


# 4 Lessons of Security Leaders for 2022





The past two years have been a challenge for security leaders. 2020 started with COVID-19 and a pell-mell shift to remote work, and finished with the gut-punch of a major breach ([SolarWinds](#)) 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.

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.

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 industry verticals with research firm Enterprise Strategy Group.

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?

- **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 security challenge driving security investment.

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.

Many security leaders told us they 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 the leaders' key recommendations for security priorities for 2022:

# 01

## 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: 1) Verify everyone and everything, 2) provide the least privileged access, 3) 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. Security information and event management (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.

# 02



## 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.

# 03

## 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 "video conferencing 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.



# 04

## 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 the last 2 years to advocate for the importance of integrated security thinking, at every stage of IT and the business.

After all, who knows what 2022 (and beyond) will hold.



For more insights on security trends and the best practices of security leaders globally, check out the free State of Security Report.

[Get Report](#)

