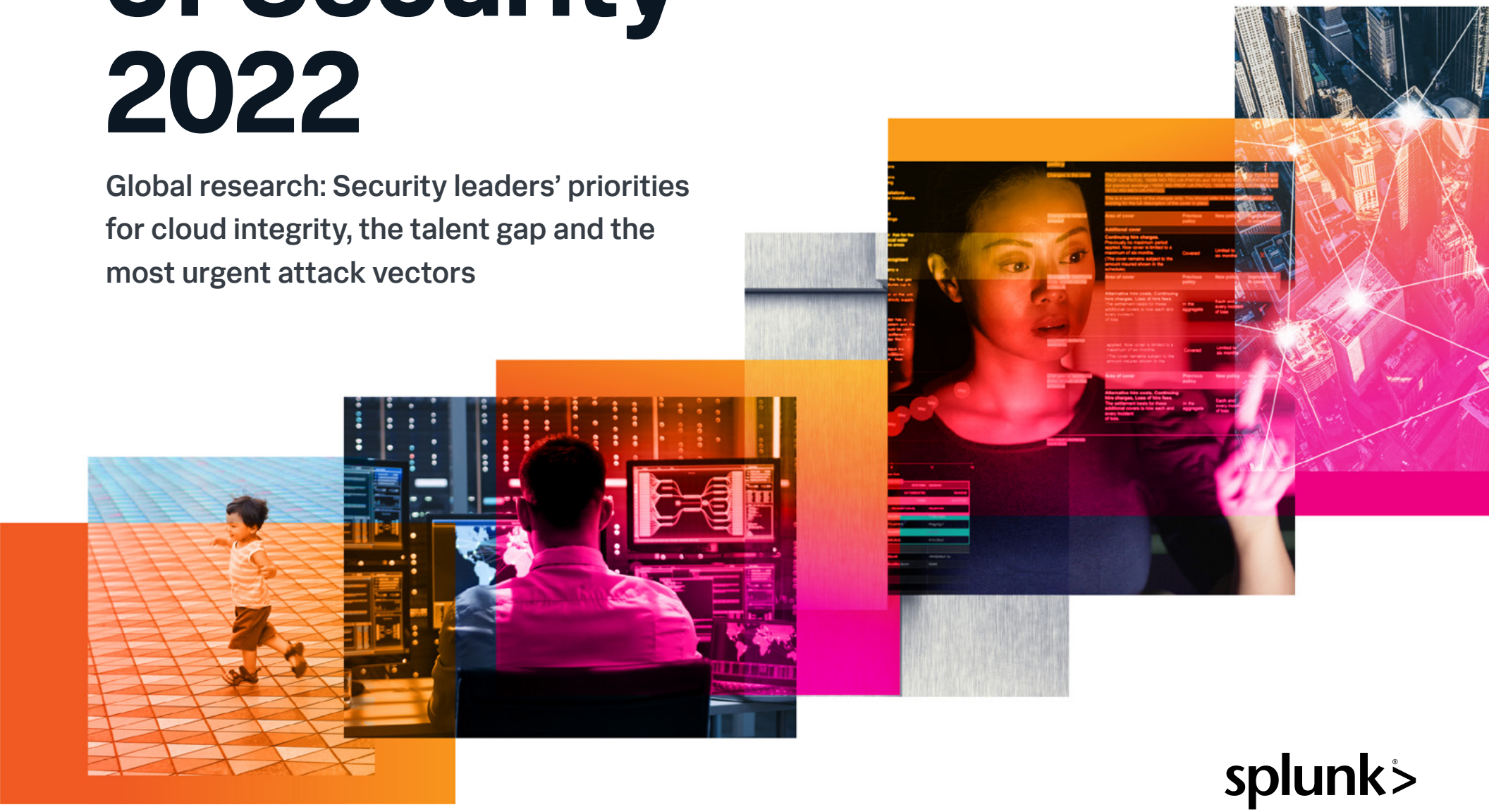
The State of Security 2022

Global research: Security leaders' priorities for cloud integrity, the talent gap and the most urgent attack vectors



splunk>

The Heat Is (Still) On

The state of security in 2022 is highly adrenalized — more so than usual. Two years into the deadly and disruptive global pandemic, not only are we continuing to see more attacks, we're also seeing more actual breaches.

New global research conducted by Splunk and the Enterprise Strategy Group of more than 1,200 security leaders found that 49% of organizations say they'd suffered a data breach over the past two years, up from 39% in our survey a year earlier. And while certain attack vectors dominated headlines in the last year or two, criminals are still finding success with traditional playbooks:

- 51% report business email compromise, up from 42% a year ago.
- 39% of organizations report insider attacks, up from 27% a year ago.
- 79% say they've encountered ransomware attacks, and 35% admit one or more of those attacks led them to lose access to data and systems.

Additionally, 40% of respondents report a regulatory violation (up from 28% a year ago). More and more sophisticated attacks, acute talent shortages and pandemic-specific challenges have SOCs reeling.

It's not clear whether these numbers are a sobering indication that attackers are significantly more successful today or if, as Splunk Distinguished Security Strategist Ryan Kovar notes, it's a question of causation versus correlation. Are intruders better at penetrating our defenses, or are security teams better at detecting intruders? The answer is probably "both," with offense and defense each improving aspects of their game.

"And ransomware skewers this because they actively tell you that you're compromised," Kovar says, "while traditional attackers try to get in and out without being detected."

Regardless of why security teams are detecting more breaches, they're having to work a lot harder, and are feeling greater effects than ever before.

All told, 59% of security teams say they had to devote significant time and resources for remediation (up from 42% a year ago). Forty-four percent say they've suffered disruption of business processes (versus 35% a year ago), and 44% say they've lost confidential data (up from 28% a year ago).

Methodology

Researchers surveyed 1,227 security and IT leaders who spend more than half their time on security issues.

11 Countries

Australia, Canada, France, Germany, India, Japan, Netherlands, New Zealand, Singapore, United Kingdom, United States

15 Industries

Aerospace and defense, consumer packaged goods, education, financial services (banking, securities, insurance), government (federal/national, state and local), healthcare, technology, life sciences, manufacturing, media, energy, retail/wholesale, telecom, transportation/logistics, utilities

The costs of these incidents are not theoretical, and they matter to more than the security budget. In addition to lost business, ransoms and reputation loss, downtime is hugely expensive for the entire organization. The majority of respondents (54%) report that business-critical applications suffer unplanned downtime due to a cybersecurity incident on at least a monthly basis, with a median of 12 outages per year.

Moreover, the median time to recover for business-critical workloads suffering from unplanned downtime tied to a cybersecurity incident is 14 hours. We asked respondents to estimate the hourly cost of downtime for business-critical apps, which across the survey sample averaged about $200,000. That told us that the average annual cost of downtime tied to cybersecurity attacks for organizations today is about $33.6 million.

In short, the eternal battle between attackers and defenders has been made worse by rising complexity. Intricately woven hybrid, multicloud environments host modern cloud-native, microservices-based applications alongside legacy technologies, and now everyone needs to be able to access it all from their spare bedroom.

Security teams must gain complete understanding of, and visibility into, their cloud infrastructures to focus on cloud hygiene. They face new challenges around secure configuration, software vulnerabilities, compliance, and the need to maintain an audit trail of access and activity for all of it. At the same time, they need to revisit org-specific threat models based on novel attack chains.

Let's see how that's going.

Cyberattacks Cause Frequent Downtime

54% report at least monthly outages

Security teams are falling behind

Fully 64% of respondents say keeping up with security requirements has gotten harder in recent years, up from 49% a year ago. Top reasons include:

- **The dangerous threat landscape (say 38% of respondents; down from 48% but still ranked first).**
- **An overwhelmingly complex security stack (30%, up from 25% and fifth place a year ago).**
- **Skilled labor recruitment and retention issues (both 29%, both up slightly from last year).**

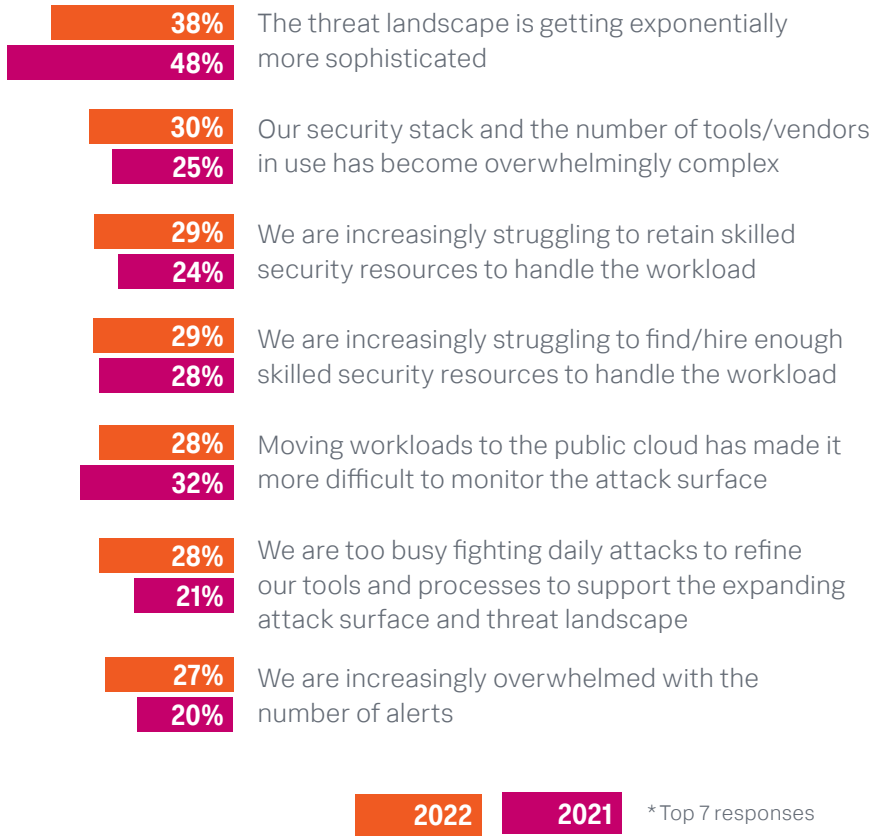
Top challenges for security teams include:

- **Over-rotating to focus on compliance over best practices (29%, up from 23% and the fourth most cited response last year).**
- **Spending too much time addressing emergencies (28%, up from 26% and the second most frequently cited response a year ago).**
- **Struggling to manage the complexity of security technologies (26%, up from 24% and maintaining its position as the third most cited challenge).**
- **Dealing with the challenges of being understaffed (26%, up from 22% a year ago and the fifth most cited challenge).**

All told, the necessary attention to compliance, too much time on reactive footing, and the challenges of too much complexity and too few people conspire to distract the SOC from focusing on emerging threats.

Why Security Keeps Getting Harder*

More threats, more complexity, fewer people.



Remote workers remain a challenge

The advent of the COVID-19 pandemic in early 2020 created unprecedented challenges for security experts and, as we noted in last year's report, new levels of collaboration and cooperation among security, IT and business teams. Two years later, many of the challenges remain vexing, perhaps none more than remote work.

Organizations are still supporting, on average, double the number of remote workers compared to pre-pandemic norms. While today's average, 46% of workforces, is 10 points lower than in 2021, there's no return to pre-pandemic levels in sight. Organizations expect that 12 months out, 41% of their workers will remain remote. As a result, 90% see a need to adjust security controls and policies.

This shift to more remote work has resulted in operational challenges, including ensuring access to the corporate network (noted by 29% of respondents), making sure devices in use are securely configured (28%) and securing access to cloud assets (27%).

Remote Work: Yesterday, Today, Tomorrow

Remote work has surged, and isn't expected to subside.

21%
of pre-pandemic workers were remote

46%
work remotely **today**

41%
of workers are projected to be remote **a year from now**

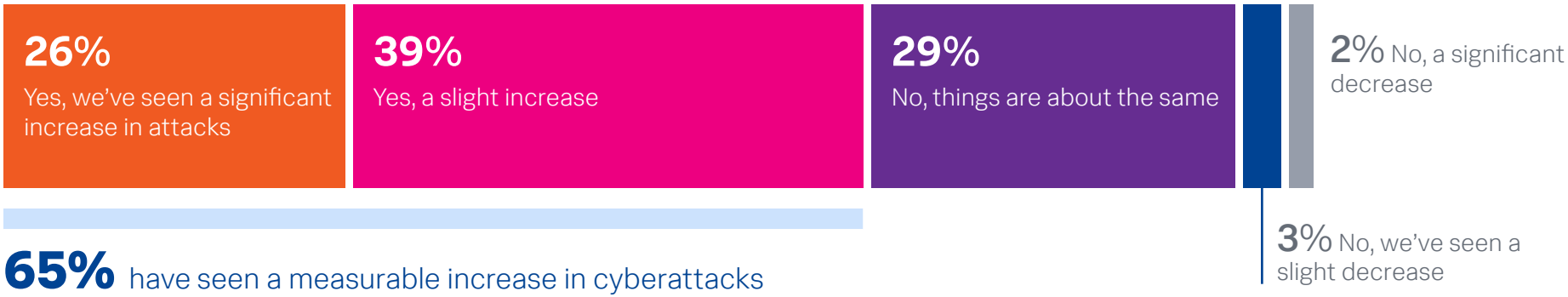
While remote work and other pandemic measures have been stressful for IT organizations and business units, security teams have been particularly hard hit: 80% say that the SOC has to continually create and implement new threat detection rules to accommodate remote workers.

Additionally, 65% of organizations have seen a measurable increase in attempted cyberattacks, which is particularly problematic since 78% say remote workers are harder to secure.

As noted above regarding successful breaches, these rising numbers aren't necessarily caused only by proliferating attacks. Organizations may also be getting better at detecting attacks.

Still, respondents attributed the rise in attacks at least in part to the greater attack surface that widespread remote work presents.

Remote Work, Rising Attacks



65% have seen a measurable increase in cyberattacks and attribute it to more remote work

Supply chain worries are front and center

There has been a lot of buzz around the concept of supply chain attacks since the discovery, in late 2020, of the SolarWinds hacks, followed by the Kaseya attack, Log4Shell and others. Our State of Security survey in 2021 was conducted two months after the SolarWinds disclosure, and at that time, only 47% of CISOs had briefed boards or the C-suite on supply chain risks. A year later, the continued buzz has inspired strategic action.

Ninety percent of organizations — nearly everyone — reported that they have increased their focus on third-party risk assessment as a result of those high-profile attacks. In fact, 61% of CISOs are now regularly briefing their boards and/or line of business executives about activity in this space (up from 47% a year ago, just two months after SolarWinds).

New attention to this attack vector has led 97% of organizations in our survey to have taken some kind of action. Most often (33%, up two points year-over-year), respondents have increased their cybersecurity budget. Also of importance is the CISO's ability to engage business leaders and the board of directors. Fifty-four percent of respondents say that such discussions accelerated actions, and another 38% say these actions wouldn't have taken place otherwise.

"All of this is a huge change," Kovar says. "In my 20 years in IT security, I've never seen software supply chain threats reach this level of visibility."

The change may not be entirely a hype response. Forty percent of survey respondents said that their organization had been affected by a supply chain attack. Kovar says that supply chain attacks will soon change how software is bought and sold.

"We're likely to see buyers require an SBOM, a software bill of materials," he says. "It will list the elements within a complex software package, so that when a supply chain attack is discovered, you can quickly know if your organization is vulnerable."

Top Responses to Rising Supply Chain Attacks

33%
Increased cybersecurity budget

29%
Assessed security controls to determine whether they'd prevent/detect such attacks

27%
Increased the frequency of meetings between CISO and execs/board

27%
Adopted some form of strong authentication technology, such as multifactor

Ransomware: Playbooks and payoffs

If there's something driving more concern in 2022 than supply chain attacks, it's probably ransomware (which, as in the Kaseya and Log4Shell cases, can come through the supply chain). Last June, in the wake of its executive order on cybersecurity, the Biden Administration issued a memo specifically on ransomware. Beyond concern, organizations are taking action: 84% of organizations surveyed have developed a formal ransomware playbook — a list of required steps for responding to a ransomware attack. But to date it's been a reactive response; of organizations that suffered a successful ransomware attack, 71% only developed a playbook after they had been successfully attacked.

The top response to ransomware: Pay up. Among respondents who fell victim to a successful ransomware attack, only 33% avoided the ransom by restoring from backup. About 66% reported that the criminals were paid, either by the organization (in 39% of cases) or their insurance company (27%). Asked how much the largest ransom paid to attackers was, the average response was about US$347,000.

It's worth noting that those who have not been successfully hijacked have more swagger. Among respondents who had not fallen victim, only 42% reported that their organization is likely to pay off the attackers.

"That may be a case of overconfidence in remediation plans," Kovar says. "Once their disaster recovery or backup capability is put to the test, many orgs might discover that it's not as easy as they thought."

Apart from better response planning, security leaders are putting their faith in data: 88% agreed that better capture and analysis of detection data is one of their most effective tools for preventing successful ransomware attacks.

Most Orgs Were Ransomware Targets

79% fended off an attack … or fell victim.

Security teams reel from talent crisis

Security talent is always scarce. But this year, security leaders are facing an especially daunting labor shortage.

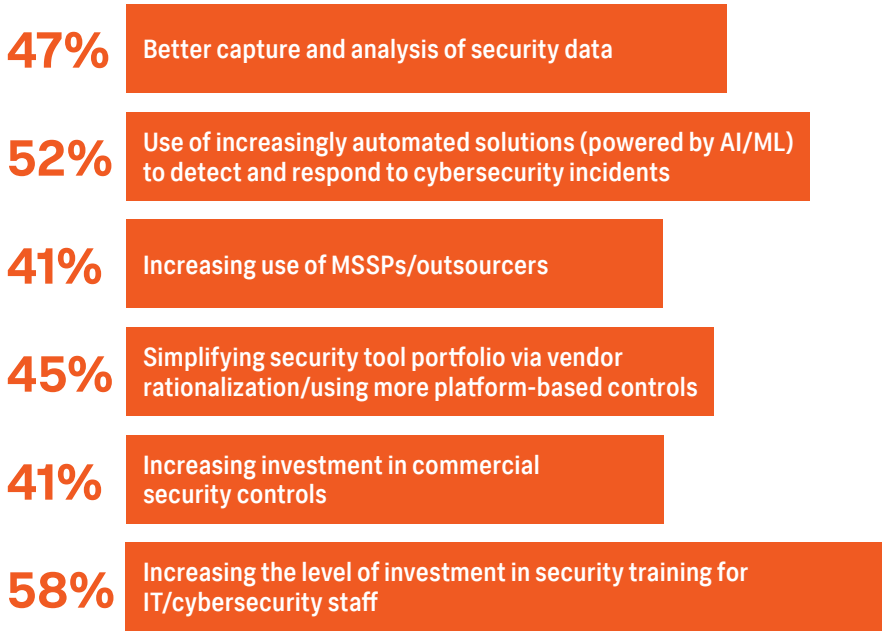
Fully 87% of respondents report skills or staffing challenges; 53% say they can't hire enough staff and 58% cite an inability to find talent with the right skills. Again, a perennial issue, but these trends are heading in the wrong direction: 85% say it has gotten harder to recruit and retain talent over the past 12 months — during which the so-called "Great Resignation" played out across industries.

The ongoing talent challenges have led to a number of issues:

- **70% say that the resulting increase in their workload has led them to consider looking for a new role.**
- **76% say team members have been forced to take on responsibilities they aren't ready for.**
- **68% report that talent shortages directly led to the failure of one or more projects/initiatives.**
- **73% say that workers have resigned, citing burnout.**

That last stat is especially troubling. If resignations lead to more resignations, the talent crisis becomes self-perpetuating.

Most Promising Security Strategies (Besides Hiring)



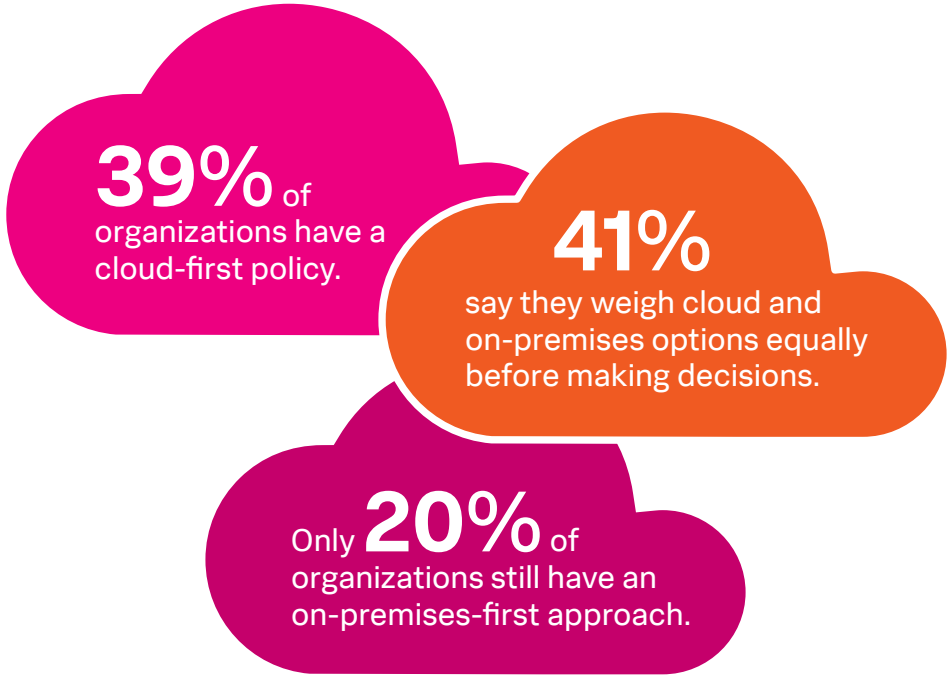
The State of Cloud: Business-Critical Baseline

Across the board, the still-growing role of cloud computing has become essential to organizations. About 73% use multiple public clouds today, and when compared to a year ago, we see multicloud realities have continued to expand: 34% use three or more public cloud service providers (up from 29% a year ago). The trend will continue: 56% expect they will use three or more public cloud service providers (IaaS and PaaS) 24 months from now.

And those secondary clouds aren't secondary. Sixty-five percent of multicloud users report meaningful utilization across clouds; only 35% say that their secondary clouds are minor/niche.

Cloud-hosted applications are now performing business-critical functions across lines of business; 66% of respondents say the majority of their business-critical apps are cloud-hosted, up from 41% a year ago.

Cloud has taken over IT infrastructure



Cloud hampers security visibility

Though the migration to cloud has been a steady story for years, it greatly accelerated with the COVID-19 pandemic. Security teams find the resulting complexity daunting. The growing criticality of cloud puts pressure on security leaders to understand the cloud. More than three-quarters of respondents (79%) say their CISO is under pressure to demonstrate increased cloud fluency.

Two cloud-native security challenges continue to stand out:

- **Maintaining consistency across data centers and cloud (45%, down from 50% but still the top cloud security challenge)**
- **Use of multiple security controls leads to cost and complexity (37%, down from 42% but still the No. 2 response)**

It would seem that one problem begets the other: More point tools create more silos and potential blind spots, which may spur the adoption of more narrowly focused tools.

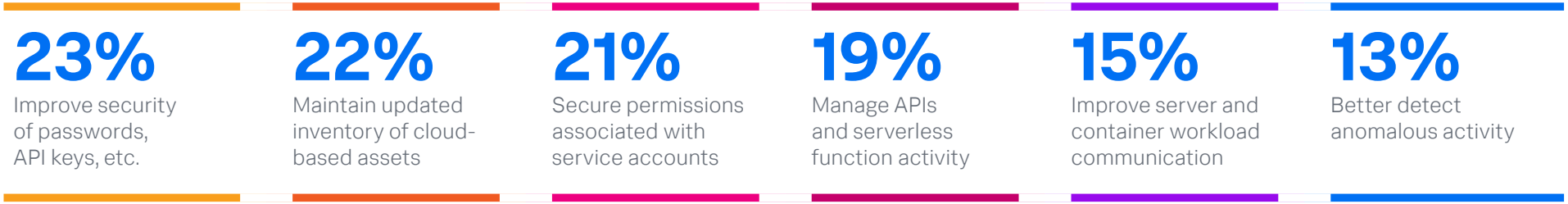
In terms of cloud security visibility areas in need of improvement, the top two responses (see chart below) were also leaders last year. A notable change is that the No. 3 response, maintaining a clear audit trail of account activity, rose from the fifth most common spot last year to No. 3 in 2022.

As with talent shortages leading to burnout leading to attrition, cloud complexity has a self-perpetuating aspect: The complexity of infrastructure elements leads to a crazy quilt of multiple point tools. The resulting silos further hamper visibility and exacerbate operational cost challenges.

"Security teams generally seem to just be figuring out the scope of their cloud challenges," says Ryan Kovar. "Three years ago, I was hearing, 'Wait, I have to monitor the cloud?' Now it's, 'Of course I have to monitor the cloud. But how?' That's what I think of in terms of increasing organizations' cloud fluency."

Most Important Ways to Improve Cloud Visibility

Configuration issues lead concerns.



Responding to Rising Challenges

Having taken measure of the multifarious challenges of modern IT security, we turn our attention to solutions, to the technologies and techniques that organizations worldwide are using to keep up with — and maybe get ahead of — the bad guys.

Talent solutions

Asked to pick strategies that will overcome the talent crisis, our respondents picked a combination of tools and training.

- **58% selected "increase funding for training" from a list of options.**
- **52% picked "increase use of cybersecurity tools with AI/ML."**

Additional strategies included:

- **Better capture and analysis of security data: 47%**
- **Simplifying security tool portfolio (vendor rationalization or platform-based controls): 45%**
- **Increasing use of MSSPs/outsourcers: 41%**
- **Increasing investment in commercial security controls: 41%**

Of course, those two strategies are not mutually exclusive, and pretty much everyone is embracing automated tools powered by AI/ML: 80% agree that at some point in the next three years, the majority of security operations center activities (e.g., threat detection, investigation and response) at their organizations will be automated with little human oversight.

That's not to say that you can automate your way out of a talent crunch, and many organizations are trying new approaches. One of the more difficult cybersecurity roles to find are cloud security architects and cloud security engineers. The Venn diagram of cybersecurity skills and cloud computing knowledge just doesn't have enough overlap. In response, many organizations are asking their developers to codify security processes so that they are reusable and repeatable across project teams.

"Automation can help, if you're careful that you're not just giving people more tools to monitor," says Splunk Distinguished Security Strategist Ryan Kovar. "And on the recruitment front, we have to start considering alternative talent pools because there will never be enough security talent as it's traditionally defined."

For more on both those strategies, see **Key Recommendations**, below.

The talent shortage, in brief:

- **30%** of security leaders say they can't hire enough staff to handle the workload.
- **35%** say they can't find staff with the right skills.
- **23%** say both factors are a problem.
- A lucky **13%** say they suffer neither challenge.

Analytics and automation are increasingly essential

Analytics and automation capabilities let security analysts work smarter and respond to threats at machine speed. Eighty-two percent of respondents say their CISO is under pressure to increase their data analysis capabilities. Fully 85% (up from 82% last year) say that security analytics plays a bigger role in their overall cybersecurity strategy and decision-making today than it did two years ago.

Organizations' strong investment in analytics, automation and SOAR (security orchestration, automation and response) technologies continues:

- **67% of organizations are actively investing in technologies designed for security analytics and operations automation and orchestration.**
- **Of those, 35% report that their organization uses or will use the automation and orchestration capabilities built into their security information and event management (SIEM).**

The embrace of automation and analytics tools correlates with DevSecOps trends (more below); 35% of respondents report that their organization has built or will build security rules using DevOps tools for automation and orchestration (the most frequently cited approach).

77% of organizations have integrated non-security analytics solutions (for business, IT operations, risk management) with cybersecurity-specific analytics to support decision-making.

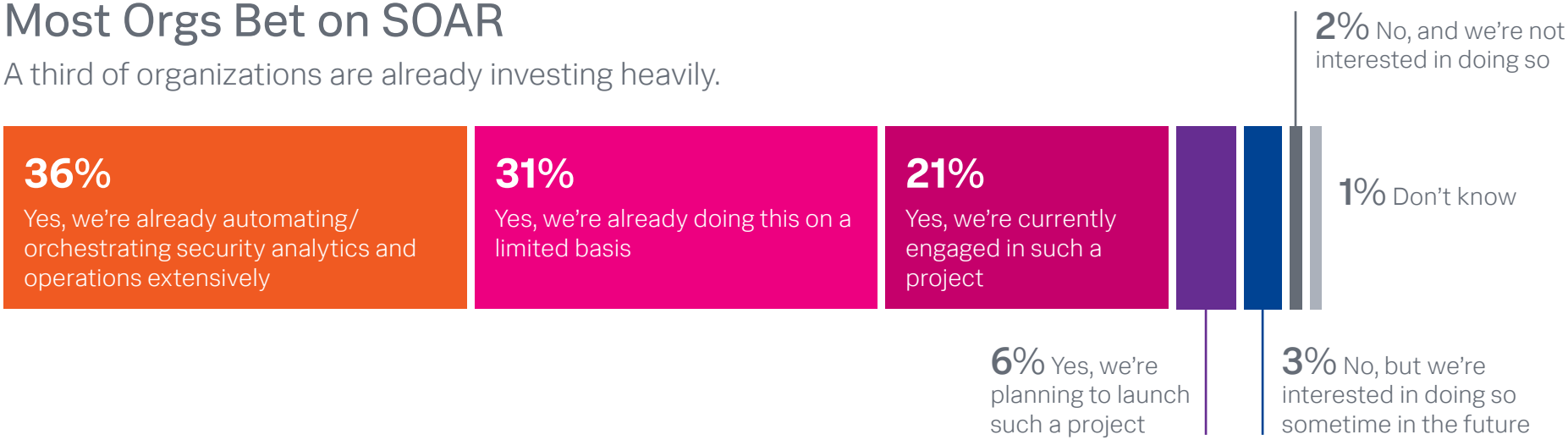
Analytics and automation technologies are not only more prevalent in SOCs worldwide, they're increasingly sophisticated. Now 63% of organizations (up from 54% a year ago) have deployed machine learning technologies for security analytics. Most often organizations look to ML-based technologies to improve threat detection (37%), get more scale from junior analysts (31%) and to automate remediation (30%).

The top priorities for incident response automation were to:

- **Integrate security tools with IT operations systems: 29%**
- **Improve security/ITOps collaboration: 28%**
- **Provide capabilities for "hunting" activities: 28%**
- **Automate basic remediation tasks: 26%**
- **Integrate external threat intel with internal security data analysis: 26%**
- **Collect and centralize data from various security tools: 24%**

Most Orgs Bet on SOAR

A third of organizations are already investing heavily.



The shift toward DevSecOps

DevSecOps has increasing mainstream appeal to help security scale alongside pressures to drive faster development and deployment of applications. Fully 80% of respondents say their CISOs are under pressure to develop their DevSecOps skill sets. (Like DevSecOps adoption, the number of things CISOs are under pressure to improve continues to grow.)

For our research, we defined DevSecOps as "a collaborative software engineering, operations and cybersecurity practice of incorporating the cybersecurity measures and controls at each phase of the CI/CD [continuous integration and delivery/deployment] process." Not that we needed to tell them — 75% of organizations say they use DevSecOps today.

Roughly three-fifths report that DevSecOps entails automating security workflows such as:

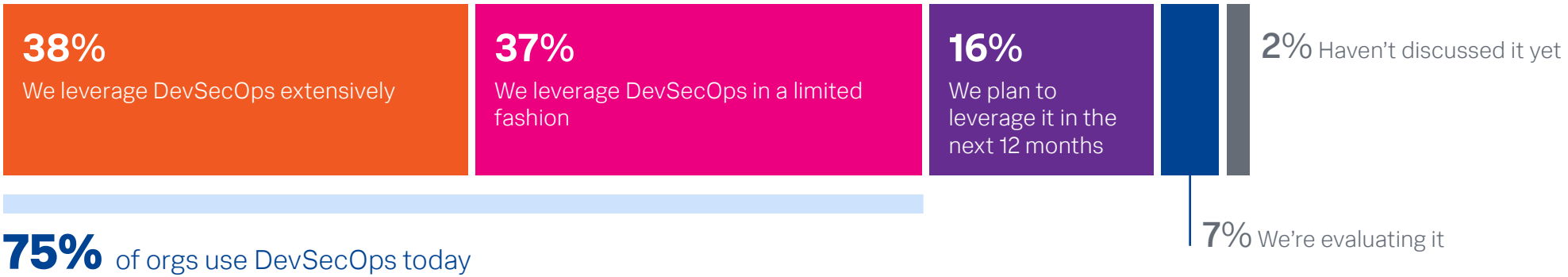
- **Identifying and remediating software vulnerabilities prior to production (62%)**
- **Identifying and remediating malware prior to production (64%)**
- **Applying runtime API security controls (61%)**
- **Logging code changes for audit (59%)**

Though the general DevSecOps principle of baking security into the beginning of the development process, rather than as a late-stage gating factor, is well understood, we asked respondents why they've adopted the DevSecOps approach. The leading drivers:

1. **To allow cybersecurity to keep pace with fast-moving development teams (46%)**
2. **To establish a more proactive security posture (43%)**
3. **To gain greater operational efficiencies via automation (41%)**
4. **To better secure cloud-resident data (41%)**
5. **To foster collaboration between our cybersecurity, development and operations teams (39%)**

But does it work? Yes. Seventy percent of DevSecOps adopters report an improvement in the cybersecurity team's ability to keep pace with development teams; 70% report a more proactive posture; and 69% report an improvement in their ability to secure cloud-hosted data.

DevSecOps Is Mainstream



The Path Forward

While the challenges continue to increase, our research shows that organizations are taking smart steps to keep up — and maybe even get ahead — of the ever-shifting threat landscape.

Pressure is a key theme coming out of this 2022 research. Criminal and nation-state adversaries maintain pressure through attacks of increasing volume, variety and sophistication. And as business leaders better recognize the intensity of the cybersecurity landscape, and the existential stakes, they demand more of security leaders. Fortunately, there's also a degree of willingness to pay for it.

Nearly every organization we surveyed — 93% — expect to increase spending on security over the next 12-24 months (up from an already impressive 88% a year ago). Increasing training for cybersecurity and IT operations staff is still the leading area of focus (cited by 26% of respondents).

Immediate Security Priorities*

Actions orgs will focus on in the next two years.

* Top 9 responses

Key Recommendations

There's more attention on security concerns, from the board of directors on down. There's more pressure on security teams, from the CISO on down. And for many organizations, there's more funding, but does anyone ever think it's enough?

In a world suffering ever-rising threats of ransomware, supply chain attacks and staff burnout, to say nothing of the constant threats of insider attacks and social engineering — the baseline hurricane, if you will — here is the advice that emerges from this global survey.

1. Seek talent, teach skills.

Organizations are already telling us that they're prioritizing efforts to find, train and retain talent. All the traditional efforts in that sphere are important, and recommended. But they're not enough. The field of security analysts is just too small to ever meet the demand, which is why Ryan Kovar focuses on "talent" in its original meaning, not just as a euphemism for "workers."

"You're never going to fill the gaps with the traditional security workforce," he says. "We have to consider alternative candidate pools."

That can include people with experience in non-security IT roles, but Kovar says he looks even further afield. "We need raw talent, not trained skills," he says. "I've had a lot of luck recruiting people with journalism, HR and creative backgrounds. I just need people with innate curiosity and a talent for synthesizing and understanding data."

People with a degree in the humanities, he has found, can be phenomenal at that — often better than those with traditional computer science degrees.

"I can teach the security analyst role to someone who can synthesize data and communicate it more easily than I can teach someone who just knows how to code in C++."

2. Know your cloud.

Nearly eight in 10 respondents told us that CISOs are under pressure to increase their cloud fluency. A significant number also expressed confusion over where security responsibilities between their teams and their cloud providers connect. Everyone from senior security leadership to tier one security analysts needs to understand their hybrid, multicloud environment.

Organizations must dedicate time and training to understand the complex interplay of their public, private and SaaS solutions. They need the tools and training to securely configure various environments, to manage access and authentication, and to minimize MTTD and MTTR (mean times to detect and recover).

Many organizations are still in a state of confusion about the cloud, and that's a risk that has to be eliminated through a comprehensive approach to skill sets, tool sets, cross-team collaboration and education.

3. Build an SBOM.

We mean *really* know your cloud. And all your software. Every software organization should maintain — as in, keep relentlessly current — a software bill of materials that lists all software components running in production via software composition analysis (SCA).

"A lot of organizations don't do this yet," Kovar notes. "Thanks to the attention to supply chain attacks, customers are going to begin demanding SBOMs from their vendors, and it will quickly become standard."

4. Use automation to enhance human analysts.

If we're never going to have enough humans on the team, the solution is to just automate everything, right? Kovar warns that automation can create as many human headaches as it solves.

"Analysts being overwhelmed, and then burned out, is a difficult challenge, and in one sense, automation can make it worse," he says. "The more disparate tools you give someone, the more things they have to do, the more they have to keep up with. That doesn't necessarily help with burnout."

So automate with the intention of liberating your human analysts to do their job better. That can mean fewer tools, not more. It can mean a platform approach that makes it easier for analysts to not only keep up with their tools, but take action on significant events, while the basic stuff is remediated at machine speed. The result should be less sense of being overwhelmed — and less burnout.

"Security people got into the business to solve problems," Kovar says, "not to fill out spreadsheets."

5. Take DevSecOps forward.

To the 23% of respondents who haven't gotten around to DevSecOps yet, we say, "Don't delay." To the 2% who aren't even thinking about it, we really urge you to do some reading on the topic. For the vast majority who are already making strides: Keep going.

Our research found that 75% of organizations are using DevSecOps to identify and fix vulnerabilities and to remediate malware prior to deployment, as well as logging code changes for audit and applying runtime API security controls. Add it up, and DevSecOps is helping organizations solve visibility challenges (and keep bad software out of production). Classic DevSecOps benefits.

The next step, Kovar says, is to apply DevSecOps specifically to defending against ransomware and advanced persistent threats. "A DevSecOps approach helps you consolidate your network defenses to remove inefficiencies," he says. "It's an important step, because adversaries are increasingly combining attack techniques in a way that better exploits our coverage gaps or inefficiencies."

And make sure that your DevSecOps approach covers all software development, not just the official engineering team's work. "These days, everyone is developing software," he says. "People don't necessarily realize that someone in a Fortune 50 company using Microsoft VBA [Visual Basic for Applications] in Excel might be generating more revenue alone than whole companies at the bottom of the Fortune 1000."

6. Consolidate sprawling tool sets.

You need the right tool for the right job, as pretty much everyone's grandfather would say. But a piece of software isn't just a tool waiting in a box. It's an active application that requires monitoring to be effective, a degree of care from which we distill feedback. In that sense, it's more like a pet, and there are only so many of those you can have running around your house before you're mired in chaos. And poop.

Consolidation is about having the right tools for the right jobs, while also making sure that your team can manage the responsibility of care. As with haphazard automation, careless tool consolidation can increase frustration and burnout. Focusing on the necessary set of tools, particularly with a platform approach that can gather multiple inputs on one dashboard, empowers your analysts with information, rather than burdens them with the busywork of checking a million outputs. In the long run, organizations save on maintenance, training and licensing costs, and can put that savings to better uses. At the same time, a smart tool set improves visibility into infrastructure, application performance and security posture.

Industry highlights

Standout data points from seven select industries worldwide.

Communications and media

Communications and media organizations suffer from more frequent downtime than other industries: 33% of respondents say their organization suffers from weekly outages of critical applications tied to actions by bad actors versus a 22% average among other industries.

Nearly half — 46% — of communications and media companies attribute failure of projects or initiatives at their organizations in the past 12 months to skills gaps/shortages, compared to the cross-industry average of 34%.

CISOs are having outsized impact on supply-chain focus in communications companies. Of organizations that have taken action (new policies or investments) in this area as a result of attacks, 55% said these actions would not have taken place without the CISO leading the charge (versus 37% of respondents reporting the same in other industries).

On the cloud front, communication and media companies tend to be more diversified than in other industries. Only 18% work with a single public cloud infrastructure provider today (versus an average of 28% across other industries) and 41% work with three or more partners (versus 32).

Financial services

Financial services organizations surveyed tend to have larger SOCs than their peers: 27% report that their SOC consists of more than 50 full-time equivalents (versus 16%, on average, across other industries).

Possibly related: Financial services orgs were significantly less likely to report that daily attacks keep them from refining tools and processes (19% versus 29% on average for other industries) or to list finding enough talent to handle the workload as their top challenge (21% versus 30%).

Financial services organizations take a cloud-friendly tack when it comes to new application deployments; 50% report that they have a cloud-first policy when it comes to new applications compared to 38% of organizations in other industries.

Financial organizations are also ahead of their peers in the adoption of DevSecOps practices, with 84% reporting that these approaches are in place either extensively or in a limited fashion (versus 73% of respondents in other industries).

Healthcare and life sciences

Healthcare organizations are more cloud reliant: 81% say that they run most of their important applications on cloud infrastructure versus 64% of respondents in other verticals.

More healthcare organizations that say keeping up with cybersecurity requirements (i.e., deploying/tuning controls, monitoring network behavior, following threat intelligence, etc.) is much more difficult today than it was two years ago (46% versus an average of 25% across other industries).

Cloud challenges: 37% of healthcare orgs (versus 26% across other industries) said that moving workloads to the public cloud has made it more difficult to monitor the attack surface; 33% (versus only 18% across other industries) say that their security tools don't effectively support the move to cloud.

Data breaches were reported to be the most common among healthcare companies: 58% reported that their organization had encountered one or more recent breaches versus 37% of respondents in other industries.

Manufacturing

Manufacturing companies surveyed tend to have smaller SOCs than their peers: 8% report that their SOC consists of more than 50 FTEs (versus a 20% average across other industries).

Manufacturers have seen fewer incidents and attacks in their environments in the recent past, including being less likely to have suffered from a data breach (39% versus 51% across other industries), an insider attack (32% versus 41%) and DDoS attacks (36% versus 46%).

Manufacturers appear to be taking a more reactive approach to software supply chain attacks. Only 20% report an increase in the meetings between the CISO and business executives as a result of these attacks (versus 29% across other industries) and 19% report an uptick in threat hunting activity (versus 26%).

In a similar vein, manufacturers also conduct less-frequent third-party risk assessments, such as auditing partners, requesting vendors complete security questionnaires or reviewing penetration test results.

Public sector (Education and government agencies)

Only 33% of public sector organizations forecast a significant uptick in their cybersecurity investments over the next 12-24 months (versus 52% across other industries).

Analytics are catching on more slowly: 26% of public sector orgs say that security analytics play a much bigger role in our overall cybersecurity strategy than two years ago (versus 44% of respondents across other industries). However, 24% report that hiring one or several individuals with data science skills is a top priority over the next few years (significantly more than other industries, averaging 15%).

DevSecOps approaches have less momentum in the public sector, with just 24% reporting that they've shifted left extensively (versus 39% across other industries).

Public sector organizations also exhibit more cloud reticence than their peers: 45% report that the majority of critical applications currently run in the public cloud, a significantly lower number than the average of other industries (68%).

Retail

Retailers embrace cloud: 50% have a cloud-first policy for new applications compared to 38% of organizations across other verticals.

Another sign of cloud comfort: 31% of retailers report a full understanding of the security responsibility model across cloud types, well above the 21% average across other industries.

Retailers are apparently more likely to pay off ransomware attackers. Of those that experienced such an attack, 51% paid the ransom directly (versus 37% of their peers).

Retailers surveyed tend to have smaller SOCs than their peers: 8% report that their SOC consists of more than 50 FTEs (versus 20% of SOCs across industries). Also, 33% say the cybersecurity team being understaffed for the size of their organization is a top challenge (versus 25% across other industries).

Technology

Tech companies tended to have larger SOCs than their peers: 28% report that their SOC consists of more than 50 FTEs (versus 15% of SOCs, on average, across other industries).

Tech companies lead on multicloud adoption: 42% partner with three or more public cloud infrastructure providers today (versus a 29% cross-industry average), and 67% expect to do so in 24 months (versus 52% of their counterparts in other industries).

Tech companies have seen more malicious activity than their peers: 57% report successful phishing attacks (versus 45% across other industries); 44% have seen account takeover attacks (versus 35%), and 49% have uncovered fraudulent websites posing as their brand (versus 38%).

When it comes to skill gaps, tech companies are more apt to see the promise of data to cross the chasm: 54% say that better capture and analysis of security data is among the most promising ways to overcome near-term staffing challenges.

Country highlights

Standout data points from 10 countries worldwide.

Australia and New Zealand

Respondents across Australia and New Zealand reported fewer attacks in the previous 24 months than in other nations, including: a data breach (35% versus 49% of organizations in other countries), business email compromise (33% versus 52%) and successful phishing attacks (33% versus 48%).

Orgs in Australia and New Zealand experience longer downtime tied to security incidents. Only 57% say that their typical MTTR is measured in hours or less versus 75% of respondents in other countries.

Only 72% of respondents in Australia and New Zealand report an uptick in difficulty versus 86% of their peers globally. Less stress may be why only 22% report that they've considered leaving their job due to the stress associated with staff/skill shortages, compared to 38% of respondents in other countries.

Australia and New Zealand are less bullish about the promise of AI and ML in security automation. Only 15% — versus 36% across other countries — strongly agree that security operations center activities (e.g., threat detection, investigation and response) at their organization will be automated, with little to no human administrator intervention, in the next three years.

Canada

Respondents in Canada report that their organizations are increasing their investment in cybersecurity at a slower rate than their counterparts globally. While 37% of respondents say that their organization will increase investments significantly in the next 12-24 months, 52% of their peers in other countries say the same.

In Canada only 26% of respondents say their CISO is under extreme pressure to develop their ability to use data to identify patterns to optimize security operations, versus 40% of respondents in other countries report.

Organizations in Canada are not as far along on security analytics. While 38% of respondents outside of Canada have extensively deployed technologies designed for security analytics and operations automation and orchestration, only 18% of orgs in Canada have done so.

Respondents in Canada report an average of 56% of their company's employees currently work remote versus the 46% reported by their peers globally.

France

French orgs have a lower level of current cloud infrastructure reliance; 41% report that their organization runs most of its important applications on cloud infrastructure — versus 68% of respondents in other countries.

When it comes to downtime, French respondents report that their organizations are more resilient. Only 3% reported outages to apps tied to security incidents on a weekly basis versus 23% of their peers globally.

French respondents were also significantly less likely than their peers to report a number of disruptive outcomes tied to recent security incidents had been experienced, including disruption of business processes (29% versus 45%) and allocating a significant amount of IT/security staff time to remediation (38% versus 60%).

Respondents in France expect slower multicloud adoption. Only 12% expect their org to leverage four or more public cloud providers two years from now, less than half of the average (25%) for other countries.

Germany

An odd juxtaposition: A higher-than-average number of German respondents (48% versus 38% across the rest of the world) say their organization has a cloud-first policy for new applications. Yet Germany also stands out for on-prem-first policies, with 27% versus 19% of other countries surveyed.

When asked about their biggest public cloud security challenges, 35% reported that "meeting prescribed best practices for the configuration of cloud workloads and services" was on the shortlist compared to 26% of their peers globally.

German orgs' struggle to recruit and retain security talent was on par with other countries, but they more often reported that these challenges had caused multiple project delays in the past 12 months (53% versus 43% across other countries).

Germans are betting on automation to solve the talent crisis. They're more apt to say that automation holds the most promise in the next 12-24 months than other countries (63% versus 50% elsewhere). And they're less likely to say outsourcing to managed security service providers holds promise (32% versus 43% in the rest of the world).

India

Indian respondents report that only 33% of their organizations' employees are currently working remotely, significantly lower than the average in the rest of the world (49%).

Among Indian organizations that have ramped up the number of remote workers since before the pandemic, 70% report that they've seen a significant uptick in attempted attacks on these individuals (versus 21% globally) and 35% report challenges securing tools purchased to assist in the transition to remote work (versus 21% globally).

Indian organizations are aggressively integrating non-security analytics (such as IT operations, business and risk management analytics) with security analytics to improve decision-making: 77% report significant integration versus 37% across other countries.

Similarly, Indian orgs are on the leading edge when it comes to adopting security controls with machine learning capabilities: 72% report extensive adoption versus 28% of their peers in the rest of the world.

Ninety percent of respondents in India say that their organization will increase investments significantly in the next 12-24 months versus just 45% of their peers across the globe.

Japan

Japanese organizations are less reliant on cloud infrastructure than the rest of the world; 53% report that their organization runs most of their important applications on cloud infrastructure versus 67% of respondents in other countries.

When speaking broadly about their organizations' biggest security problems, Japanese respondents more often report issues keeping up with the number of new devices and device types being added to their environments (43% versus 25% in the rest of the world) and issues with their alerts lacking sufficient context, which makes investigations challenging and time-consuming (38% versus 23%).

Respondents in Japan were significantly less likely than their peers across the globe to report having experienced several types of security incidents in the prior 24 months, including: a data breach (20% versus 51% of orgs outside of Japan), regulatory violations (23% versus 41%), and insider attacks (18% versus 41%).

Japanese organizations have been more conservative in their adoption of DevSecOps approaches: 22% of respondents in the country report extensive adoption by their organization versus 39% globally.

Singapore

Organizations in Singapore are more tentative in their approach to the cloud. While 40% of their peers globally have a cloud-first policy, just 22% of respondents in Singapore do.

Organizations in Singapore were less likely to report that their organization had recently faced several cybersecurity incidents such as: DDoS attacks (22% versus 45% in the rest of the world), fraudulent websites (24% versus 41%), and a software supply chain attack (16% versus 41%).

When it comes to downtime, Singapore-based respondents report that their organizations are more resilient. Only 2% reported outages to apps tied to security incidents on a weekly basis versus 22% of their peers globally. Singapore-based respondents more often report annual or less often downtime (33% versus 18% elsewhere).

Cybersecurity skills shortages appear to be particularly challenging in Singapore with 44% reporting challenges related to both hiring and retention (versus 22% of the peers globally reporting this to be the case).

United Kingdom

While the cybersecurity labor market in the UK looks no less challenging, respondents in this country are less likely to report that the resulting disruption has caused multiple projects to fail (26% versus 36% in the rest of the world) or be delayed (34% versus 45%) over the last 12 months.

Relevant software supply chain attacks have not made as big an impression on UK orgs. While 45% of respondents in the UK say that their organization is significantly more focused on such attacks today, the percentage in the rest of the world is notably higher (59%).

UK orgs are significantly less likely to report that the majority of their important applications run on cloud infrastructure (57% versus 67% of their peers globally), and these organizations are much more likely to consider on-premises and cloud locations equally for new application deployments (53% versus 39%).

That said, UK-based respondents were less likely to report that their existing security controls do not support cloud environments (9% versus 18% of their peers globally).

United States

63% of U.S. organizations expect to use three or more public cloud infrastructure providers 24 months from now (versus 52% globally), and 70% report that the majority of their critical apps run in the cloud today (versus 64% globally).

U.S. orgs appear to have more sophisticated security controls: Just 16% report that their controls do not support the cloud effectively (versus 23% internationally), 22% report that they are bogged down in firefighting mode (versus 31%), and 15% say their controls can't protect them from modern threats (versus 21%).

U.S. orgs appear to suffer from more alert fatigue than their peers, with 30% saying keeping up with alerts is among their top challenges (versus 21%).

U.S. organizations see more promise for machine-learning-backed security analytics solutions to help identify cyber risks (34% versus 28% internationally) and improve threat detection (41% versus 35%).

Learn how Slack, REI, Aflac, Nasdaq and others use Splunk's data-centric security operations platform to deliver accurate threat detection, investigation and automated response across cloud, on-premises and hybrid environments.

Learn More

22-22513-Splunk-State of Security-EB-108

splunk>