US SIGNAL

US SIGNAL 2022 SECURITY CENSUS

highlights and insights

TABLE OF CONTENTS

THE STATE OF IT SECURITY

Things aren't bad, but they could be better. That's how the majority of respondents to US Signal's 2022 Security Census view the state of their organizations' current IT security.

When queried about their satisfaction with their companies' IT security strategy and infrastructure, 60% selected one of these two responses: "I love it. When people ask, I'm happy to share our approach and why" or "It's not bad but if I had more resources, I'd definitely make some improvements." Another 10% chose "To be fair, I'm not really sure if I should be satisfied or not, everything seems to work."

That high level of satisfaction may seem contrary to the findings of many major industry research firms and consultancies. Their reports typically point out IT professionals' growing concerns and frustrations with staff shortages and talent gaps, shrinking budgets, pressure to move the needle on digital transformation, competing priorities, increasing cyber threats and the many other security-related issues they face.

The respondents to US Signal's survey deal with those same challenges. Is there something about their IT security strategies that is enabling them to overcome the issues and feel so comfortable, even confident, in their approaches?

Survey results provide a glimpse into what's on the minds of the participants — in this case, IT professionals — and offer general indicators for future actions or behaviors. However, they don't always tell the whole story. How questions and answer choices are worded can make a difference. So can the context in which they're viewed. Personal experiences, company and staff size, and other factors come into play as well.

As the results of US Signal's 2022 Security Census show, there are many reasons that respondents seem content with their current IT security approach. The survey also reveals why so many felt things could be much better. Before digging into the responses to all 14 survey questions, we'll use the next two sections to discuss why the respondents may have assessed their security strategies as they did.

BEHIND THE OPTIMISM

The US Signal customers and prospects participating in the 2022 Security Census may have good reason to be optimistic about their security approaches. For example, only 5% of them said they had experienced what was considered a major security incident over the past year. The other 95% likely feel confident in how well their IT security approach is working. ***(See Strategy Satisfaction.)***

In terms of compliance issues — typically a major concern and challenge for IT professionals, more than one third (35%) of the survey respondents stated they weren't subject to at least one of the seven primary compliance frameworks listed. If that's the case, that 35% isn't dealing with the ambiguities, costs, ramifications of potential non-compliance and other stressors associated with regulatory requirements and industry standards. ***(See Compliance Matters.)***

The majority of respondents (72%) also noted that the perceived importance of security by leadership and users has improved over the last year. That, too, may cause them to feel their security approach has support and, by extension, is working well. ***(See Security Improves Its Standing.)***

ROOM FOR IMPROVEMENT

Despite high levels of satisfaction with their security approach, many respondents acknowledged things could be better. While the perceived importance of security among leaders and employees is high, 45% of the respondents' organizations had no dedicated IT security professionals; 20% had only one.

That may have something to do with why 29% indicated that lack of employee bandwidth for security initiatives is the number one thing holding back their security programs. An insufficient budget to hire and retain knowledgeable staff was noted by 17%, while 21% listed the lack of funds to purchase the breadth or maturity of security needed.

Given the staffing issues, it's surprising that only 14% of respondents listed hiring staff as their most important budget priority for 2022. It ranked as the lowest priority for 37%.

Outsourcing to managed service providers also doesn't seem to be high on the list. On a scale of 1 to 7 with (1 being the highest priority and 7 being the lowest), outsourcing was ranked as the highest priority by only 4% of respondents; 54% ranked it as the least important. Only 43% of respondents said they're currently working with external service providers to augment their security programs, although 16% plan to do so.

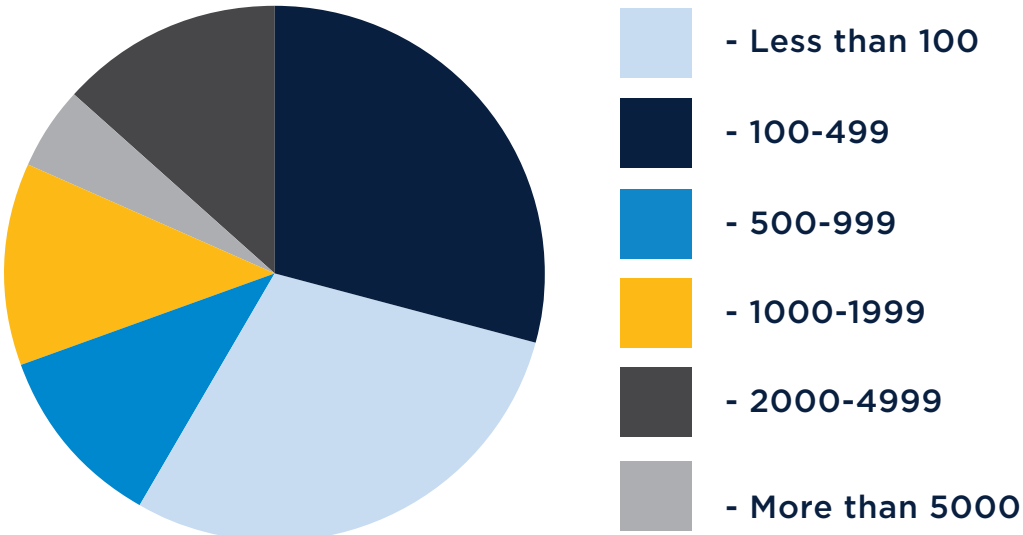
The takeaway: the respondents to the US Signal Census Survey may be fairly satisfied with their security approach, but they recognize it could be better with the right resources. The concern: they aren't taking advantage of what managed services providers and managed security services providers can do to help.

WHAT THE RESULTS SAY AND DON'T SAY

In the sections that follow, we look individually at the 14 questions contained in the survey, and discuss what the responses indicate at face value – and what considerations they raise or insights they reveal.

KNOW YOUR ENDPOINTS

Q1 As background info – how many user endpoints AND servers are in your environment?



By themselves, these numbers don't reveal much as they don't account for the number of locations where these endpoints reside, or company size and number of IT employees. The information may not matter anyway as there are so many factors that can affect staff workload issues, and there's no optional ratio of IT staff to endpoints. It's probably safe to say that companies with smaller IT staffs that are dealing with larger numbers of endpoints and multiple locations face more significant challenges than those with larger staffs and simpler operations.

One consideration arising from this question is whether the respondents had full knowledge of their IT environments. Research indicates that 30% of IT professionals may not have a firm grasp on how many endpoint devices their companies have. That percentage may be even higher now given the millions of US organizations forced to accommodate work-from-home operations in the last two years.

With more remote employees, devices constantly changing hands, and other issues, maintaining an accurate inventory of endpoints is challenging. Research from ***Tanium*** reveals that 71% of IT decision discover unknown endpoints within their IT environments weekly. More than half of the respondents in that survey (54%) pointed to IT solutions that are added without permission as their biggest challenge in maintaining control of their IT environments, while 40% claim a lack of endpoint visibility and control is one of the biggest barriers to maintaining compliance regulations.

That same research indicates that 57% of CIOs worldwide are concerned that a lack of visibility and endpoint control will make their organizations more susceptible to cyberattacks. Unpatched devices open doors for malicious actors. Even with a large IT staff and extensive resources, IT departments can't patch what they don't know they have.

LESS ISN'T MORE

Q2 How many IT staff does your organization have?

The US Signal survey included a question commonly found on IT-centric surveys. How many IT staff does your organization have? The more insightful, yet highly subjective, question may be, "Do you have enough IT staff to do what needs to be done within your organization?" Given the extensive IT shortages — and analysts predicting they won't be resolved any time soon, the answer to that question would likely be "no."

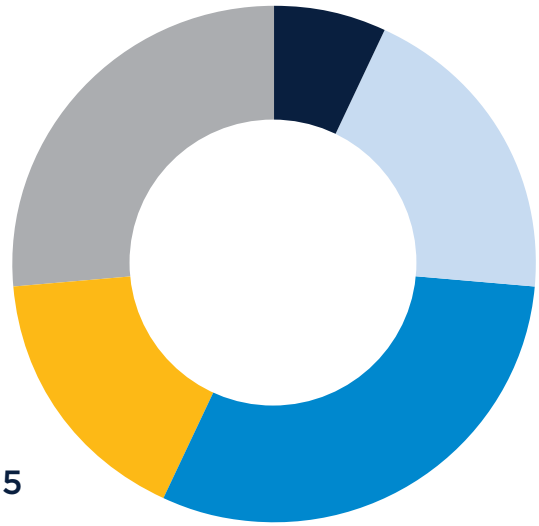
Without knowing company size, responsibilities, if managed services are used, and other factors, not much can be extrapolated from answers to the question of staff size. It's clear that most companies don't have extensive IT staffs. Only 19% of the respondents reported IT staffs of more than 25 people, while another 19% had one or less.

Other studies, as well as media reports, tell us that IT is continually told to do more with less – less budget in many cases, and almost always with less staff. Increased productivity can only do so much, so the low staff numbers raise flags concerning the ability of organizations to provide around-the-clock security, as well as day-to-day IT support. That's particularly true for those with less than five staff members. Unfortunately, there's not one-size-fits-all rule for IT staffing levels. Company size, types of positions needed, and other factors all play roles. One IT support company suggests using a general rule of thumb, at least for larger businesses, of one full-time IT employee per 75 to 125 users.

For less than 75 users, an organization may still want at least one IT support person on staff, but outsourcing is an option. Regardless of current staffing levels, companies of all sizes can ensure they have the right mix of IT skills and expertise by leveraging managed services, such as staff augmentation, managed security, and remote monitoring and management.

Even if organizations choose to activity recruit additional IT professionals, it may become more difficult to retain them. According to a survey from learning software firm ***TalentLMS and Workable***, 72% of US tech workers are considering quitting their jobs in the next 12 months.

5% of organizations have **zero** IT staff



HELP WANTED: SECURITY EXPERTISE

Q3 How many full-time security staff members does your organization have?

When asked the number of security professionals they have on staff, the majority of organizations represented in the 2022 US Signal Security Census results reported having only one or less. That isn't surprising for many reason but may be cause for concern.

Those percentages aren't surprising for many reasons, but they may be cause for concern. The most frequently cited ***reason for security lapses*** is that the number of people with appropriate expertise and experience who hold cybersecurity jobs is far below what's needed.

The skills of IT security professionals are critical for helping organizations protect sensitive data and systems safe against malicious hackers, defend an ever-expanding security perimeter, and comply with stringent regulatory requirements.

However, it's a massive undertaking building a security operations center — and not just because of the expense. The demand for skilled IT security talent, including cybersecurity, continues to exceed the supply of job candidates. There are approximately ***465,000 unfilled cyber jobs*** across the nation; various sources have reported that the cybersecurity industry has a ***0% unemployment rate***.

The shortage of IT professionals, in general, may also grow given trends that show more of these individuals choosing to leave the workforce. According to a ***Forrester survey***, 51% of cybersecurity professionals experienced extreme stress or burnout, with 65% saying they had considered leaving their job because it.

To overcome the issues, organizations must get creative with their recruiting efforts to find and cultivate top cybersecurity talent. Paid internships and mentoring of entry-level employees are both great ways to find talented workers early and teach them the skills needed to be successful in IT security. Both programs require giving participants real security-centric work experience, rather than relegating them to grunt work no one else wants to do.

Yet another option: managed security service providers. The big advantage they offer is that they invest in recruiting and retaining top talent because it's that talent that makes their business. They're better positioned to offer the latest security technologies and automation tools.

They also can provide 24/7/365 coverage. Security issues aren't confined to normal working hours, and cyber criminals often strike on major holidays. When issues do occur, time is of the essence. Data exfiltration can start within 30 minutes of an attack, total domain compromise can be achieved within 90 minutes, and ransomware of all systems in less than 20 hours.

45%

of organizations have **zero** full-time security staff

A LITTLE OUTSIDE HELP

Q4 How many security vendors are you using (i.e., MSPs, MDR services, equipment vendors, services companies, or VARs)?

Global spending on security products and services is slated to reach ***$174.7 billion by 2024***. Some of that spending is currently coming from respondents to the US Signal Security Census survey.

Only 22% aren't using security vendors, such as managed services providers, managed detection and response (MDR) services, equipment vendors, and value-added resellers (VARs). Meanwhile, 67% are using one to nine vendors and 11% are using more than 10.

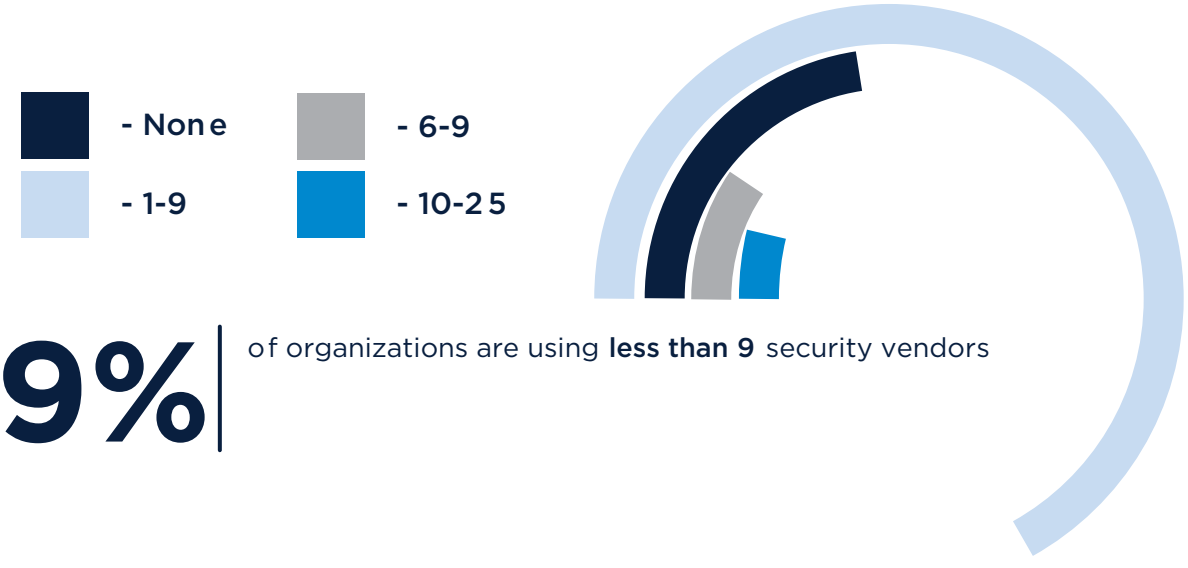
More vendors isn't always better, however. According to ***Cisco***, approximately 50% of the risk companies face is due to having multiple security vendors. In the ***2020 CISO Benchmark Report***, 81% of that survey's respondents reported that managing a multi-vendor environment is challenging.

Part of that may be due to lack of integration between security services and products. In the US Signal survey, 25% cited lack of simple interoperability and automation between security products as the biggest impediment to their security strategy while 19% ranked it second.

Another ***study*** noted that 83% of IT leaders with in-house security teams were now considering outsourcing their security efforts to a managed service provider; 45% were doing so due to a lack of strategic counsel from existing tools. The report's authors noted that they'd seen the phones of CIOs and CTOs light up with security alerts from their cybersecurity tools during meetings — but these security alerts usually offered no real solution to the problem flagged.

Two important observations from this. First, most organizations recognize they can benefit from working with third-party companies specializing in IT security services and products. The third-party companies that will excel and provide the most value are those that can offer more integrated services and provide actionable counsel on how to optimize the use of security tools and address threats.

Second, integration between tools and technologies, as well as with security teams and processes, is critical for driving efficiency and effectiveness, and eliminating repetitive tasks to free up resources for other activities.



89% of organizations are using **less than 9** security vendors

COMPLIANCE MATTERS

Q5 Does your organization fall under any of the following? Check all that apply. (PCI-DSS, HIPAA, DFARS, FedRAMP, SOC2, SOX, GDRP, Other, None of those listed)

As noted earlier, more than one third (35%) stated that their organizations didn't fall under at least one of the seven primary compliance frameworks listed. Only 13% selected "other," with respondents citing FERPA, GLBA and CJIS, among others. Compared to other studies, those percentages are low. One explanation could be that the respondents weren't aware of their organizations' compliance requirements.

Nonetheless, these numbers may help explain why when asked about plans for adding or improving security items, 34% of the respondents said they would be maintaining what that have for risk and compliance management and 41% only planned a small change.

We do know that few companies are exempt from regulatory requirements and industry standards, particularly related to data privacy and security. For example, any organization that accepts, processes, stores or transmits credit card information is subject to compliance with ***PCI-DSS***.

CCPA applies to all companies that serve California residents and have at least $25 million in annual revenue. Companies of any size that have personal data on at least 50,000 people or collect more than half their revenues from the sale of personal data also fall under the law. Companies don't have to be based in California or have a physical presence there to fall under the law.

Any business that wants to do contract work for the Department of Defense (DoD) and other federal agencies must comply with ***DFARS***. ***HIPAA*** specifically covers the healthcare industry, but it also affects any organization that deals with healthcare data. It includes employers and business associates who would have access to medical records for any reason. ***GDPR*** applies to any industry that collects, processes or stores personal data about European citizens or EU corporations and companies that offer goods or services in Europe.

It's important to note that IT weaknesses, such as the lack of endpoint visibility discussed earlier, carry compliance risks. Both the ***CCPA*** and the ***GDPR*** hold companies strictly accountable for the personal information they store and process. According to the ***Tanium*** study, as many as 67% of the respondents worried that poor IT hygiene threatens their ability to remain compliant with CCPA.

Even if companies currently aren't affected by compliance requirements, they likely will be at some point. ***Gartner*** expects 75% of the world's population to have data privacy protection because of legislation by 2023. The process that kicked off with EU's General Data Protection Regulation (GDPR) will only proliferate.

There are two considerations to note. First, compliance and security are related but aren't the same. Organizations can be fully compliant with a data privacy or security requirement but still not maintain a fully secure IT environment. Conversely, the most secure IT environments don't necessarily allow for checking all the boxes for compliance with any particular regulatory requirement.

Second, meeting compliance requirements can be time consuming and complex. According to one ***survey***, almost half (49%) the respondents said that ensuring compliance can be the most stressful part of their job. Nearly six in 10 (57%) predict that regulation will become more heterogenous and time-consuming in the years to come.

A privacy-driven technology market is emerging. Through 2022, privacy-driven spending on compliance tooling will rise to $8 billion worldwide. Over 40% of privacy compliance technology will rely on artificial intelligence (AI) by 2023, up from 5% today, according to ***Gartner***.

35% of organizations don't fall under any of the common compliance frameworks

- None
- PCI-DSS
- DFARS
- HIPAA
- Other
- SOC2
- GDRP
- FedRAM P
- SOX

SECURITY ISSUES HAPPEN

Q6 Has your organization experienced a major security incident in the past 12 months? (Major qualifying as a substantial monetary loss or impact to your ability to function as an organization.)

The Ponemon Institute reports that 68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. According to ***Statista***, 61% of SMBs experienced a data breach in 2021; 74% of large businesses did.

However, only 5% of the respondents to US Signal's survey said they had experienced what was considered a major security incident over the past year. Are they do something that the larger firms that fell prey to cyberattackers should have been doing? Were they truly spared from data breaches, or did they consider any incidences they experienced not to be "major?" Is a significant security incident waiting to happen?

Cliché as it sounds, IT security issues are not a matter of "if" but "when." Few organizations escape them, whether it's malware, ransomware, Distributed Denial of Service (DDoS), a phishing attack data breach, ransomware attack, SQL attack, zero-day exploit or something else. The ones hitting the big-name companies make the news, but that doesn't mean other organizations aren't experiencing them. They just may not be as devastating or something that these companies wish to share.

Without a common definition of "major security incident," it's difficult to say that the 95% of respondents to the US Signal survey should really be that confident in their current IT security strategies. In addition, given that many vulnerabilities exist layers deep in systems and software, there's the possibility that many breaches have not yet been discovered. Oftentimes, cybercriminals go undetected for long periods of time. Many use that time to get the proverbial "lay of the land" before attacking.

Another issue to keep in mind, it's not just their own IT security to be concerned about. Third-party risk can be a problem too. A survey by ***Accenture*** reported that successful breaches to organizations through the supply chain increased from 44% to 61%.

As vulnerabilities ***such as Log4j*** spread through the supply chain, more threats are expected to emerge. ***Gartner*** predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

of organizations experience a major security incident **5%**

SECURITY TECHNOLOGY FAVORITES

Q7 Rank the following technologies in terms of their importance to your security practice (0 being not in use, 1 being least important, 4 being most important)

①	Endpoint Detection		Email Protection	Next-Gen Firewall
②	System Hardening / General Security Hygiene		SIEM / Log Aggregator	Zero Trust
③	SIEM / Log Aggregator	DLP	CASB / SASE	SOAR / Automation

Endpoint detection, email protection and next-generation firewalls were deemed most important. Least important were security orchestration, automation and response (SOAR) and cloud access security broker (CASB)/secure access service edge (SASE). Those ratings were surprising given the growing market for both.

The SOAR market is expected to grow at a compound annual growth rate of 14.6% to reach ***$2,027.2 million by 2025***. ***Gartner*** expects investments in cloud access security broker (CASB) will see a 41% compound annual growth rate between 2018 and 2023. Although these technologies are increasingly considered security best practices, they may not have yet gained support due to their complexity and lack of maturity in the market.

Zero Trust also wasn't deemed highly important despite studies that show Zero-trust technologies are a ***top spending priority*** for CISOs in 2022. That's likely to change as the United States government issued an executive order in 2021 that requires U.S. federal agencies to move towards a zero-trust security posture. Other companies will follow.

The takeaway here is that survey respondents seem inclined to go with what they know works. The three leaders noted in the survey represent popular, well-vetted technologies for addressing some of the biggest IT security issues organizations face.

#1 Endpoint Detection

The Global Endpoint Detection and Response (EDR) Market was valued at ***$1.76 billion*** in 2020, and it is expected to reach $6.72 billion by 2026, registering a CAGR of 25.15% during the period of 2021-2026. Enterprises are increasingly adopting more decentralized and edge-based security techniques, due to an increasing number of data breaches worldwide. This is driving the demand for endpoint detection and response (EDR) solutions.

According to a ***study by the Ponemon Institute***, 68% of organizations experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. The same report noted that 68% of IT professionals found that the frequency of endpoint attacks had increased since the prior year.

While there are numerous EDR options available, many companies don't have the internal resources to manage them. However, an increasing number of vendors are now offering managed detection and response (MDR) solutions that remove the management burden.

#2 Email Protection

In 2020, the cloud-based email security market was valued at approximately ***$763 million*** U.S. dollars. It is expected to reach around 1.25 billion U.S. dollars by 2026. The need for email protection solutions is borne out by statistics such as these:

+ ***94%*** of malware is delivered via email Phishing attacks account for ***90%*** of data breaches
+ The FBI's Internet Crime Complaint Center (IC3) reported a total of ***19,369 complaints of Business email compromise (BEC)***, also known as email account compromise (EAC), in 2020. It was the costliest kind of cyber attack for that year, totaling $1.8 billion out of a reported total of $4.1 billion in cybercrime losses.
+ ***More than 90%*** of cyberattacks infiltrate an organization via email.
+ According to the FBI, there has been a ***400% increase*** year-over-year in phishing attacks.
+ ***IBM's 2021 Cost of a Data Breach Report*** found phishing to be the second most expensive attack vector while business email compromise (BEC) took first place, costing businesses an average of $5.01 million. A breach caused due to phishing costs organizations an average of $4.65 million.

For more comprehensive protection, it's typically recommended that organizations employ a combination of technologies and tools; incorporate email security best practices; and provide frequent employee training of email security.

#3 Next-Gen Firewalls (NGFW)

The next-generation firewall market is expected to reach ***$4.27 billion by 2023*** at a CAGR of 12.3% from 2017 to 2022. As cybercriminals become more adept at avoiding traditional firewalls, next-gen firewalls have become essential for stopping them and blocking threats like malware.

NGFWs are integrated network security platforms that consist of inline deep packet inspection firewalls, IPS, application inspection and control, SSL/SSH inspection, website filtering and quality of service (QoS)/bandwidth management. They're designed to protect networks against the latest in sophisticated network attacks and intrusions.

Look for NGFWs that can detect potential breaches and prevent further attacks like malware or SQL injections using techniques such as sandboxing, behavior analysis, URL filtering, and intrusion prevention systems (IPS).

They should be capable of detecting any threats that make it past your initial defenses, quickly stopping them before they can do any damage. In addition, they should be able to utilize the latest intelligence data to change itself over time.

If a breach happens, NGFWs should notify you within minutes or hours of the event. They should also prioritize which issues are alerted to you so you can react to top priority threats. Seek out NGFWs that will work seamlessly with and share crucial information with other security tools in your network. They should also be able to automate critical security tasks like identifying users and managing network policies.

SECURITY STRATEGY OBSTACLES

Q8 Rank what you feel holds your security strategy back the most (1 being the most important, 5 being the least important)

1. Lack of Employee Time
2. Lack of Simple Interoperability
3. Lack of Budget to Purchase Security Needed
4. Lack of Budget to Hire and Retain Staff
5. Too Confusing to Setup and Deploy

It's not too surprising the highest percentage of respondents (29%) cited lack of employee time/bandwidth to easily maintain and upgrade IT systems, and investigate alerts. One study noted that ***27%*** of enterprise security teams see more than ***one million*** alerts per day while 55% see in excess of 10,000 such alerts.

That's not to mention that just a decade ago, there were only 50 threat types to detect. Now there are more than one million. It doesn't help that attack methods are increasingly sophisticated.

With the growing number of intrusions, breaches, and outages, IT professionals find it increasingly difficult to detect, prevent, and respond to everything. Over the last year, the mean time to identify a data breach incident went from ***191 days to 197 days***. The average cost of a data breach has increased 6.4% to $3.86 million.

Given that vendor consolidation and building interoperability between products weren't high priorities for the respondents, it is somewhat surprising that 25% felt that the lack of simple interoperability and automation between products was the leading factor holding their security strategy back.

We would have expected limited budgets for hiring staff and purchasing the breadth and maturity of security products to be much higher. As the incidence of cyber attacks increase and budgets do as well, it's likely that more organizations will see the importance of beefing up both security staff and tools to advance their security strategies.

Here again, there's a strong case for using managed services. Doing so can free up staff time to devote to other endeavors, including security. The use of managed security services, in particular, can enable organizations to take advantage of more advanced information security practices, such forensic investigations and vulnerability management, that they wouldn't have time to do otherwise.

STRATEGY SATISFACTION

Q9 How satisfied are you with your current security strategy and infrastructure?

In the State of IT Security section, we noted that 60% of the respondents had a favorable opinion of what they're doing in terms of IT security — including 15% that "love" it and the 45% who said "It's not bad but…" However, it's important to point out that 68% expressed that there were insufficiencies (45% saying "…if I had more resources, I'd definitely make some improvements" and 23% selecting "It needs a lot of work but we do what we can with what we've got.")

Those that "love" their approach may be among the 95% that claim their organizations haven't experienced a major security event. Or they may include the 35% that don't have to deal with at least one of the seven major compliance frameworks listed in the US Signal survey. It also may help that the importance of IT security is increasing among company leaders and users.

However, most studies indicate that IT professionals aren't satisfied with the current security approaches. They know they could be doing more – and perhaps never enough. Other responses to questions in the US Signal survey have revealed that the lack of resources — staff and budget — for IT security are limiting security approaches for many organizations.

Many aren't in a position to invest in the latest technologies, and struggle just maintaining what they have. They also must deal with the security issues that can arise from shadow IT. Working with multiple security vendors is complex and time consuming. IT professionals often receive so many secure alerts that they have a hard time prioritizing and dealing with all of them.

The nature of IT security makes it difficult to develop, implement and maintain a perfect security strategy. However, there are a few things that can help beef up existing strategies. For example, offloading some day-to-day IT responsibilities to managed services providers could free up IT staffs to devote more time to their IT security strategies. Taking advantage of managed security services, such as remote monitoring and management, SOC as a Service, vulnerability management and managed detection and response (MDR) also can alleviate much of the burden of overseeing IT security. The use of managed security services also enables IT teams to take advantage of some of the latest security technologies that their own budgets couldn't accommodate.

WHAT MATTERS MOST

Q10 Rank your security investment priorities going into 2022(1 being the most important, 5 being the least important)

1. Upgrading / Expanding Existing Technology
2. Building Interoperability Between Products
3. Adding New Security Vendors to Fill Previous Gaps
4. Hiring More Staff
5. Migrating from On-Premise Devices to Virtual
6. Vendor Consolidation
7. Outsourcing to Partners to Handle Security

Upgrading and/or expanding existing technology to handle business growth and capacity requirements was deemed the most important investment priority by 64% who listed it as first or second.

That percentage is only slightly higher than the findings of ***study by Deloitte*** that reported the average IT department invests more than half (55%) of its technology budget on maintaining business operations and only 19% on building innovative new capabilities.

It was surprising that so little priority was given to adding new security vendors to fill previous gaps and business requirements (32% selected ranked it 1 or 2; 17% ranked it 6-7), outsourcing to partners to handle security (14% chose 1 or 2; 54% chose 6-7) and hiring more staff (25% chose 1 or 2; 52% chose 6-7).

Gartner forecasts that the IT services segment – which includes consulting and managed services – will have the second highest spending growth in 2022, reaching $1.3 trillion, up 7.9% from 2021. Business and technology consulting spending, specifically, is expected to grow 10% in 2022. Much of that will be on the security side.

Moving forward, vendor consolidation may rise in the rankings. By ***2024***, 30% of enterprises are expected to adopt cloud-delivered Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) and Firewall As a Service (FWaaS) capabilities from the same vendor. Security leaders often manage dozens of tools, but plan to consolidate to fewer than 10. That's in line with what 67% of the respondents in the US Signal survey said they're currently doing. As they adopt and implement more security tools, vendor consolidation will likely be a consideration.

WHAT'S CHANGING

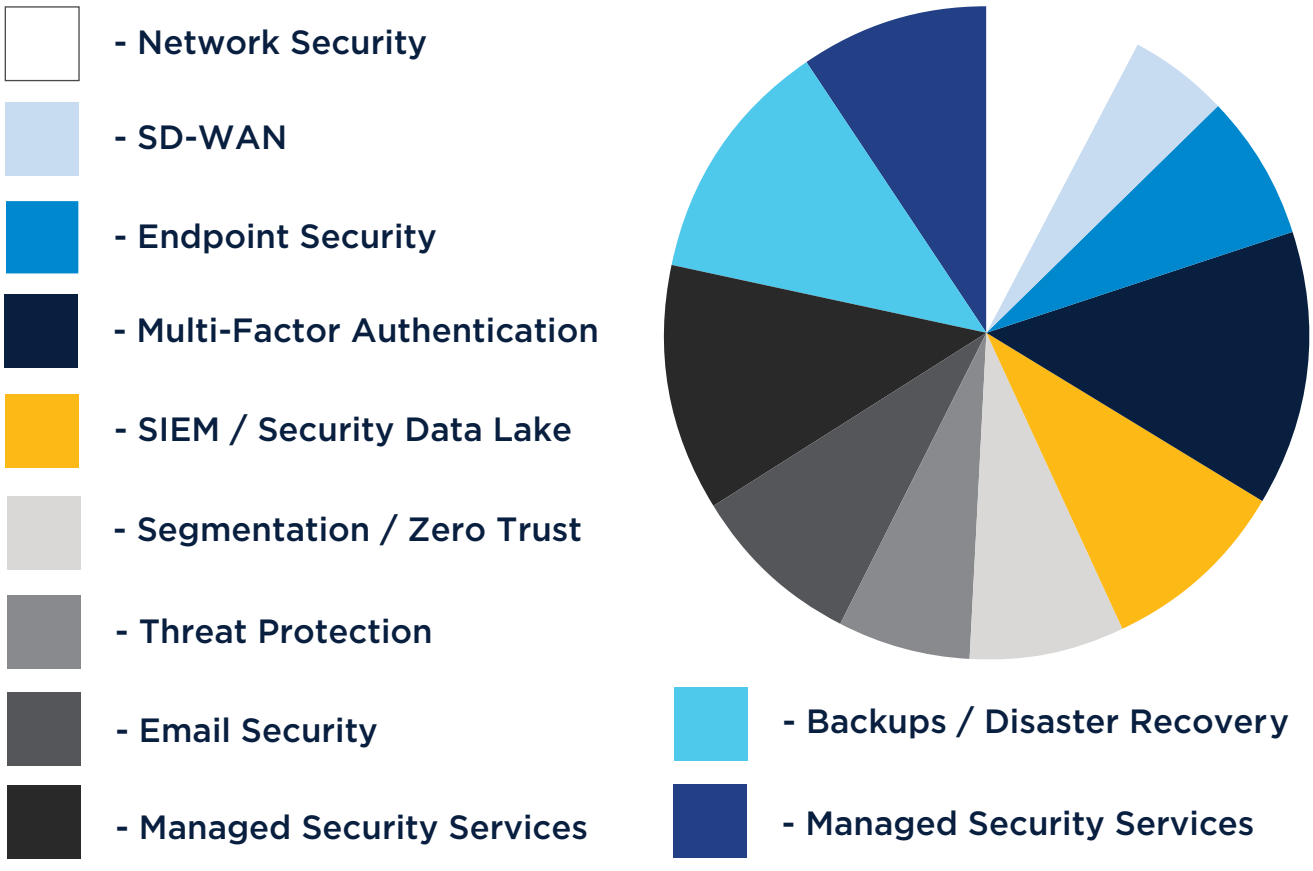
Q11 What security items are you looking to improve or add going into 2022? (If no 2022 investments, select No Change)

+ *Network Security*
+ *Endpoint Security (AV/EDR)*
+ *SIEM / Security Data Lake*
+ *Threat Protection (URL Filtering*
+ *E-Mail Security*
+ *Backups / Disaster Recovery*
+ *SD-WAN*
+ *Multi Factor Authentication*
+ *Segmentation / Zero Trust*
+ *DNS protection, Content filtering),*
+ *Managed Security Services*
+ *Risk and Compliance Management*

Survey respondents seem happy with most of the technologies and tools they consider most important to their security strategies.

In fact, not many of the respondents stated they'd be making major changes in time or investment for any of the security items listed in the survey. Multifactor authentication (MFA) was noted for "big" changes by the highest percentage of respondents – 19%. Backups/disaster recovery and managed security services each were expected to be the biggest areas of change by 17% each. Small changes were anticipated by 41% for risk and compliance, while 38% expected small changes for network security, such as firewalls.

The low response rate for change is likely due to budget constraints, since most of the respondents said their budgets are remaining steady. Low numbers of IT staff, particularly security professionals, may also play roles.



THE FATE OF THE IT SECURITY BUDGET

Q12 Do you foresee your 2022 security budget increasing, decreasing, including partner expenses?

Only 27% of the respondents in the US Signal survey see their 2022 security budgets increasing (by at least 25%), while 71% say they'll stay the same. Only 2% see their budgets decreasing by more than 25%.

In comparison, CSO's ***2021 Security Priorities Study*** found that 44% of security leaders expect their budgets to increase in the upcoming year, while 54% expect their budgets to remain the same. Like the US Signal survey results, only 2% said they're expecting a decrease.

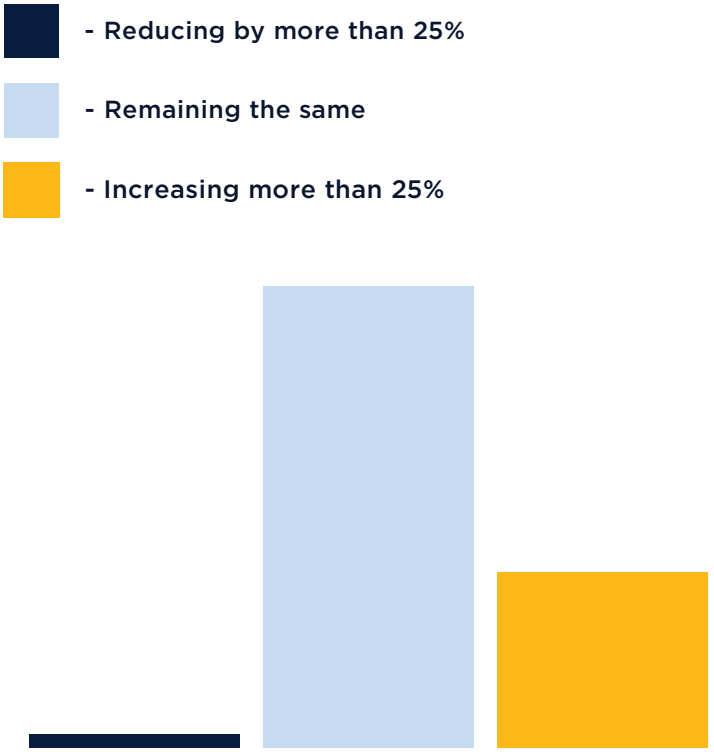
Meanwhile, ***Gartner*** estimated that spending on information security and risk management will total $172 billion in 2022, up from $155 billion in 2021 and $137 billion the year before.

In 2022, nearly $77 billion will go to security services, $30 billion to infrastructure protection, $19 billion to network security equipment, and $17 billion to identify and access management. Other areas with significant budgets include application security ($6.6 billion), integrated risk management ($6.4 billion), data security ($4 billion), software ($2.7 billion) and cloud security ($1.4 billion).

Other security leaders concur, saying they're investing in access and identity management software, authentication technologies such as role-based access control (RBAC), user behavior analytics, and micro segmentation to support their maturing ***zero trust*** architecture. They're also buying automation and analytics to deal with the vast scale of security data more effectively and efficiently, and they're engaging managed security services providers (MSSPs) to augment their own staff's efforts.

Security budget allocations, such as those for endpoint protection, are likely being influenced by the need to support remote workers. ***President Biden's May 2021 Executive Order*** to beef up the nation's cybersecurity may also be an influencing security budgets, as well as the growing list of country- and state-issued.

According to ***CSO's Security Priorities Study***, 49% of respondents said compliance, regulations, or mandates as influencing their budget decisions while 49% of respondents cited best practices. Those were followed by the need to address the evolving risks posed by changing workforce or business dynamics—notably hybrid and remote work (41%); addressing risks that result from digital transformation such as the move to the cloud (38%); responding to a security incident that happened in their own organization (35%); and responding to a security incident that happened in another organization (25%).



SECURITY IMPROVES ITS STANDING

Q13 How do you feel your leadership and users' perceptions of the importance of security has changed this past year?

As noted earlier, the majority of the US Signal survey respondents (72%) felt that the perceived importance of security by leadership and users has improved over the last year. That percentage was broken down by 28% who noted a noticeable improvement and 44% that said things have been better although security is still not a top priority. Another 21% felt there had been "no change but luckily it was not already bad."

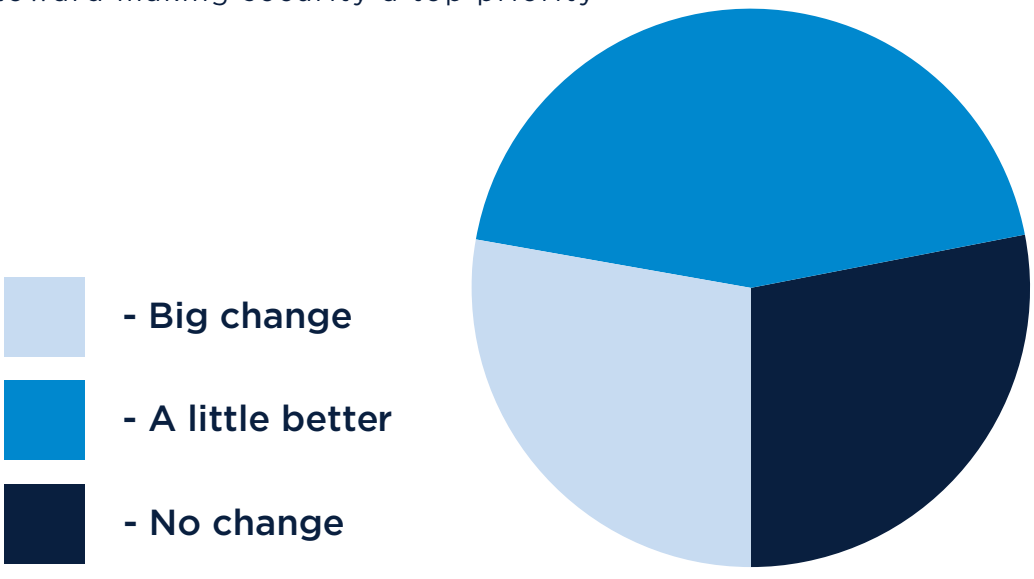
Increased understanding of the importance of IT security is something industry analysts and researchers are seeing as well. Part of that may be due to extensive media coverage of data breaches in recent years, as well as more focused security awareness and education at the C-suite level.

Growing awareness of IT security risks and solutions will have noticeable effects at the upper levels of many organizations. Gartner predicts that ***40% of company boards will have a dedicated cybersecurity committee by 2025*** — and that by ***2024, 75% of CEOs will be personally liable for cyber-physical security incidents***. It's crucial that executives are seen as advocates for security, and that their behaviors translate to all employees.

In addition, 70% of CEOs will mandate a culture of organizational resilience and security by ***2025*** to survive coincident threats from cybercrime, severe weather events, civil unrest and political instabilities. Building this culture from the ground up will take time and resources, but eventually, it will become a critical defense wall to protect employees and the overall company from the growing threat landscape.

It won't be easy. People tend to become oblivious to security threats. They understand the potential risks of certain behaviors but don't stop them. For example, in the ***Psychology of Passwords survey***, 91% of respondents knew the risks of repeatedly using the same password. Nonetheless, 66% continued doing it.

72% of organizations have made a change toward making security a top priority



STILL GOING IT ALONE

Q14 Do you currently use any external service providers to augment your security program such as a Managed Security Services Provider (MSSP), Managed Detection and Response provider (MDR), or Security Operations Center as a Service?

As has already been shown, many of the survey respondents face struggles in terms of budgeting for, recruiting and retaining IT security professionals. We know that lack of budget to purchase the breadth or maturity of security needed and to hire and retain knowledgeable staff is holding security strategies back. IT staff have insufficient time to easily maintain, upgrade, and investigate alerts.

So, it's surprising that 57% aren't currently using an external service provider to augment their security programs. Of the 43% that are, 11% aren't sure the value is there. Kudos, however, to the third-party companies working with the survey respondents who said "Yes, our provider is great!".

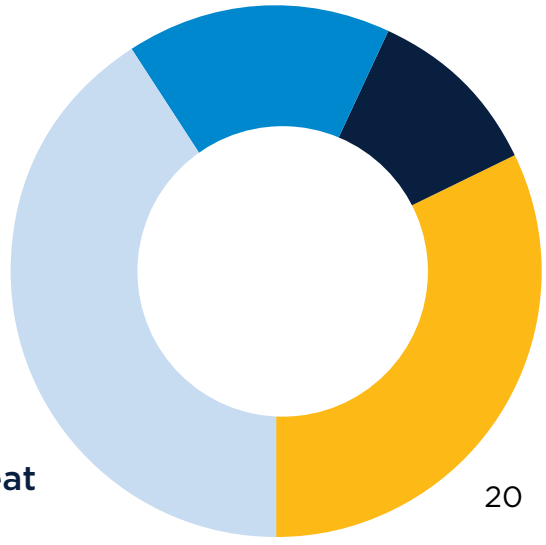
If industry trends are correct, opting to augment internal security will likely increase. According to Gartner, organizations are expected to invest ***$77 billion*** in outsourcing of security services in 2022, making it the largest area of cybersecurity spending across all categories. There are good reasons for them to do so.

There's a ***scarcity*** of cybersecurity talent available, and filling vacant positions on an organization's internal security team can be difficult and expensive. Partnering with a third-party company enables an organization to fill gaps within its internal security team or to replace it entirely.

Organizations also may require specialized cybersecurity expertise if a security incident occurs. Managed services providers have the scale required to retain this expertise in-house and make it available to their customers.

There's also the reality that some security functions can be difficult and time consuming to handle internally, not to mention the investments required. That includes network and endpoint monitoring, cloud monitoring, threat hunting, and vulnerability. Drawing upon managed services not only alleviates the burden; it allows organizations to take advantage of the latest technologies. And because security incidents can happen anytime, not just during an organization's standard business hours, a service provider can offer 24/7 continual detection and response to potential cyberattacks.

of organizations are using external service providers or plan to do so **59%**



- No
- Not currently
- Yes but not sold on it
- Yes our provider is great

THE WRAP UP

Surveys can only provide so much information, much of it dependent on the individual respondents' experiences and perspectives. When comparing the results to those of numerous other studies, some of the specific percentages may vary but the same challenges and potential solutions seem to affect everyone.

There are numerous options for dealing with IT security, including many emerging technologies. IT professionals shouldn't feel bad if their organizations aren't ready to invest in them. Simply focusing on the "basics" of IT security, consistently, can go a long way in helping ensure safer IT environments.

There are some trends that IT professionals should be taking note of, however. Addressing them will become increasing important and affect decisions on budget, investments, staffing, and the use of outside companies. For example, new platform approaches, such as extended detection and response (XDR), security service edge (SSE) and cloud-native application protection platforms (CNAPP), can reduce complexity and administration overhead, as well as increase effectiveness.

By 2024, ***Gartner*** predicts that 30% of enterprises will adopt cloud-delivered secure web gateway (SWG), cloud access security broker (CASB), zero-trust network access (ZTNA), and branch office firewall as a service (FWaaS) capabilities from the same vendor. Consolidating security functions will lower total cost of ownership, improve long-term operational efficiency and generate better overall security.

A cybersecurity mesh architecture (CSMA) can help provide a common, integrated security structure and posture to secure all assets, whether they're on-premises, in data centers or in the cloud. Gartner anticipates the adoption of ***mesh architecture*** will cut the cost of security incidents by 90% by 2024.

It's increasingly important to look beyond traditional approaches to security monitoring, detection and response to manage expanding surfaces. Also expect to see more threats emerging as vulnerabilities ***such as Log4j*** spread through the supply chain. ***Gartner*** says that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains. That's a three-fold increase from 2021. Digital supply chain risks, in particular, require new mitigation approaches that involve more defined vendor/partner segmentation, requests for evidence of security controls and best practices, and more.

Keep in mind that human error continues to play a major role in many security incidents, indicating that traditional approaches to security awareness training aren't working. It's time to start employing holistic security behavior and culture programs. These programs are meant to inspire new ways of thinking and embed new behaviors that can result in more secure ways of working.

METHODOLOGY

The US Signal 2022 Census was administered as a 14-question online survey to US Signal's email subscribers, which includes current and prospective customers across of wide range of industries, business sizes and at least 17 states. A total of 219 IT professionals responded although not to all questions.

Not all responses add up to 100% due to the nature of the some of the questions and the answer choices, and because percentages were rounded up or down as appropriate.

LINKS / RESOURCES

Know Your Endpoints
Research - http://logmeincdn.azureedge.net/lmimedia/central/resources/pdf/en/LogMeIn-Endpoint-Management-Whitepaper.pdf
Tanium - https://www.tanium.de/press-releases/tanium-study-over-90-percent-of-global-organizations-surveyed-have-major-gaps-in-it/

Less Isn't More
TalentLMS and Workable - https://www.talentlms.com/tech-employees-great-resignation-statistics

Help Wanted: Security Expertise
Reason for Security Lapses - https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html
465,000 Unfilled Cyber Jobs - https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/
0% Unemployment Role - https://www.monster.com/career-advice/article/tech-cybersecurity-zero-percent-unemployment-1016
Forrester Survey - https://www.forrester.com/report/predictions-2022-cybersecurity-risk-and-privacy/RES176406

A Little Outside Help
$174.7 Billion by 2024 - https://www.idc.com/getdoc.jsp?containerId=prAP47619121
Cisco - https://blogs.cisco.com/security/when-it-comes-to-security-how-many-vendors-is-too-many
CISO Benchmark Report - https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html?CCID=cc000160&DTID=oblgcdc000651&OID=ebksc020457
Study - https://info.syntax.com/ebooks/3/syntax-it-trends-benchmark-report-2021

Compliance Matters
PCI-DSS - https://www.pcisecuritystandards.org/
CCPA - https://oag.ca.gov/privacy/ccpa
DFARS - https://www.federalregister.gov/defense-federal-acquisition-regulation-supplement-dfars-
HIPAA - https://www.hhs.gov/hipaa/index.html
GDPR - https://gdpr-info.eu/
Gartner - https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w
Survey - https://www.ey.com/en_us/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

Security Issues Happen
Ponemon Institute - https://www.morphisec.com/hubfs/2020 State of Endpoint Security Final.pdf
Statista - https://www.statista.com/statistics/1280029/companies-experiencing-data-breach-can-us/#:~:text=Share%20of%20companies%20experiencing%20a,U.S.%20and%20Canada%202020%2D2021&text=In%202021%2C%2074%20percent%20of,had%20experienced%20a%20data%20breach.
2021 Data Breach Report - https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/
Accenture - https://www.accenture.com/us-en/insights/security/invest-cyber-resilience
Such as Log4J - https://www.gartner.com/en/articles/what-security-leaders-need-to-know-and-do-about-the-log4j-vulnerability
Gartner - https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

Security Technology Favorites
$2,027.2 Million by 2025 - https://www.globenewswire.com/news-release/2021/10/26/2320799/0/en/Security-Orchestration-Automation-and-Response-SOAR-Market-to-Reach-USD-2-027-2-Million-by-2025-Report-by-Market-Research-Future-MRFR.html
Gartner - https://www.ciodive.com/news/gartner-security-risk-covid-strategy/585218/
Top Spending Priority - https://dynamicciso.com/by-embracing-emerging-security-strategies-like-zero-trust-and-improving-automation-tactics-cisos-are-looking-to-be-better-positioned-to-support-the-demands-of-a-new-hybrid-workforce-finds-dynamiccis/

Security Technology Favorites
$2,027.2 Million by 2025 - https://www.globenewswire.com/news-release/2021/10/26/2320799/0/en/Security-Orchestration-Automation-and-Response-SOAR-Market-to-Reach-USD-2-027-2-Million-by-2025-Report-by-Market-Research-Future-MRFR.html
Gartner - https://www.ciodive.com/news/gartner-security-risk-covid-strategy/585218/
Top Spending Priority - https://dynamicciso.com/by-embracing-emerging-security-strategies-like-zero-trust-and-improving-automation-tactics-cisos-are-looking-to-be-better-positioned-to-support-the-demands-of-a-new-hybrid-workforce-finds-dynamiccis/
Study by the Ponemon Institute - https://www.morphisec.com/hubfs/2020 State of Endpoint Security Final.pdf
Further Research - https://www.keepersecurity.com/en_GB/ponemon2020.

html?campaignid=386642075&adgroupid=1209463242065314&adid=&hsa_acc=2895762531&hsa_cam=11384568876&hsa_grp=1209463242065314&hsa_ad=&hsa_src=o&hsa_tgt=kwd-75591784808097:loc-188&hsa_kw=cybersecurity%20remote%20work&hsa_mt=p&hsa_net=adwords&hsa_ver=3&msclkid=b7070edce8e316a41c0e6ebfe6177bb7&utm_source=bing&utm_medium=cpc&utm_campaign=B2B%3A%20Search%20-%20Ponemon%20-%20EN%20-%20EMEA&utm_term=cybersecurity%20remote%20work&utm_content=Cyber%20Security%20Remote%20Work
94% - https://www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-dbir-2019
90% - https://www.verizon.com/business/en-gb/resources/reports/dbir/
19,369 Complaints of Business Email Compromise (BEC) - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
More Than 90% - https://www.graphus.ai/blog/91-of-cyber-attacks-come-by-way-of-phishing-know-the-different-types/
400% Increase - https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html
IBM's 2021 Cost of a Data Breach Report - https://d.docs.live.net/9b806f35f81f7490/Desktop/1094741_635584586460384_1156969747_o.jpg
$4.27 Billion by 2023 - https://www.marketsandmarkets.com/Market-Reports/next-generation-firewall-ngfw-market-32240698.html

Security Strategy Obstacles
27% - https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-fortianalyzer-security-architect.pdf
One Million - https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-fortianalyzer-security-architect.pdf
191 Days to 197 Days - https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-fortianalyzer-security-architect.pdf

What Matters Most
Study by Deloitte - https://www2.deloitte.com/us/en/insights/focus/cio-insider-business-insights/tech-finance-technology-investment-budgeting-processes.html/#endnote-4
Gartner - https://www.gartner.com/en/newsroom/press-releases/2022-01-18-gartner-forecasts-worldwide-it-spending-to-grow-five-point-1-percent-in-2022#:~:text=Gartner%20forecasts%20that%20the%20IT,to%20grow%2010%25%20in%202022.
2024 - https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022-1

The Fate of the IT Security Budget
Studies - https://swzd.com/resources/state-of-it/
53% - https://swzd.com/resources/state-of-it/
2021 Security Priorities Study - https://resources.idg.com/download/security-priorities-executive-summary
Studies - https://www.csoonline.com/article/3644457/security-priorities-for-2022-advancement-not-revolution.html
Gartner - https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html
Zero Trust - https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html
President Biden's May 2021 Executive Order - https://www.csoonline.com/article/3618730/biden-administration-releases-ambitious-cybersecurity-executive-order.html
CSO's Security Priorities Study - https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html

Security Improves It's Standing
40% of Company Boards will Have a Dedicated CyberSecurity Committee by 2025 - https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-
By 2024, 75% of CEOs will be Personally Liable for Cyber-Physical Security Incidents - https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl
2025 - https://d.docs.live.net/9b806f35f81f7490/Desktop/.HPIMAGE.VFS
Psychology of Passwords Survey - https://www.lastpass.com/resources/psychology-of-passwords-2020

Still Going It Alone
$77 Billion - https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html#tk.rss_identityandaccessmanagement
Found - https://f.hubspotusercontent40.net/hubfs/1624046/2021_Security Priorities Executive Summary_final.pdf
Scarcity - https://www.zdnet.com/article/the-cybersecurity-jobs-crisis-is-getting-worse-and-companies-are-making-basic-mistakes-with-hiring/

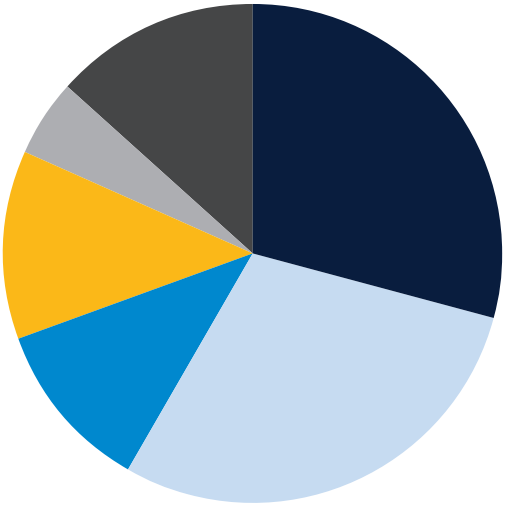
The Wrap Up
Gartner - https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022
Mesh Architecture - https://www.cybersecuritydive.com/news/security-risk-management-trends-gartner/608452/
Such as Log4J - https://www.gartner.com/en/articles/what-security-leaders-need-to-know-and-do-about-the-log4j-vulnerability
Gartner - https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

US SIGNAL®

US SIGNAL 2022 SECURITY CENSUS

highlights and insights

As background info — how many user endpoints AND servers are in your environment?

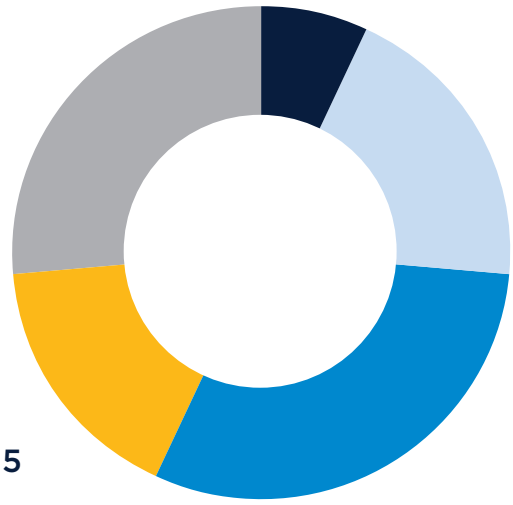


- Less than 100
- 100-499
- 500-999
- 1000-1999
- 2000-4999
- More than 5000

41% of organizations have 500 or more endpoints and servers

How many IT staff does your organization have?

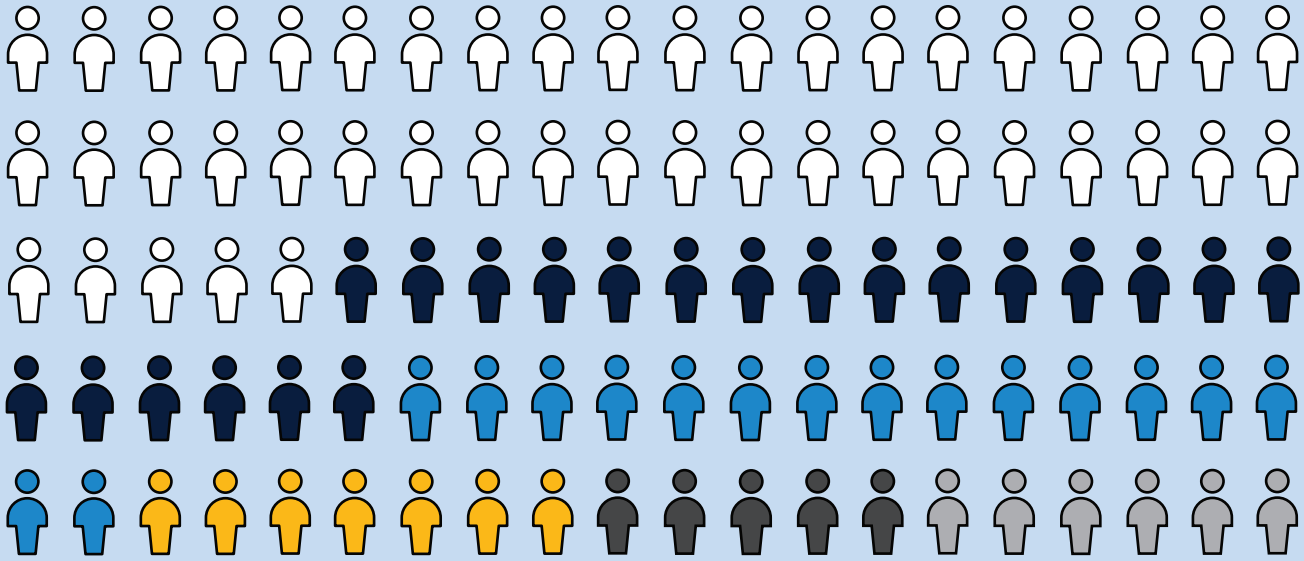
5% of organizations have **zero** IT staff



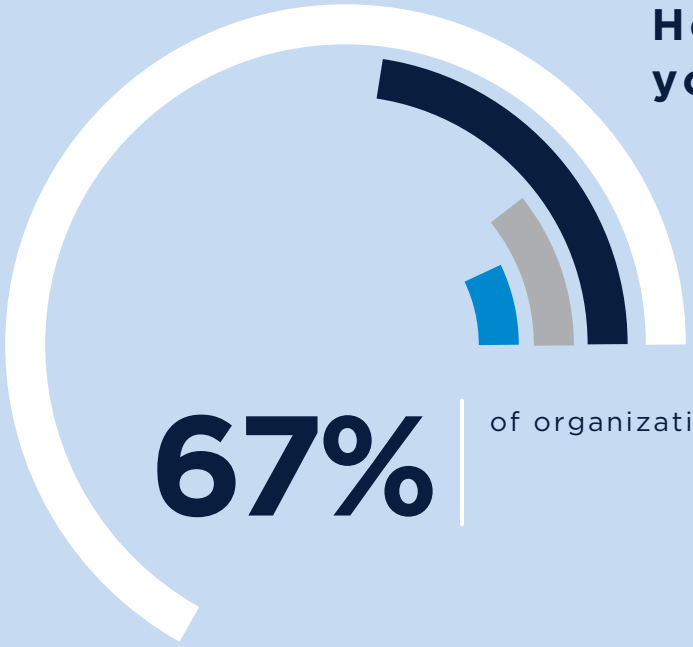
- None
- 2-5
- 6-9
- 10-25
- More than 25

How many full-time security staff does your organization have?

45% of organizations have **zero** full-time security staff



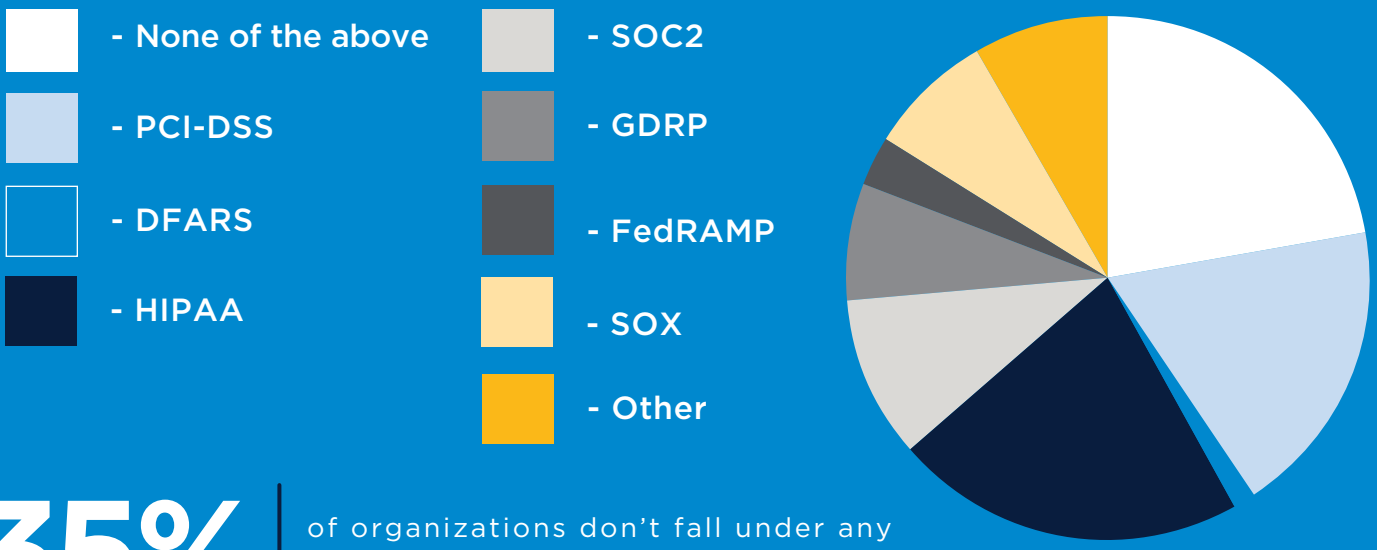
How many security vendors are you using?



- None
- 1-9
- 6-9
- 10-25

67% of organizations are using **less than 9** security vendors

Does your organization fall under any of the following compliance frameworks?



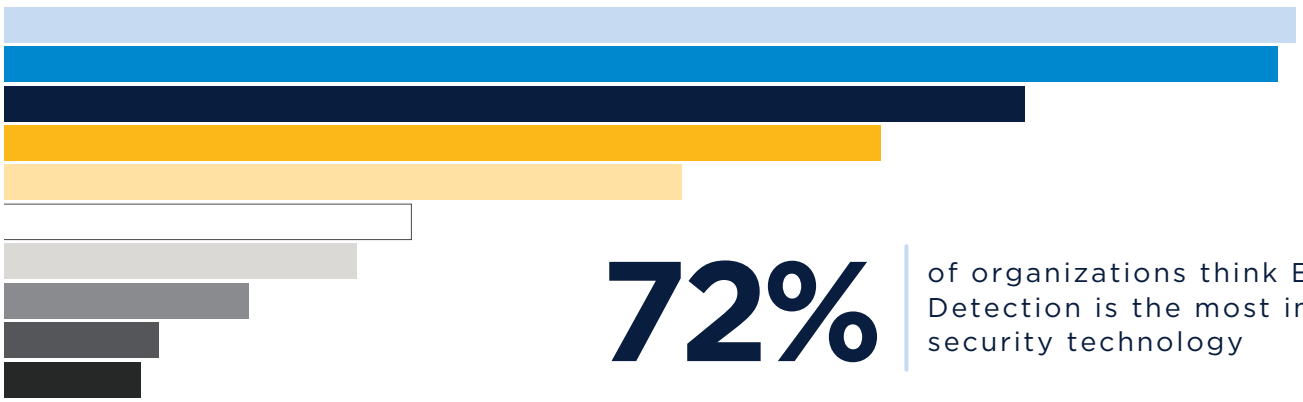
35% of organizations don't fall under any of the common compliance frameworks

Has your organization experienced a major security incident in the past 12 months?

- Yes
- No
- Unsure

5% of organizations experience a major security incident

Rank the following technologies in terms of their importance to your security practice?



72% of organizations think Endpoint Detection is the most important security technology

Note: Percentages do not add up to 100 as many respondents ranked more than one technology the same.

Rank what you feel holds your security strategy back the most?

29% of participants felt lack of employee time was most responsible for holding their security strategy back

- Lack of simple interoperability
- Lack of budget to purchase
- Too confusing to setup
- Lack of budget to hire staff
- Lack of employee time

How satisfied are you with your current strategy and infrastructure?

- Love it
- It's not bad
- It needs a lot
- Not sure
- Outsource
- Not my expertise

68% of organizations believe their security strategy needs improvement

What security items are you looking to improve or add going into 2022?

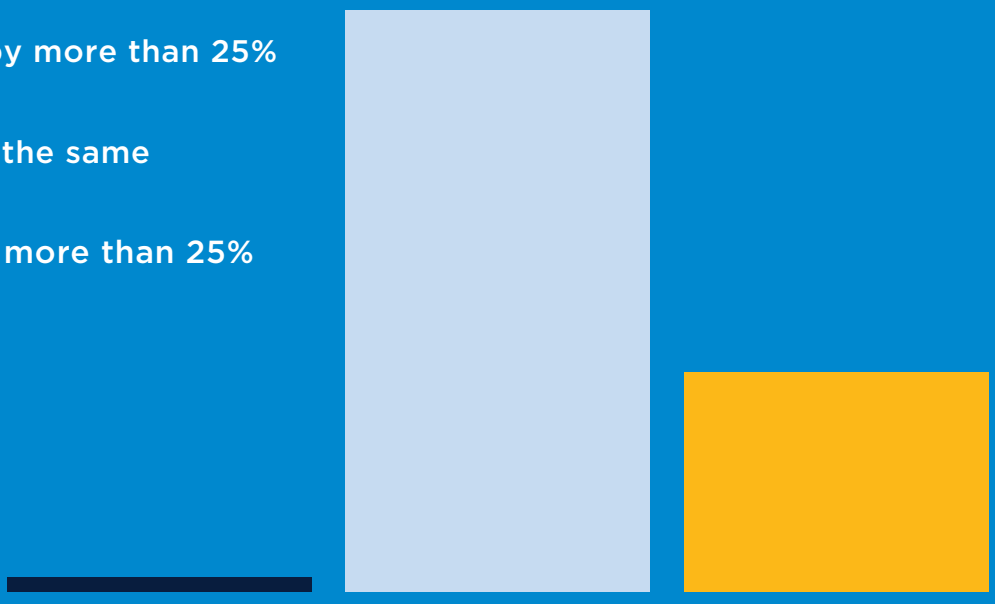
- Network Security
- SD-WAN
- Endpoint Security
- Multi-Factor Authentication
- SIEM / Security Data Lake
- Segmentation / Zero Trust
- Threat Protection
- Email Security
- Managed Security Services
- Backups / Disaster Recovery
- Managed Security Services

19%

of organizations will add or improve Multi-Factor Authentication

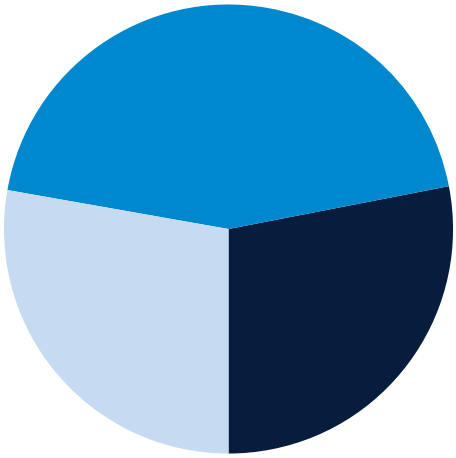
Do you foresee your 2022 security budget increasing, decreasing, or remaining the same including partner expenses?

- Reducing by more than 25%
- Remaining the same
- Increasing more than 25%



98% of organizations say their security budget will increase or remain the same in 2022

How do you feel your leadership and user's perception of the importance of security has changed in 2022?



- Big change
- A little better
- No change

72% of organizations have made a change toward making security a top priority

Do you currently use an external service providers to augment your security program?

59% of organizations are using external service providers or plan to do so

- No
- Not currently, but are planning to
- Yes but not sold on it
- Yes our provider is great

THE US SIGNAL ADVANTAGE

Strengthen the security of your data and applications while freeing up internal resources with US Signal.

Built using the latest technologies and security best practices, US Signal provides critical protection to mitigate threats, risks, and potential damage — all while meeting the unique demands of your business. They can even help you meet compliance requirements.

866.2.SIGNAL | info@ussignal.com | ussignal.com

US SIGNAL®