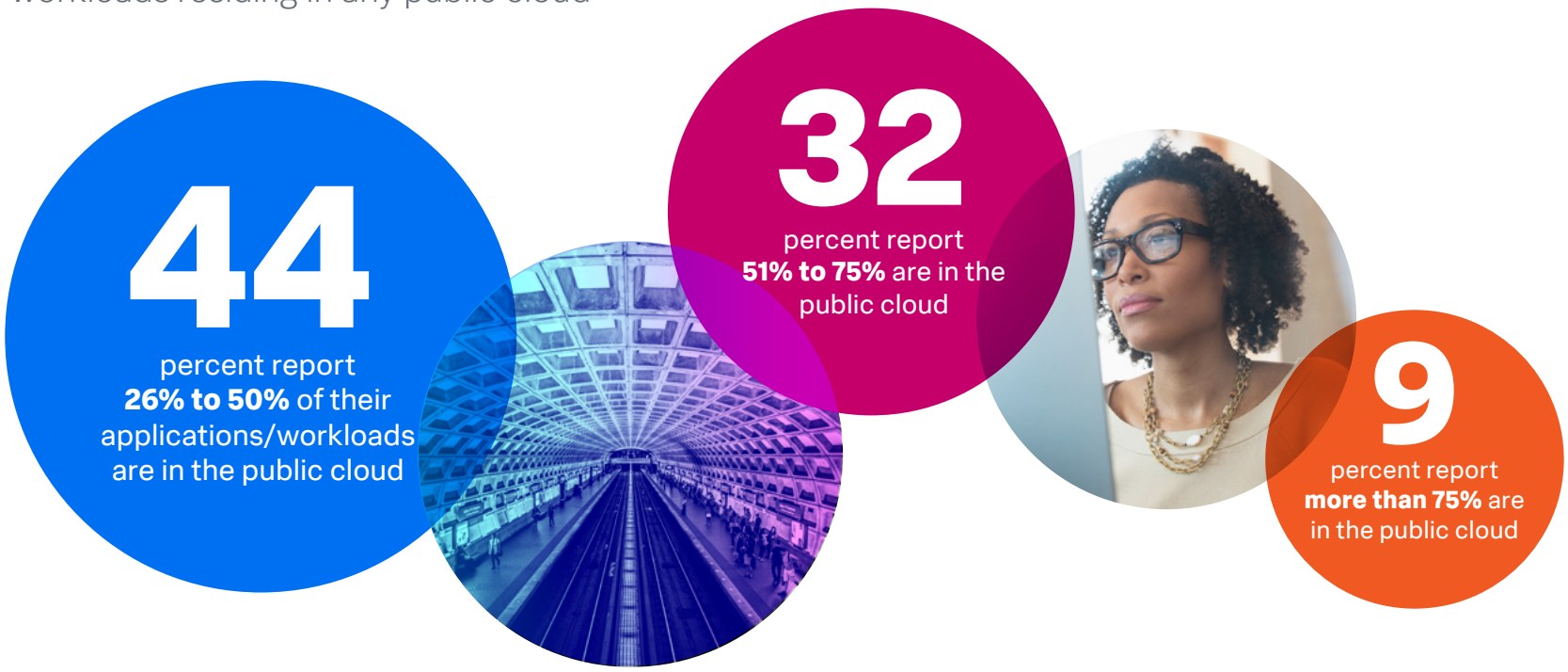
87% total users

Already, nearly nine out of 10 organizations run a substantial portion of their business-critical applications in the public cloud. Only 15% of respondents said that they run 25% or less in the cloud, and 41% said they run more than half in the cloud. Further findings about our cloud-first future include:

- **43% of organizations have a cloud-first policy for new applications. Only 14% have an on-premises policy that would only consider cloud as an exception.**
- **75% of cloud infrastructure users are multicloud today, and two years from now 87% expect to use multiple cloud service providers.**
- **The percentage of organizations using three or more providers is expected to increase from 29% to 53% over the next two years.**
- **While respondents say that 29% of their workloads are cloud-native today, they expect that to nearly double, to 55%, in two years.**

Public Cloud Is Essential

Percentage of organizations' business-critical applications and workloads residing in any public cloud



Multiple trends around cloud adoption will exacerbate existing security challenges. Among our survey group, the top two identified challenges were maintaining security consistency across the data center and public cloud environments (cited by 50% of respondents) and the cost and complexity of using multiple cybersecurity controls (42%). Other challenges include a lack of visibility into public cloud infrastructure (23%), being excluded from development and DevOps teams who worry about velocity (24%), and existing security tools that don't support cloud-native environments (22%).

When it comes to improving security visibility into cloud-native applications, organizations are prioritizing foundational capabilities like "identifying workload configurations that are out of compliance" (42%), "detecting malware" (33%) and "identifying software vulnerabilities" (33%) over more advanced monitoring like auditing permissions associated with service accounts (16%), monitoring for anomalous activity (15%), or watching lateral server and container workload communication (15%).

Cloud-Native Architectures Bring Security Challenges

Top challenges identified by respondents

50%

struggle to maintain security consistency across data center and public cloud environments

42%

find using multiple cybersecurity controls increases associated costs and complexity

29%

struggle with a lack of visibility into public cloud infrastructure

Hard jobs get harder

No one gets into IT security looking for a soft, low-stakes gig. But our respondents uniformly agree that cloud complexities and the disruptions of the pandemic make their jobs even harder. For all its elasticity and speed, the cloud leaves security teams with less visibility and fewer security measures in place — exacerbated by 2020's pandemic rush into the cloud, which shortened security review cycles. For the 49% of respondents who said security is a harder job than it was two years ago, the leading security challenges were:

- **Addressing the increasingly sophisticated threat landscape (48%).**
- **Moving workloads to the cloud making it more difficult to monitor the attack surface (32%).**
- **Workforce hiring (28%).**

Looking at the cloud, key issues were:

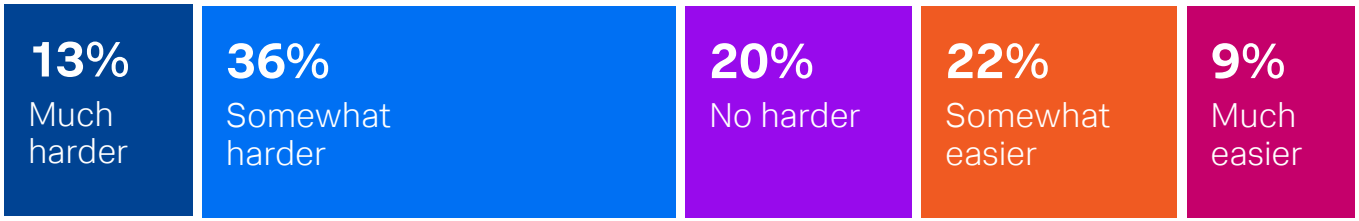
- **Identifying workloads that are out of compliance (42%).**
- **Detecting malware (33%).**
- **Identifying software vulnerabilities (33%).**

The overwhelming number of alerts speaks to the challenge of tool sprawl, and the need for both a consolidated view of security data and automated event triage to reduce the number of alerts escalated for human intervention.

In all, the data points to a specific set of requirements for a security team's success. The teams that will best manage this new era will be adaptive, able to learn quickly. They'll be able to effectively leverage automation to improve reaction time to familiar threats, and free up human attention for the weird and urgent ones. They'll understand their multicloud environment and partner well with the development and operations organizations that run them.

Sounds easy, right?

Security Teams Are Losing Ground



49% of respondents say keeping up with security requirements has gotten harder in the past two years

only **31%** say it has gotten easier

Remote work taxes the SOC

Last March, many organizations made the decision, on short notice and often without adequate preparation, to convert the majority of their office operations to work-from-home. That sudden scramble required heroic efforts from both IT and security teams. More importantly, it required them to make those heroic efforts together.

The COVID-19 pandemic made security teams more tightly integrated partners with business and IT leaders than ever before. Because it was a survival necessity. It also underscored for executives the value of IT security, which helps explain most organizations' plans to increase security spending now.

The most visible challenge of the pandemic was the shift to remote work. As this report is released, many organizations continue some level of pandemic-related remote operations, and numerous surveys have found that most organizations intend to continue remote work policies that are more liberal than they were pre-pandemic. Which works out well, because large numbers of workers report a desire to continue to work from home more often.

Our respondents report that their organizations are securing more than twice as many remote workers now as before COVID-19. The pre-pandemic average was that 23% of workers were remote before the pandemic, and in early 2021, the number was 56%. While this is great for commute-weary workers, it's no party for the SOC: Remote workers are a ripe target for bad actors, for reasons that include network security strategies that are outdated in this remote-work environment, and more employees using personal devices to access work systems, where lower security and shared devices can lead to data leakage.

And, indeed, most respondents report an uptick in attacks:

- **76% of respondents say that remote workers are harder to secure.**
- **53% say there's been an increase in attacks during the pandemic — 12% call it a significant increase.**

Top Remote Worker Security Challenges

31%
Ensuring remote employee devices run endpoint security software

29%
Ensuring remote employee devices have secure configuration

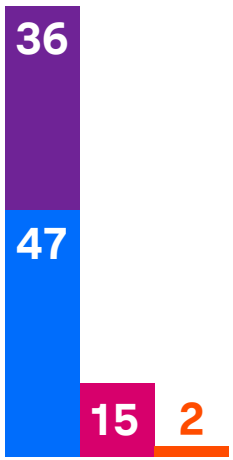
29%
Providing secure access to cloud-based apps/resources

27%
Providing secure access to the corporate network

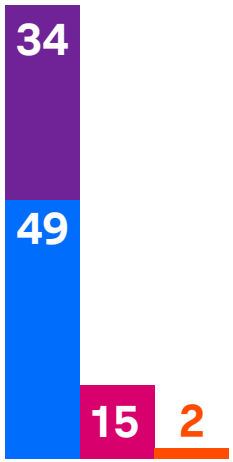
Securing remote workers is hard, and security teams are looking to automate processes, adopt cloud-based controls and more continuously tune detection rules. Their work to date has focused on basic hygiene, access and management of security controls. Only 20% of respondents list monitoring traffic and user behavior of remote employees as a significant challenge tackled in 2020, suggesting that more effort went, necessarily, into securely spinning up remote capabilities than into checking just how secure those capabilities ultimately were.

The greater security/IT/business collaboration during the initial rush to remote work has resulted in positive policy changes, and a stronger focus on process automation and the use of security analytics. This greater collaboration increases the value of viewing and sharing data appropriately across the entire organization, to the benefit of analytics initiatives. We're seeing the results, which include organizations combining security and non-security data to better identify cyber risks that could impact business. These risks can then be tracked to specific business processes.

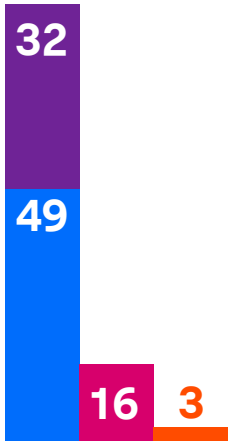
The Security Implications of Remote Work



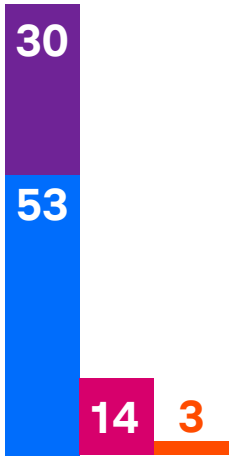
The remote work shift strengthened collaboration between IT/security operations teams



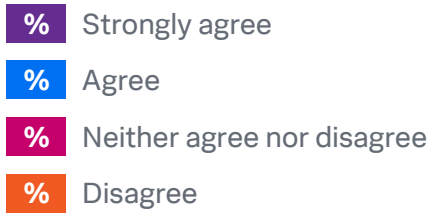
The rise of remote work led to better security process automation



Remote work trends caused an increase in cloud-based security technologies



SOC continually implements rules to address remote-work-related risks



Response to SolarWinds attacks

In December, apparent nation-state hacks of a SolarWinds software update were revealed to have affected up to 18,000 organizations worldwide. Two months after that, we asked our respondents how they had reacted to the crisis, which forced tens of thousands of organizations to check whether they'd been affected by the malware. It also should have forced everyone to reassess how they defend against the possibility of supply chain attacks.

The most surprising finding was that, despite the high level of concern voiced by security teams, two months later, not even half of CISOs had briefed their senior leadership or boards about the SolarWinds hacks and their own organizations' position. We have to ask: What are they waiting for?

Board-Level Discussion of SolarWinds Hacks Lags

Percentage of orgs in which CISO had briefed senior execs/board (as of Feb. 2021)

Respondents did indicate that they'd undertaken a number of steps in the wake of the SolarWinds attacks. The top answers make sense: assessing security controls (35%), increasing security budgets (31%) and more scanning of software updates (30%). But given that only about a third of organizations said they've taken each of those measures, it's not clear whether security leaders were responding sufficiently both to this high-profile compromise and the threat of similar attacks in the future.

Of course, specific responses to the SolarWinds revelation come on top of security practices that were already in place.

For instance, nine out of 10 organizations reported that they frequently scrutinize a vendor's security when considering a purchase, and at least 95% perform various assessments of a vendor's security annually — with high percentages performing some assessments at least quarterly.

Yet these are the practices that were in place before SolarWinds went undetected for most of a (very crazy) year. It's concerning that additional practices hadn't gained more traction.

Post-SolarWinds Security Measures Vary

Percentage of orgs that took specific actions after the SolarWinds hacks

35% Assessed current security controls

31% Increased cybersecurity budget

30% Increased software update scanning efforts

29% Added new detection rules

27% Conducted penetration testing or red teaming exercise

27% Adopted more supply chain security policies

26% Adopted strong authentication tech

26% Conducted third-party risk assessment

26% Conducted incident response activities

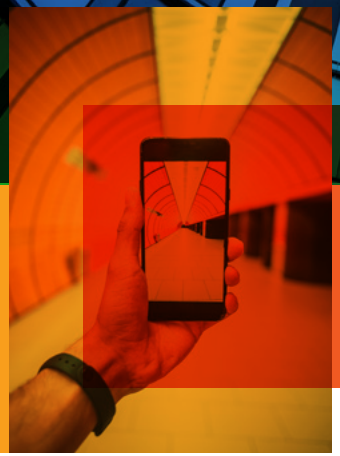
24% Increased meetings between CISO/ executives/board

23% Segmented org network

23% Reassessed vendor risk management policies

17% Replaced infrastructure software with suboptimal security policies

Forward Thinking



Last year required a lot of attention to the immediate security challenges presented by pandemic disruption. As we surveyed security and IT leaders in early 2021, we also looked at their plans to improve their security postures for the future.

With an unbelievable year behind them, we asked our survey group to name their security priorities for the next two years. Their top answers were:

- **Conduct more security training for security and IT operations staff (cited by 25% of respondents).**
- **Investigate or deploy cloud-based security analytics/ operations technologies (22%).**
- **Invest in tools to help automate and orchestrate security processes (22%).**
- **Test security operations processes more often (21%).**
- **Move security analytics/operations technologies to the cloud (19%).**
- **Actively develop an integrated software architecture for security analytics and operations tools (18%).**
- **Hire more security operations personnel (18%).**

On the one hand, these are good priorities. Between two important human-oriented skills, the priorities focus on velocity and insight: getting a better view into cloud applications and infrastructure, automating processes, and doing it all with analytics tools that deliver a better, more comprehensive view of your data and the insights therein.

On the other hand, we'd have expected to turn up a pretty similar list in 2019. For security leaders to adapt their strategies to 2021's realities, the new technologies deployed should include a zero trust strategy — because the old network-focused idea of "perimeter protection" just won't cut it. They should pay particular attention to the new cloud technologies hurriedly deployed to cope with remote workforces because of the pandemic. And tests of security processes should consider the new circumstances: more data in the cloud, and more employees — including security staff — working remotely. (For more, see key recommendations.)

Key technology: security analytics

Two invaluable uses of data are different, and sometimes conflated; there's a difference between data-driven and data-informed. The former means actions are based on data — perfect for automation. Think phishing: A malicious email is identified and remedial action is taken, no need to escalate to a human analyst. Data informed, on the other hand, means humans are making the decisions after receiving insights based on data. Think adjustments to overall security strategy in response to recent patterns of anomalous behavior.

Data analytics straddles both worlds, fueling automated response as well as giving strategic insights to analysts and security leaders. Looking at the research, we found that analytics are the tip of the security spear, aimed at identifying risk and aiding decision-making. Specifically, analytics inform decision-making on a range

of topics, from threat detection and response to decisions about security controls, investments, budgeting and automation.

Our research found not just interest in, but growing adoption of, two key data-oriented technologies: security analytics and machine learning, which powers analytics, automation and more.

Security analytics is the combination of algorithms and analytic processes that detects potential threats to the enterprise. The demand for security analytics has grown in recent years because the speed, sophistication and delivery of malware and other attacks makes it difficult for security analysts to keep up without analytics tools. The research found that 82% of organizations say that security analytics tools play a larger role in their overall security decision-making today than they did two years ago. This indicates a more top-down approach to security, in which analytics drives choices, configurations and more.

We asked respondents why they are increasingly dependent on analytics tools to keep up with modern security challenges. Their top responses were:

- **To support regulatory compliance efforts (37%).**
- **Because they're more often incorporating non-security data (36%).**
- **Because new AI/ML-driven tools are assisting with decision-making (36%).**
- **They have a lot more data to analyze than they used to (36%).**
- **They've applied more security analytics in response to increasing threats (34%).**

Security Analytics Drives Cybersecurity

35%
Agree security analytics plays a **bigger** role now

47%
Agree security analytics plays a **somewhat bigger** role now

16%
Agree security analytics plays the **same** role now

82% of respondents say that security analytics increasingly influences security strategy today compared with two years ago.

Further down the list, respondents noted that their analytics deployment corresponds to a rising use of automation and real-time data (27%) and that a recent data breach prompted a greater reliance on analytics tools going forward (24%).

It's worth noting that 73% of organizations said that they are, in fact, enriching their security analytics with other data sources, a merging of data and solutions that underscores what security leaders have known for years: *All data is (or should be) security data.*

"Analytics tools and a greater reliance on data insights help level the playing field for security analysts," says Splunk CISO Yassir Abousselham. "They need to automate familiar attack responses to give analysts a chance to sort through everything else that may require their attention."

Decisions Most Influenced by Security Analytics

45% Threat detection/ response decision

41% Risk identification

39% Security controls decisions

36% Determining areas where more analytics are needed

25% Investment decision

23% Process automation decisions

23% Budgeting decisions

22% Outsourcing/services decisions

15% Staffing decisions

Key technology: machine learning

Data theft happens fast, and with so much going on, it's easy to miss the hackers until it's too late. That's why machine learning is big: humans can only do so much, and computers are very good at crunching staggering quantities of data. To support the need for better analytics, organizations are turning to machine learning (ML) technologies en masse and looking to combine and consolidate more than just security data to support and speed up decision-making.

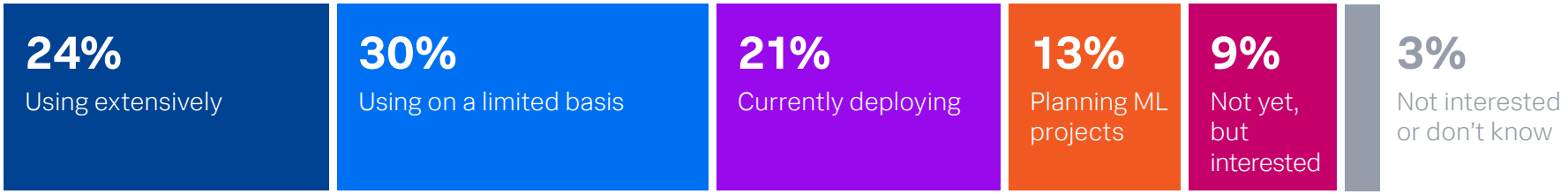
Breaches can go undetected for hours. Or months. Using ML in security analytics helps analysts speed up their discovery and response times, and helps them use data from across the organization (from assets, network performance, applications, etc.), not just traditional security data.

Among the research findings:

- **54% of security teams currently use machine learning in security analytics.**
- **43% of organizations plan to add ML to their security operations, or are interested in doing so.**
- **The leading ML use cases are:**
  - **To identify cyber risks (39%).**
  - **To improve threat detection (37%).**
  - **To handle more incidents with junior-level analysts (29%).**

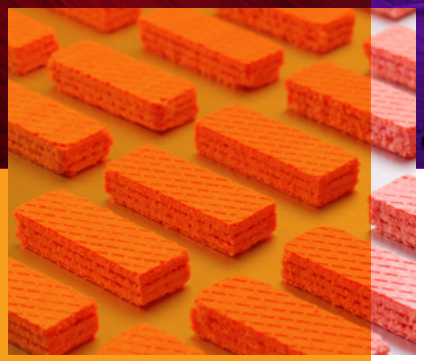
Frankly, we would've expected ML use to be even higher — and it might well be, since many organizations use ML-based products without realizing ML is baked into them.

Organizations Increasingly Deploy ML for Security



88% of respondents are deploying or planning to deploy ML for security.

Security Is a Data Problem



Security teams are experiencing the impact of the Data Age: rapid digital transformation, most notably an aggressive shift to cloud.

That shift was only accelerated by COVID-19, and the SolarWinds attacks underscored the risks that come with rapidly increasing complexity. Together, the lessons of 2020 are fundamentally changing how security is — or should be — done.

If the challenge of the post-COVID Data Age is the complexity of cloud services, hybrid architectures and convoluted supply chains, the opportunity is in all the data. With the right analytics tools, security teams can connect more data dots than ever to find more signs of anomalous activity, software and system vulnerabilities, and real-time attacks. With the right automation, they can handle most problems much faster than through manual processes, without squandering scant human resources.

The survey data also recognizes related lessons:

- **Nearly all respondents — 88% — tell us that security spending will increase at their organizations.**
- **35% say it will increase significantly.**
- **This is especially true in areas like cloud security (cited by 41%) and cyber risk management (32%).**
- **Also significant: plans to add security-focused analytics (22%) and a trend toward process automation (22%).**

The best news in the research was a heightened degree of collaboration across the IT and security spectrum, and a closer focus on increasing security spending to solve cloud complexity through analytics, automation and investment in human talent.

In response to the challenges of the Data Age, we've pivoted into a new age of IT security. And while respondents emphasized that it's harder than ever to keep up with ever-escalating challenges, it appears that security experts are now moving to position themselves for future success.

Areas Prioritized for Increases in Security Spending

41% Cloud security

32% Cyber risk management

27% Network security

24% Security operations

22% Security analytics

21% Endpoint security

20% Data privacy

19% Training cybersecurity staff

17% Security testing

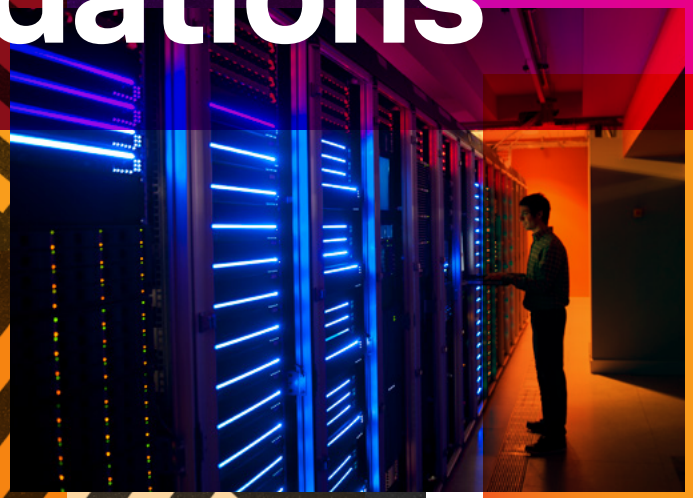
15% Application security

15% Staffing

14% Security services

12% Identity/access management

Key Recommendations



Many security leaders are taking action to keep up with intensifying security challenges. More spending and more technology are only as good as the strategies behind them, so a focus on cloud complexity, with better analytics and a clearer view of your data, is essential. Here are our key recommendations, based on the research.

1. Modernize the SOC.

Security teams are defending an increasingly amorphous battleground against a diverse, ever-improving set of threats and adversaries. They need a cutting-edge command center. Of the technologies and techniques listed below, none alone can completely meet the need. But together, they build a modern, more effective security operations center that's up to taking on today's threats.

Zero trust: Focused on users, assets and resources rather than a network perimeter, zero trust minimizes security risks. The model is built on three principles: Verify everyone and everything, provide the least privileged access, and assume you've been breached. Focusing on data security, zero trust rigorously authenticates the end user. It's a necessary strategy shift for a more fragmented and distributed security environment.

Security operations process automation: It's essential. You can't have human analysts respond to every attack. Instead, they can write the rules so that automated solutions identify and respond to those attacks without human intervention, and faster than a live actor could manage. Security orchestration, automation and response (SOAR) and user and entity behavior analytics (UEBA) are often where automation makes its mark.

Modern SIEM: This is where the analytics investment we found in our research comes to fruition. SIEM systems offer full visibility into activity within your network, empowering you to respond to threats in real time.

Training and staffing: This is every organization's struggle. All these other technologies help you do more with a leaner team, but ultimately, a growing organization facing growing threats needs to grow its security team. You can improve the effectiveness of your analysts through automation and analytics, and you can improve training by reducing the number of tools they have to use to get the job done.

2. Set your sights on a consolidated view of data.

That modernized SOC will include an arsenal of the best tools and customization available. But that can create its own headaches, in terms of training and the ability to understand an incident with data from multiple sources. In a complex, multicloud, multi-service environment, it's essential to be able to see across all that data, not just traditional security data. This highest-level, end-to-end perspective is vital not only to security and compliance efforts, but to successful development and operations as well. A consolidated view of the data creates a single source of truth for security and IT teams.

3. Rethink your approach to supply chain threats.

After the SolarWinds hacks, we're all worried about enemies who might use our friends to exploit our systems and networks. The first principle, to audit your vendors, is harder than it sounds, because your one "videoconferencing vendor" or "payment processing vendor" is actually composed of maybe a half-dozen business systems, through external APIs and services. You need visibility into every data component and flow. You also need to know how to respond quickest when a breach is discovered, both to shut it down and to determine which data may have been compromised.

For supply chain threats (and any other kind), you need to improve your ability to see suspicious lateral movement within your networks. Whether bad guys sneak in through a vendor's software patch or an employee's stolen credentials, you'll want to be able to spot them as they slither through your network looking for the goods.

But weak passwords, poor multifactor authentication methods and not using a single sign-on solution can punch holes in this strategy. This is where organizations need a modern SOC, and a well-defined and closely monitored identity policy with strong enforcement and monitoring, to fill those gaps.

4. Press your collaborative advantage.

Disaster response to COVID-19 required quick action, and drove greater security/IT collaboration. Security teams should continue to build on this shift, because their job is to mitigate potential disasters. At its most fully realized, this takes an organization into DevSecOps, the melding of three interrelated disciplines that, frankly, aren't usually as interrelated as they should be.

DevOps practices broke down the traditional silos between development and operations teams for faster software development and the high-quality delivery of software and digital experiences. The next step is DevSecOps, integrating security. DevSecOps brings all three disciplines into one flow with shared goals and measurements, and tools and practices that reduce friction between the three traditionally siloed groups. This provides an opportunity for security automation and introduces security earlier in the development process.

Even if your organization is not ready to embrace this full philosophical shift, you can use the singular experiences of 2020 to advocate for the importance of integrated security thinking, at every stage of IT and the business.

After all, who knows what 2021 (and beyond) will hold.

Key industry highlights

Across industries, responses were notably similar, though we did see a few trends and unique data points, including:

Communications/media

Communications companies most often reported suffering a data breach in the past two years: 53%, compared with 42% for tech firms, 41% for financial services firms. The cross-industry average was 39%.

Communications and media companies were about 1.5 times as likely to experience a security skills shortage: 44%, against a cross-industry average of 28%.

Communications organizations report a high rate of DevOps teams circumventing security teams: 38%, against an average of 24%.

Communications companies are most likely to have more than 75% of their critical workloads and applications in the cloud: 23%, versus an average of 9%.

Communications companies were more likely to report seeing an increase in cyberattacks due to the rise in remote work: 23%, followed by tech at 16%, against an average of 12%.

Asked if they will increase spending on security in the next 12-24 months, communications companies were most likely to answer "Yes, significantly": 50% against an average of 35%. (Only manufacturing also beat the average, at 38%.)

Financial services

Financial services firms were least likely to cite maintaining security consistency across their on-premises data center and public cloud environments as a challenge: 36% agreed, compared with a cross-industry average of 50%.

Financial services firms have adopted remote work the most aggressively, reporting that 66% of their workforces are remote — one point above the public sector, and 10 points above the average of 56%.

Financial firms were least likely to say keeping up with more devices and new device types presented an increased security challenge: 13%, versus an average of 24%, and highs of 33% (manufacturing) and 28% (tech).

Healthcare

Healthcare/life sciences orgs are least likely to say their security strategy includes moving security analytics/operations technologies from on-premises to the cloud: 11%, versus an average of 19%, and an industry high of 23% (financial services).

For healthcare/life sciences organizations that plan to increase spending, they're the least likely industry to spend on security operations technologies (process automation, security operations visualization, etc.): 14%, versus an average of 24% and a high of 39% (tech).

Manufacturing

33% of manufacturers struggle with their number and types of devices — the highest percentage, and 1.4 times the cross-industry average (24%).

Manufacturers also suffer lost productivity slightly more than most, at 42%, compared with an average of 36%.

Manufacturing companies lead in terms of integrating non-security data with security data to support decision-making.

More manufacturers use software-as-a-service solutions than any other industry (83%, versus an average of 69%).

Retail

Retailers are nearly twice as likely as the average (36% versus 20%) to struggle to keep up with an overwhelming number of alerts.

Retailers were also most likely to say that their security stack and the number of tools/vendors have become overwhelmingly complex (39%, versus an average of 25%).

Public sector

The public sector is most likely to use four or more IaaS and PaaS providers: 19% vs. a cross-industry average of 8%.

That number is expected to climb to 39% in two years, still leading, with the industry average expected to be 21%.

The public sector is most likely to have an on-premises policy for new applications (24%, versus an average of 14%).

The public sector was least likely to report having suffered a data breach in the past two years (22%; the average was 39%).

Technology

54% of tech companies suffer from significant IT time for remediation following security incidents, compared with a 42% cross-industry average.

They have also seen high rates of insider attacks: 44%, outdone only by communications/media, at 47%. The cross-industry average was 27%.

Tech orgs, along with communications/media companies, report the highest uptick in attacks.

Insider attacks were most common in tech (44%) and communications/media companies (47%), compared with an average of 27%.

Key regional highlights

Regional variations in the responses were surprisingly subtle in terms of their experiences and their response to the latest security threats, but there were a few notable differences:

Asia Pacific (APAC)

APAC organizations lag on cloud-native application architecture adoption: 52% of them have no cloud-native, business-critical workloads at the moment, while that percentage is 44% for North American orgs and 49% for Western European orgs. However, APAC will likely catch up — they on average anticipate 56% of business-critical workloads to be cloud-native 24 months from now, versus 57% for North America and 52% for Western Europe.

With respect to cloud-native apps, 38% of APAC respondents cite issues with cloud infrastructure visibility (more frequently than North America, 25%, or Western Europe, 26%). Also, 30% say that they struggle because of tools that don't support cloud-native applications (versus 19% for North America and 20% for Western Europe).

APAC organizations currently report the lowest rate of remote work, at 50% (versus an average of 56%). Pre-COVID, North American organizations had the lowest rate of remote work — 20%, versus 25% in APAC and 26% in Europe.

Western Europe

42% of European organizations tend to focus on malware detection in cloud-native scenarios (versus 32% and 25%, for North America and APAC, respectively).

With respect to cloud-native applications, respondents in North America (52%) and Europe (55%) more often report that consistency across clouds is an issue (as compared with 42% among APAC orgs).

Respondents in Europe are less concerned about SolarWinds-like attacks: 74% of their orgs are concerned/very concerned, whereas it's 77% for North America and 86% for APAC. But Western European orgs have most often increased their budget as a result (40% are planning the increase, versus 28% and 27% among North American and APAC orgs, respectively).

European organizations are 1.6 times as likely to have automated security processes with real-time data (36%, versus 23% for North America and 23% for APAC).

North America

North America leads in terms of public cloud infrastructure adoption — 47% of respondents there have more than half of their business-critical applications and workloads in the public cloud, whereas it's 40% for Western Europe and 25% for APAC.

With respect to cloud-native apps, respondents in North America (52%) and Europe (55%) more often report that consistency across clouds is an issue, as compared with 41% of APAC orgs.

Methodology and demography

The survey was conducted in February 2021 by the Enterprise Strategy Group. The 535 respondents were drawn from nine global regions, and consisted of senior decision-makers in cybersecurity and IT.

Regional demographics

- North America (U.S., Canada): 48%
- Western Europe (France, Germany, UK): 29%
- Asia Pacific (Australia, Japan, New Zealand, Singapore): 23%

Industry demographics

- Financial services: 16%
- Manufacturing and resources: 16%
- Healthcare and life sciences: 14%
- Retail and wholesale: 13%
- Communications and media: 12%
- Technology: 9%
- Public sector: 7%
- Other: 12%

Splunk security solutions

Splunk Enterprise

The Splunk platform is a customizable data analytics platform that turns data into tangible business outcomes. Unlike SaaS and other open source alternatives, Splunk Cloud and Splunk Enterprise enable you to leverage your existing technology investments, as well as the expansive and expanding data generated by your IT, security and business systems, apps and devices to investigate, monitor, analyze and act in near real time. Learn more.

Splunk Enterprise Security

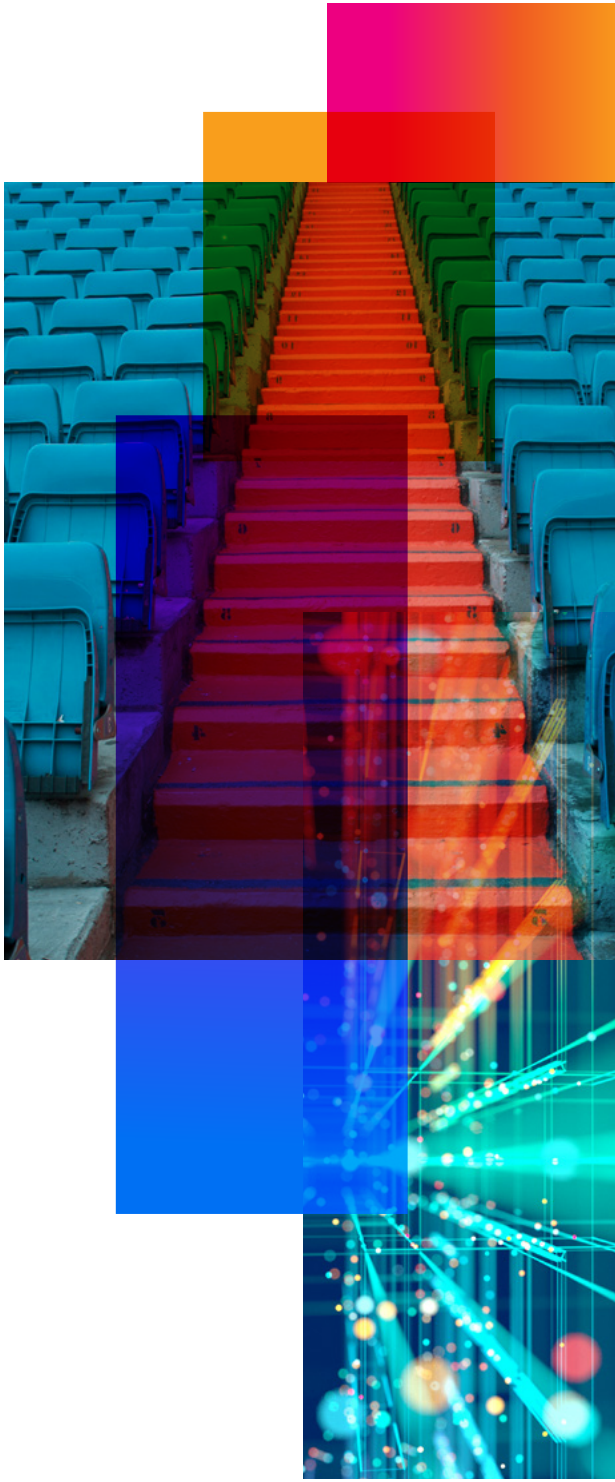
Splunk Enterprise Security (ES) is an analytics-driven SIEM solution that provides real-time security monitoring, advanced threat detection, incident investigation and forensics, and incident response for efficient threat management. Splunk ES enables faster threat detection, investigation and response. Learn more.

Splunk User Behavior Analytics (UBA)

Splunk UBA is a machine learning-powered solution that finds unknown threats and anomalous behavior across users, endpoint devices and applications. It augments your existing security team and makes them more productive by finding threats that would otherwise be missed due to lack of people, resources and time. Learn more.

Splunk Phantom

Splunk Phantom is a world-class security orchestration, automation and response (SOAR) system. Splunk Phantom combines security infrastructure orchestration, playbook automation and case management capabilities to integrate your team, processes and tools. Learn more.



Splunk Inc. (NASDAQ: SPLK) turns data into doing with the Data-to-Everything Platform. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale. Our powerful platform and unique approach to data have empowered companies to mitigate risk, improve service levels, reduce operations costs, enhance DevOps collaboration and create new product and service offerings.

Learn More

21-17605-Splunk-State of Security 2021-116

splunk>