DOMAINTOOLS®

2021

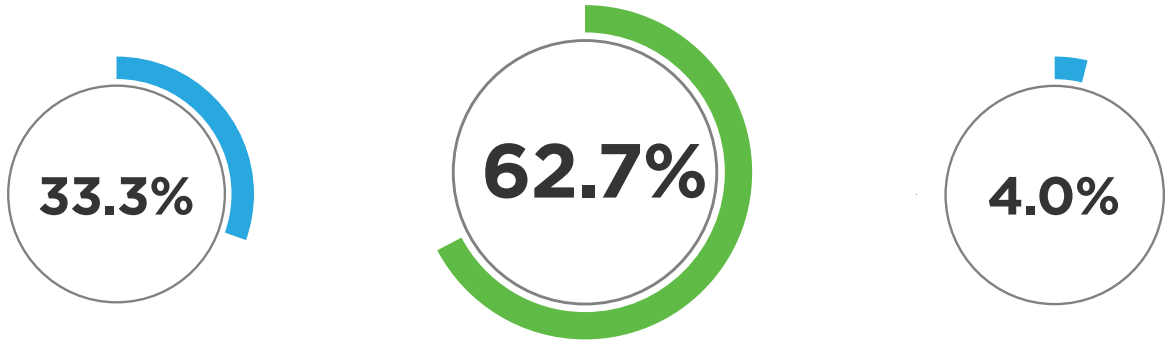
THE IMPACT OF THE SOLARWINDS BREACH ON CYBERSECURITY

The SolarWinds hack presented a cybersecurity reckoning for the US government and private enterprises. While the breadth and depth of the state-sponsored attacks are still being determined, one thing is certain: the fallout from the SolarWinds hack is going to get worse before it gets better.

From some of the most secure US government agencies to top tech companies, critical infrastructure such as energy and manufacturing, healthcare, universities, and more, CISOs at the executive level to threat hunters on the frontlines are living under a newly-minted set of rules; assume your network is compromised and figure out a path to move forward.

This survey aims to capture the effects of the SolarWinds incident felt by security researchers and analysts, threat hunters, IT managers, and those whose organizations join the collateral damage left in the wake of the biggest hack of the US government.

SolarWinds: A Wakeup Call for All; A Confidence Check for Most

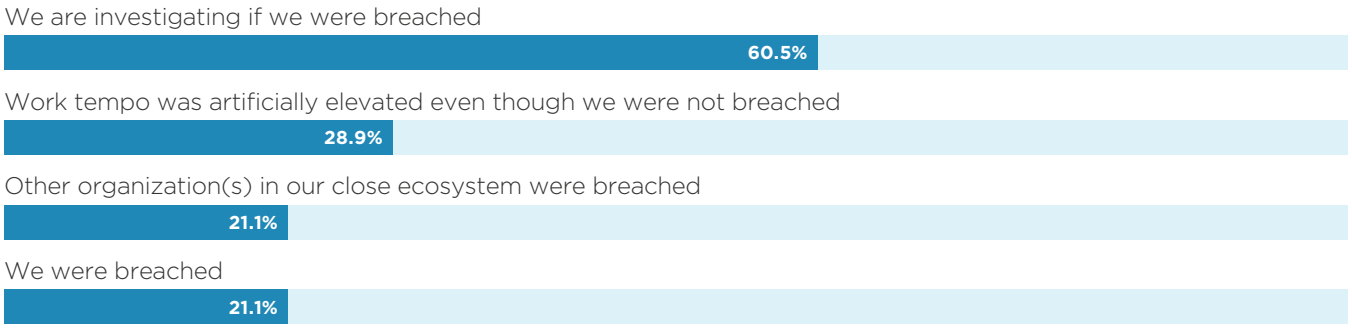


Slightly Concerned **Highly Concerned** **Not Concerned**

One out of five survey respondents' organizations (18.9%) were directly impacted by the SolarWinds event, and there was near-universal fear cast across the security practitioner landscape.

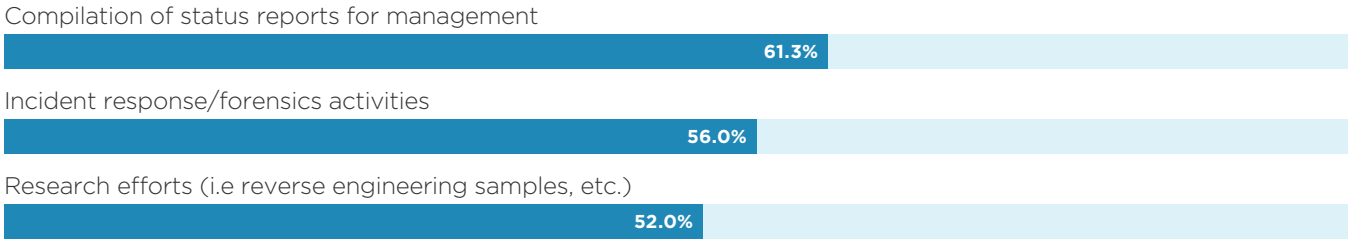
Ninety-six percent of respondents were either slightly concerned (33.3%) or highly concerned (62.7%). Only four percent stated they were not concerned at all. One might imagine those in the four percent roaring off into the sunset in a 1973 Buccaneer Red Trans Am blaring Bon Jovi's "It's My Life".

While the majority of organizations (64.7%) as a whole were not directly, and some (16.4%) still determining whether they were affected by SolarWinds, the one-fifth who were directly affected stated:



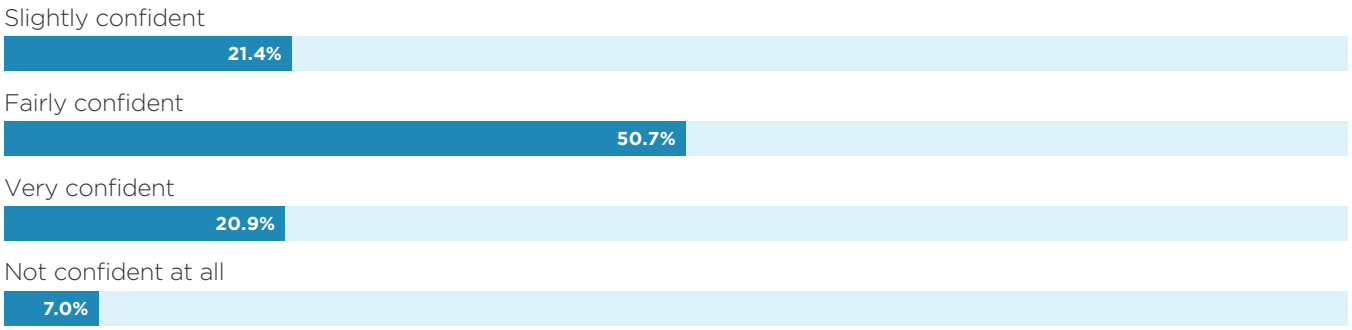
In a different line of questioning that separated the organization from the individual, Solarwinds was reported to have had a direct impact on the jobs of nearly 40 percent (37.5%) of respondents.

Top 3 Cybersecurity Job Impacts



Visibility is key to an organization's defensive success. When it came time to confront the fallout from SolarWinds and assess their organization's standing, an overwhelming majority expressed confidence in their visibility into security information or into internal processes, with 71.6 percent stating they are fairly to very confident. A small yet significant seven percent stated they had no confidence at all and for this group we might suggest Nathaniel Branden's 1994 pioneering work, "The Six Pillars of Self-Esteem".

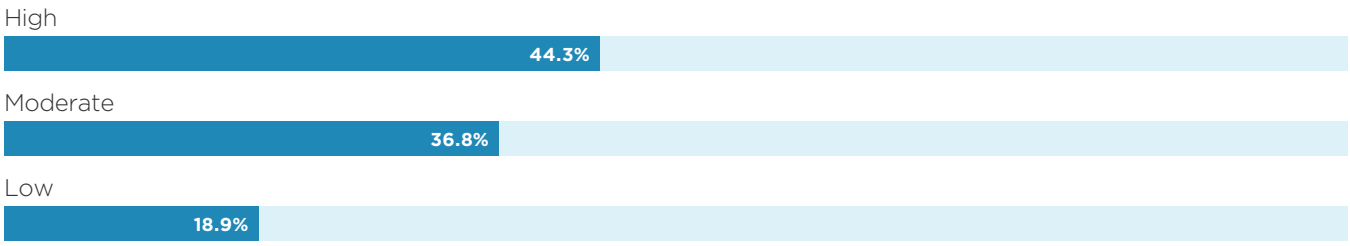
Confidence in Network Visibility



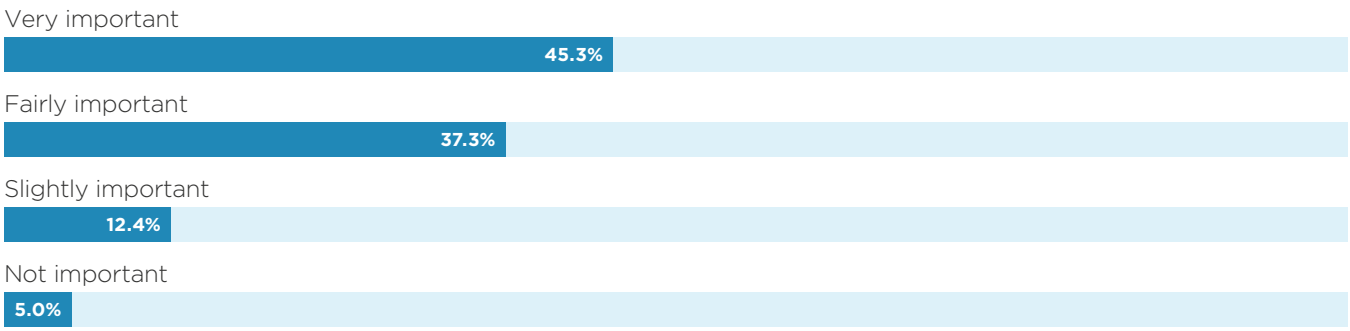
Views on Attacks Attributed to State-Sponsored Actors

Attribution, the security analyst's take on Abbott & Costello's 1942 mystery film, "Who Done It?" is often the immediate focus following every large-scale cyber-attack and data breach. However, not all security teams place attribution at the top of their list for post-attack analysis and response.

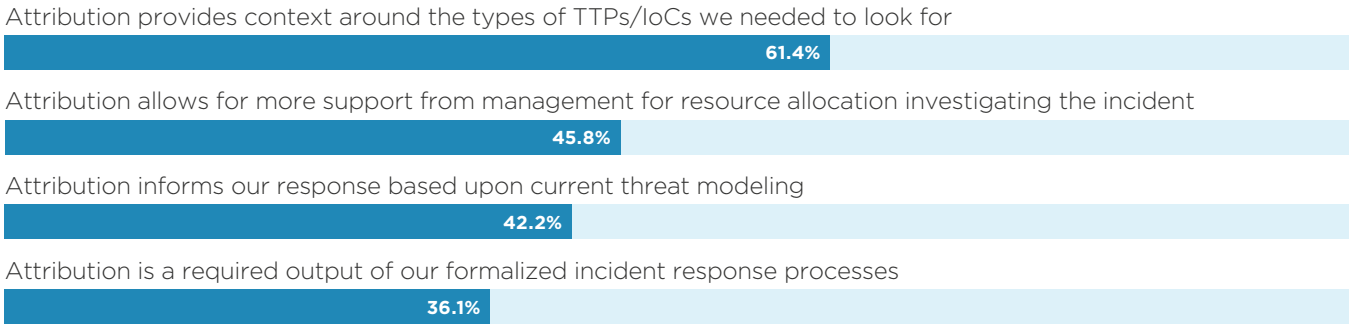
How much of an emphasis does your organization place on defending against state-sponsored attacks?



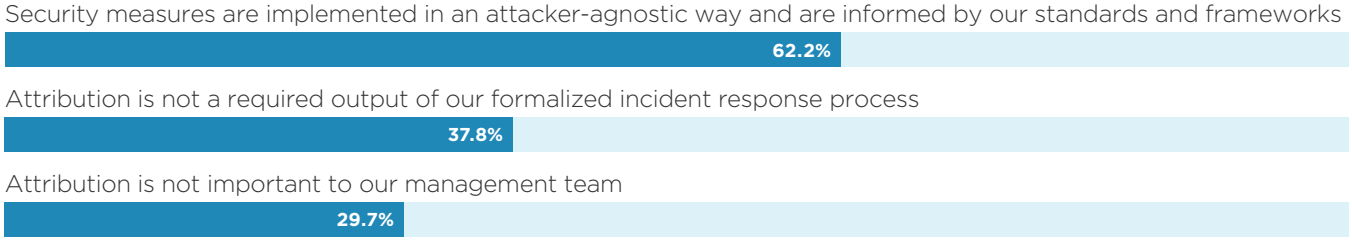
For the SolarWinds hack, how important of a role should attribution play in responding to this type of event?



Respondents state that when an attack is attributed to a specific actor, this has significance for them because:



Some respondents stated that attribution of attacks is not of great importance; their reasoning was:

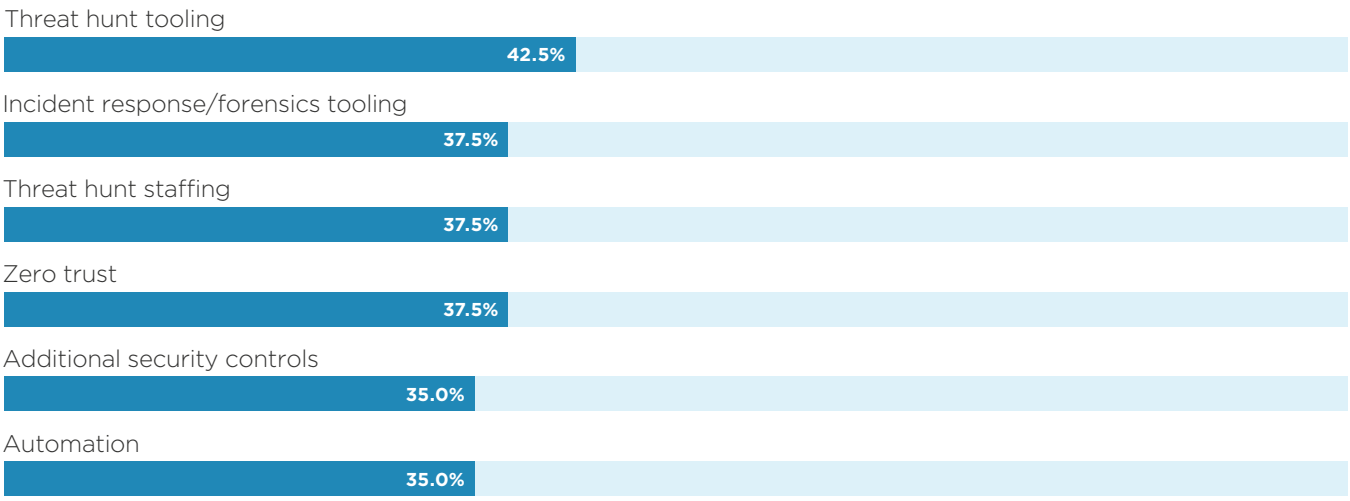


As a Result of the SolarWinds Event, Threat Hunting Continues to Gain a Foothold In Security Organizations

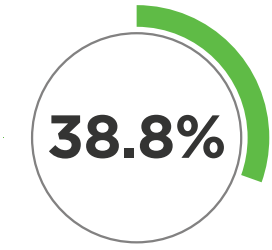
Organizations have slowly yet steadily reallocated resources and budget over the last five or six years to build proactive threat hunting teams to combat Advanced Persistent Threats (APTs) and enhance their incident response speed and accuracy. Threat hunting as a formalized practice within an existing cybersecurity team has been steadily making inroads towards becoming mainstream, and SolarWinds might be the event that puts it over the edge in industry validation.

Of the 20 percent of security organizations that will receive increases to their budget as a direct result of SolarWinds, threat hunting tooling is where the most additional resources will go to support.

What areas will the additional resources go to support?



Percentage of respondents that have a threat hunting team.



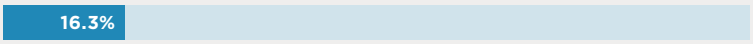
Percentage of respondents that do not have a threat hunting team.

For those organizations that already have a dedicated threat hunting team, the SolarWinds hack will impact the way those threat hunting teams operate in significant ways. Over half of teams (55.3%) will develop new hunting techniques targeting supply chain attacks and 51.2 percent plan to incorporate more threat hunting feeds into their SIEM/SOAR to remain vigilant of the latest attacks.

Tangible resources to better prepare against future attacks

Received a budget increase for supply chain incidents

Additional headcount allocated for threat hunting team



Eighteen percent (17.9%) have been given a budget increase to specifically concentrate on supply chain incidents and 16.3 percent have been allocated additional headcount for their threat hunting team.

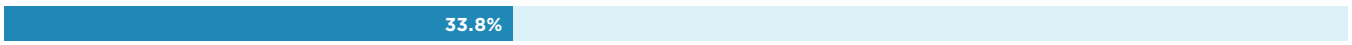
Nearly 20 percent of teams will receive real, tangible resources to better prepare themselves to defend against future attacks.

Of the nearly 40 percent (38.8%) of organizations that do not have a threat hunting team, the majority (66.2%) have no plans to add the capability at this time. However, in what could be considered a (don't say it) "solar win" (sigh…) one-third (33.8%) of them intend to raise the priority of staffing a threat hunting team.

Does the SolarWinds hack change threat hunting as a priority for your team?

No—we have no plans to add this capability at this time

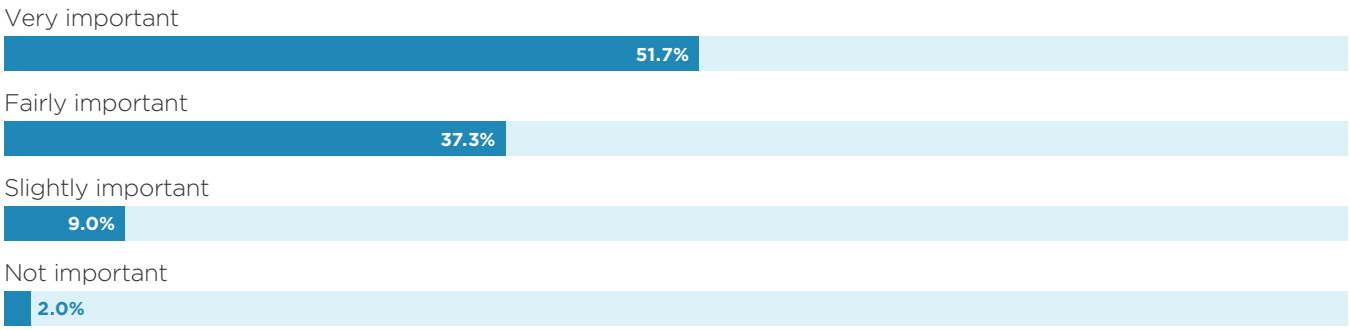
Yes—we intend to raise the priority of staffing a threat hunting team



As threat hunting's profile becomes more elevated, so will awareness of the essential role DNS data and domain-level intelligence serves in enabling threat hunting operations. The Internet's Domain Name System (DNS) is the underlying address book that maps human-readable names to machine-readable numbers. As a core fabric of the Internet's functionality, DNS is being leveraged by many research and security teams to detect and block malicious traffic.

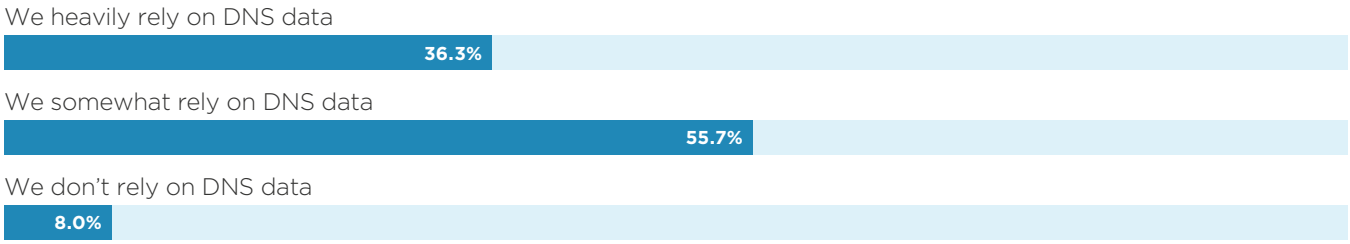
When asked to think about the infrastructure used by SolarWinds and then rate the importance of DNS and domain-level intelligence to their threat hunting capabilities, nearly all (89%) of respondents said it was fairly or very important.

Thinking about SolarWinds' infrastructure, how important is DNS and domain-level intelligence to your threat hunting capabilities?



However, when asked in general how heavily do you or your organization rely on DNS data in your threat hunting efforts, there was a significant drop in the number of respondents who heavily rely on DNS data in general (36.3%) and those who find DNS data very important (55.7%) for use in researching SolarWinds' infrastructure.

How heavily do you or your organization rely on DNS data in your threat hunting efforts?

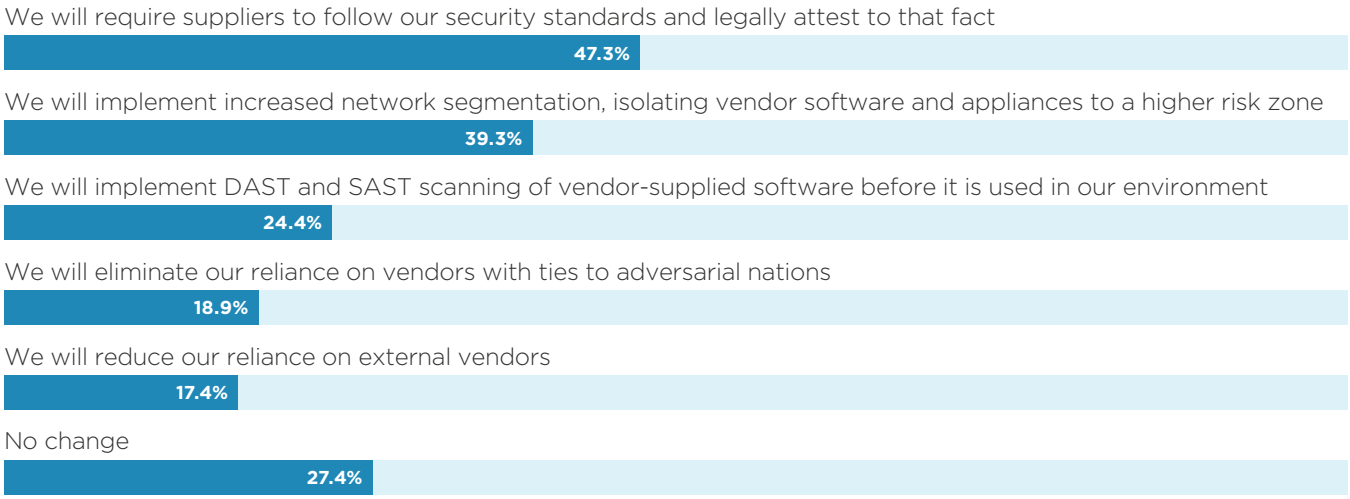


Significant Vendor Changes Following SolarWinds

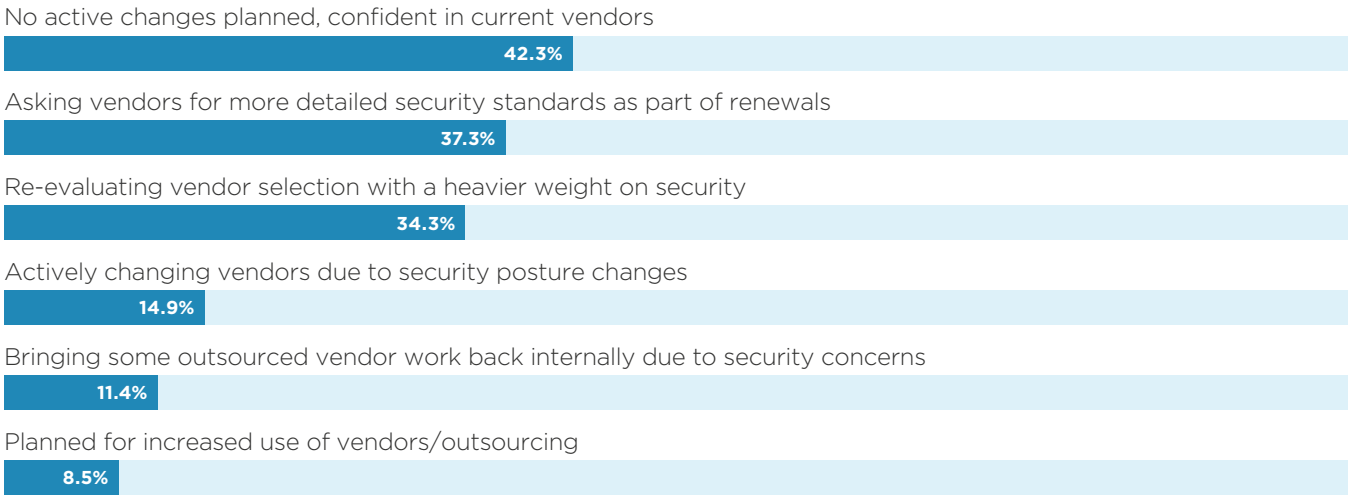
The SolarWinds attack has been the most public demonstration of supply chain attacks and their impact to date, but third-party risk has been an ongoing challenge for many years. There is no simple, single solution. Organizations at minimum should be properly evaluating third parties's cybersecurity programs in detail, assessing and auditing their SLAs, and performing regular ongoing network monitoring and analysis.

"We need to talk" are four words you never want to hear when you think your relationship is going well. SolarWinds has prompted many organizations to reevaluate their vendor relationships and will likely produce more "We need to talk" supply chain and vendor conversations than any other singular event in recent history.

How will the SolarWinds hack change your approach to how you manage vendors/supply chain security and risk in the future?



How has the SolarWinds hack impacted your organization's current vendor outsourcing strategy?



Conclusion

The SolarWinds hack affected nearly every respondent in some form, whether their organization was directly impacted by the event or not. But amidst the shared concern, there was also a shared confidence that respondents had the visibility they needed into their network to manage this latest challenge.

With a shortage of direct indicators of compromise, SolarWinds was a showcase for the value a threat hunting practice adds to a cybersecurity group. Organizations were quick to realize this, and some have increased threat hunting budgets so they can specifically concentrate on supply chain incidents and add overall headcount to their teams. For those organizations that went into SolarWinds without threat hunting capabilities, a third of them plan to prioritize staffing in this area.

Vendor and supply chain relationships are likely to undergo lasting changes as new partnerships will be placed under higher levels of scrutiny than before. Nearly three-quarters of organizations plan to implement more stringent partnership requirements. Of existing relationships, slightly over forty percent are confident in their current vendor relationships and do not plan any active changes. This shows an understanding of the complexity of this event and that many feel the majority of security vendors are perfectly capable partners under most circumstances.

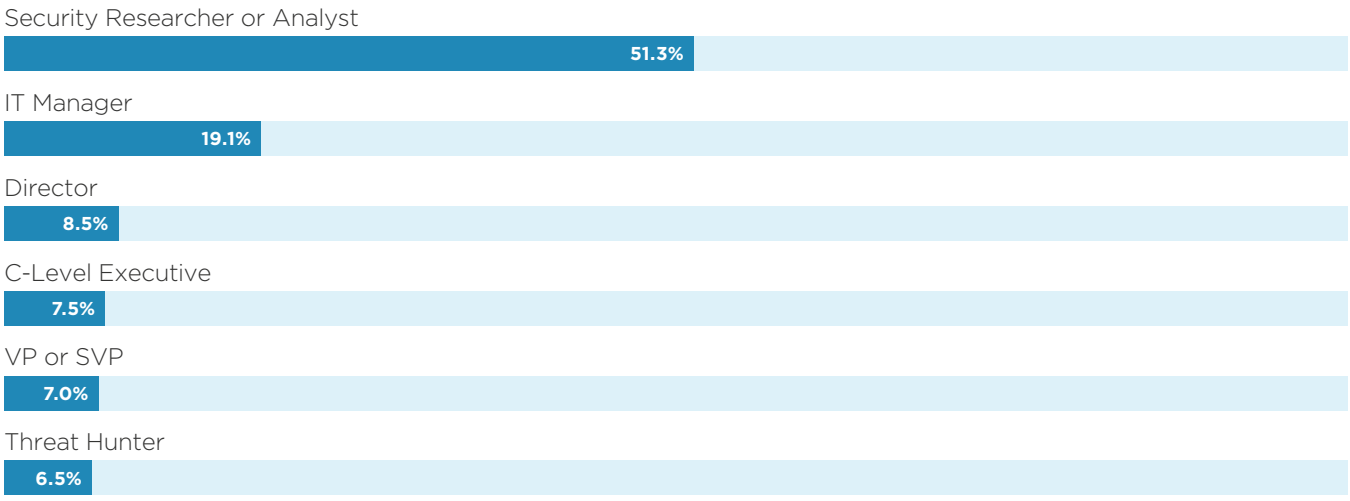
Supply chain attacks are not new; the SolarWinds attack just exposed the glaring issue it has always been. That means organizations and third-party vendors all share a responsibility moving forward to develop practices and solutions to detect or prevent the next SolarWinds.

The majority of respondents may have expressed confidence in the visibility of their networks, but the length of the SolarWinds intrusion suggests that visibility alone may not be enough. It needs to be paired with proactive security measures such as threat hunting to be able to spot the most elusive compromises. SolarWinds should be compelling evidence for security teams to win the argument for dedicated threat hunting resources.

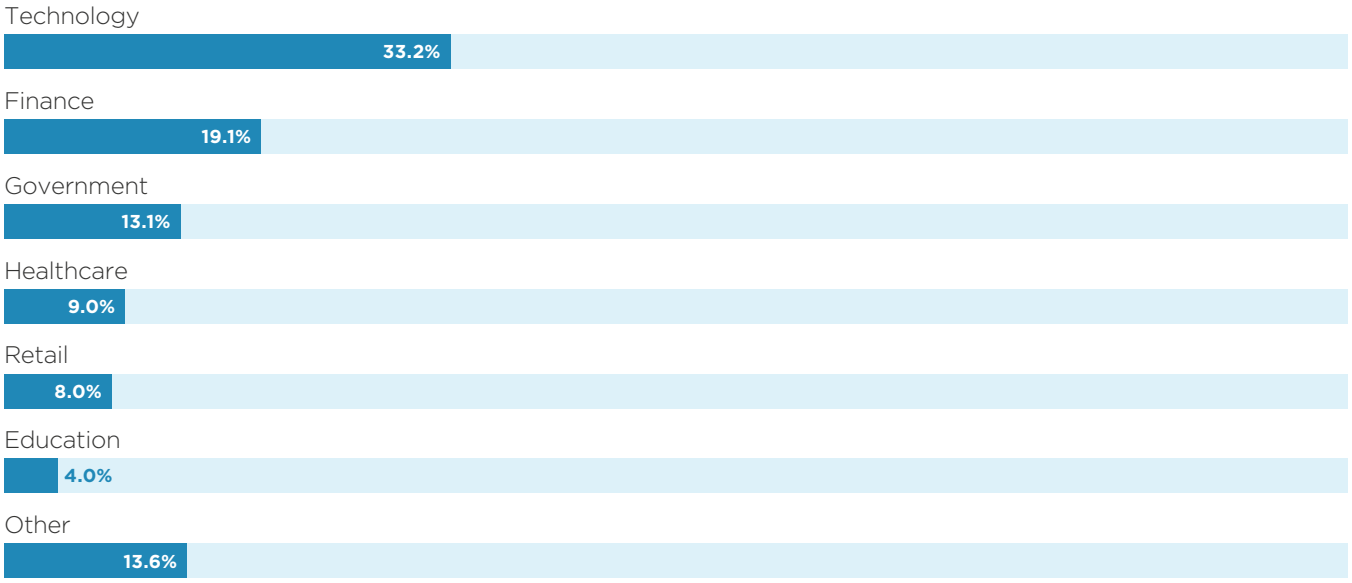
Methodology

The survey was conducted by DomainTools in February 2021, and polled 200 global security professionals and executives working in finance, government, healthcare, retail, technology and other industries in organizations of up to 10,000+ employees. Regions include North America, EMEA, APAC, and LATAM. A breakdown of the respondents' titles, roles and industries are provided below.

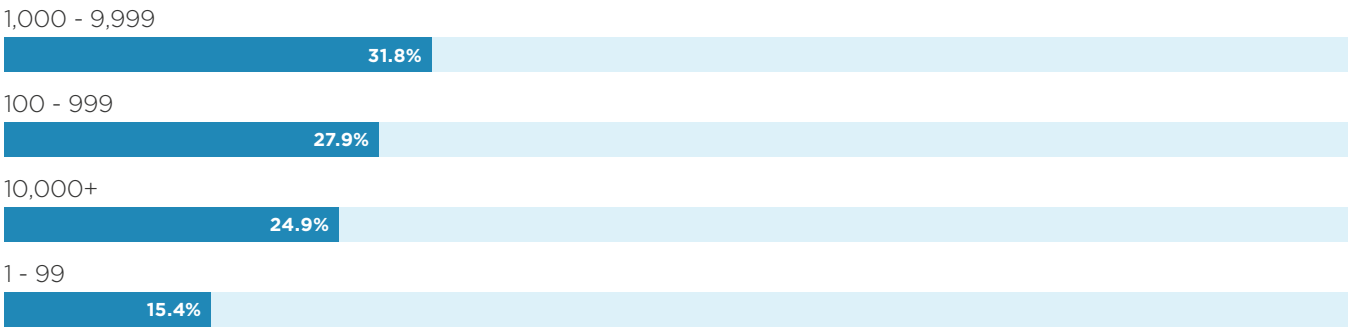
What is your title?



What is your industry?



How large is your organization?



About DomainTools

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at **http://www.domaintools.com** or follow us on **Twitter: @domaintools**.