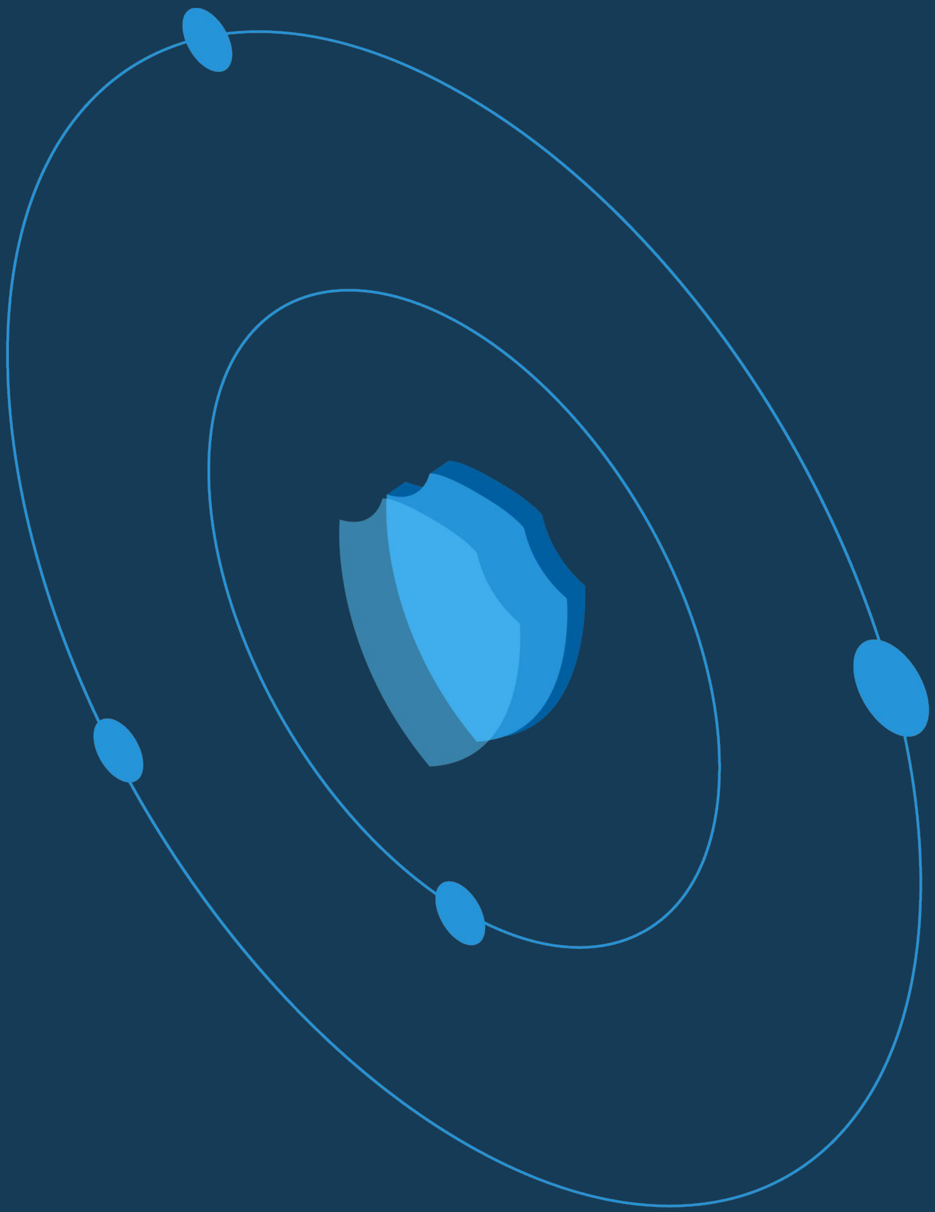
The State of Zero Trust Security in Global Organizations

Identity and access management maturity in 2020



okta

Table of Contents

Modern Security for a Perimeter-less World 3

Top five security takeaways 4

The Current State of Zero Trust 6

Zero trust across regions and industries 6

Are identity and security peas in a pod? 7

Zero Trust Maturity Curve 8

Where we are today 10

Stage 1: Unified IAM 12

Stage 2: Contextual Access 14

Stage 3: Adaptive Workforce 17

Building a Powerful Zero Trust Stack 20

Overcoming Common Barriers to Zero Trust 23

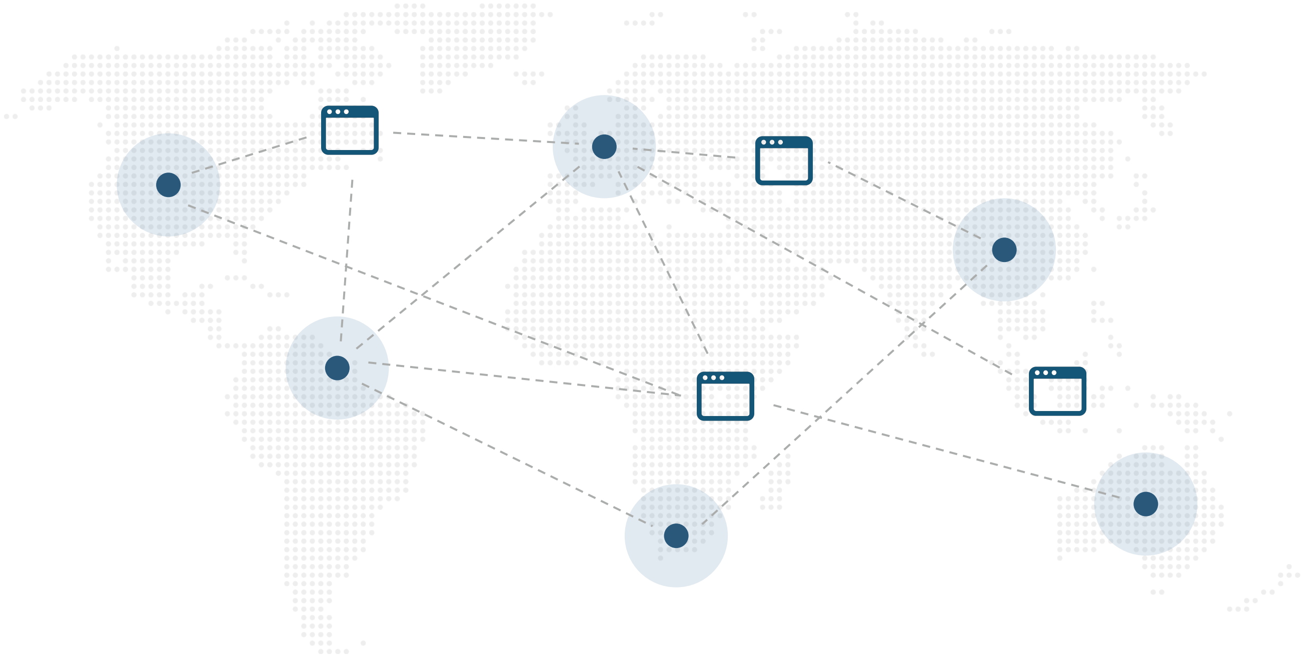
Survey Methodology 25

Who took the survey? 25

About Okta 25

Modern Security for a Perimeter-less World

There’s no denying that, among information security watchers, zero trust has gone well beyond buzzword status. The oft-discussed security framework, originally developed by Forrester Research analyst Jon Kindervag in 2009, threw away the idea that organizations should have a “trusted” internal network and an “untrusted” external network. To meet the access and usability demands of modern employees and consumers (and avoid becoming the next organization in the headlines for a data breach), companies are moving towards a more robust and comprehensive security posture that’s centered around the zero trust principle of “never trust, always verify.”



Given the new normal that’s emerging in the midst of the current COVID-19 pandemic, the implications of a perimeter-less IT environment are amplified more than ever before. And since this focus on remote work enablement — ensuring the right people have the right level of access, to the right resources, in the right context — will persist long after the crisis ends, every security leader should be working towards a long-term zero trust strategy to protect their business. Many wonder if it’s really possible to achieve the pie-in-the-sky promise of zero trust, let alone ensure that access privileges are assessed continuously without adding friction for the user. The best starting point for this journey is to replace the traditional network perimeter-centric view of security with an identity-centric mindset that ensures secure access for various user types regardless of their location, device, or network.

> *"We consistently find that enterprises have the earliest and rapidest success if they focus on improving identity management and device security. These two core components of the Zero Trust eXtended (ZTX) ecosystem drive rapid risk reduction and build confidence with executives that the organization can realize security benefits from its Zero Trust program quickly."*
>
> *— Forrester Research's "Practical Guide To A Zero Trust Implementation"*

To learn more about how organizations like this are approaching identity-driven zero trust today and where they're headed over the next 12-18 months, Okta surveyed 500 security leaders around the world about their initiatives. This report explores those findings and analyzes valuable insights across industries and regions.

Top five security takeaways

Modern, zero trust security has taken hold

Zero trust is taking hold in a very meaningful way, with 275% year-over-year growth in the number of North American organizations that have or plan to have a defined zero trust initiative on the books in the next 12-18 months. Our 2020 study finds that 60% of organizations in North America (and 40% globally) are currently working on zero trust projects.

The role of the API economy is driving a shift in security

As digital business models evolve, organizations require seamless connections with external supply chains, emerging data sources, and third-party technology systems. In this digitally connected environment, API security is absolutely critical. 21% of all organizations are planning projects to secure access to their APIs in the coming years, led by 40% of European businesses and 30% in Australia and New Zealand.

Device dominates risk signal priorities

Organizations increasingly see the value of looking at risk signals beyond checking which network users are coming from. When determining the potential riskiness of access decisions, they're elevating the importance of device health, as recommended by Forrester, Gartner, and many other zero trust proponents. Just last year, 55% of our respondents still listed the network as a top factor for context-based access decisions, but that drops to 20% in 2020. The key considerations companies — across regions and industries — now use in their access decisions are all about device posture and physical location.

We’re all in this together

The zero trust technology stack is expanding, and there’s no silver bullet. That said, forward-thinking businesses are leveraging identity and access management (IAM) systems to connect and optimize mitigation across their end-to-end security architecture. For instance, 76% of organizations outside North America plan to invest in security information and event management (SIEM) systems over the next 12-18 months. In North America, the most planned integration for IAM is orchestration and automation. And this year, just 11% of companies say they aren’t prioritizing any new security integrations with IAM (down from 36% last year), showing that the majority recognize the need for a comprehensive approach.

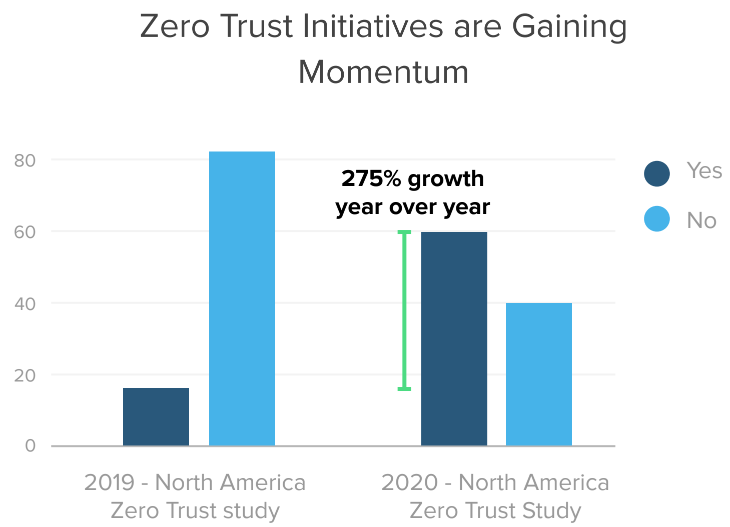
Healthy security means happy patients

We compared several aspects of zero trust maturity across industries, finding that time and time again, healthcare organizations lead the pack. This industry tops the ranked list for nearly every current and planned IAM initiative. 90% of healthcare providers are already implementing SSO for employees, and over 40% plan to implement SSO for external users in the next year or so — a number that will likely rise even more as the ripple effects of COVID-19 make their way throughout the industry. Interestingly, ownership over IAM technologies is completely in the hands of security teams at 40% of these organizations (more than twice the percentage of any other industry). Coincidence? We think not.

> *“Okta was key to accelerating our evolution to a zero trust model. This was the identity plane where we could introduce so much of the control that we needed to have in order to assess who a person is. So it was actually a way to accelerate our thinking around zero trust.”*
>
> *— Melody Hildebrandt, Global CISO, 21st Century Fox*

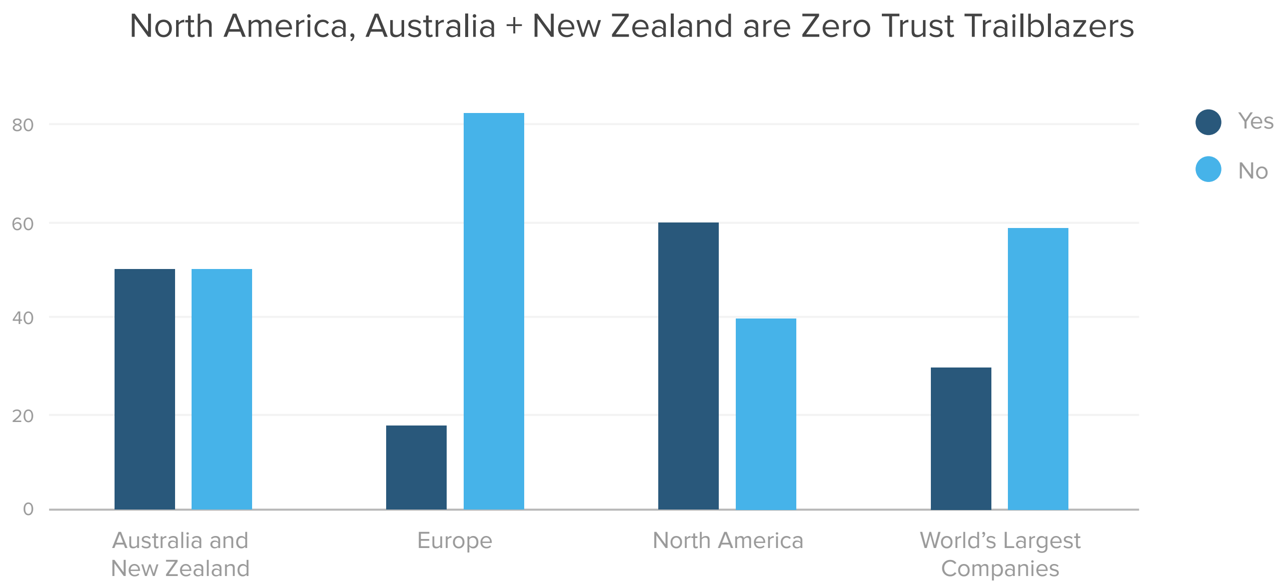
The Current State of Zero Trust

Before we dig into what a typical identity journey looks like, let's start with a glimpse into how many organizations even speak the language of zero trust. Since we started our research by asking North American companies about this topic in early 2019, we were eager to see how strategies evolved over the past year. What we found was a significant amount of growth — nearly 3X — in the number of organizations with defined zero trust initiatives or plans. That number grew from 16% in 2019 to 60% today, showing that zero trust is no passing phase.



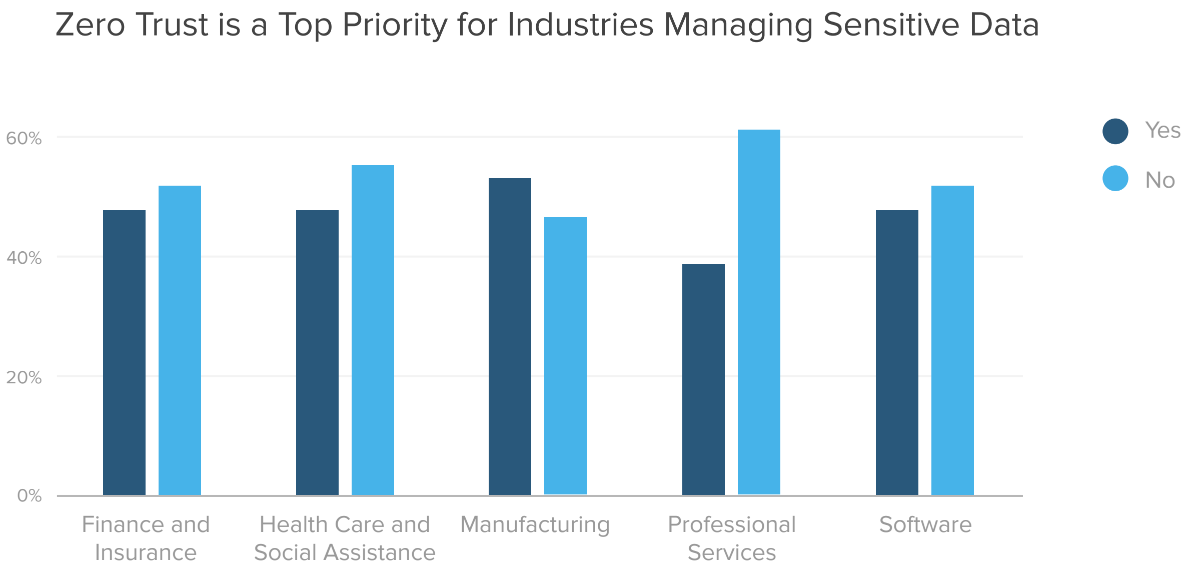
Zero trust across regions and industries

This year, we expanded our survey to learn how organizations around the world think about zero trust. North America leads with 60% of respondents embarking on zero trust initiatives. Australia and New Zealand (ANZ) are not far behind, with 50% saying they have zero trust projects underway, whereas Europe and the Middle East (EMEA) are lagging, with under 18% on board.



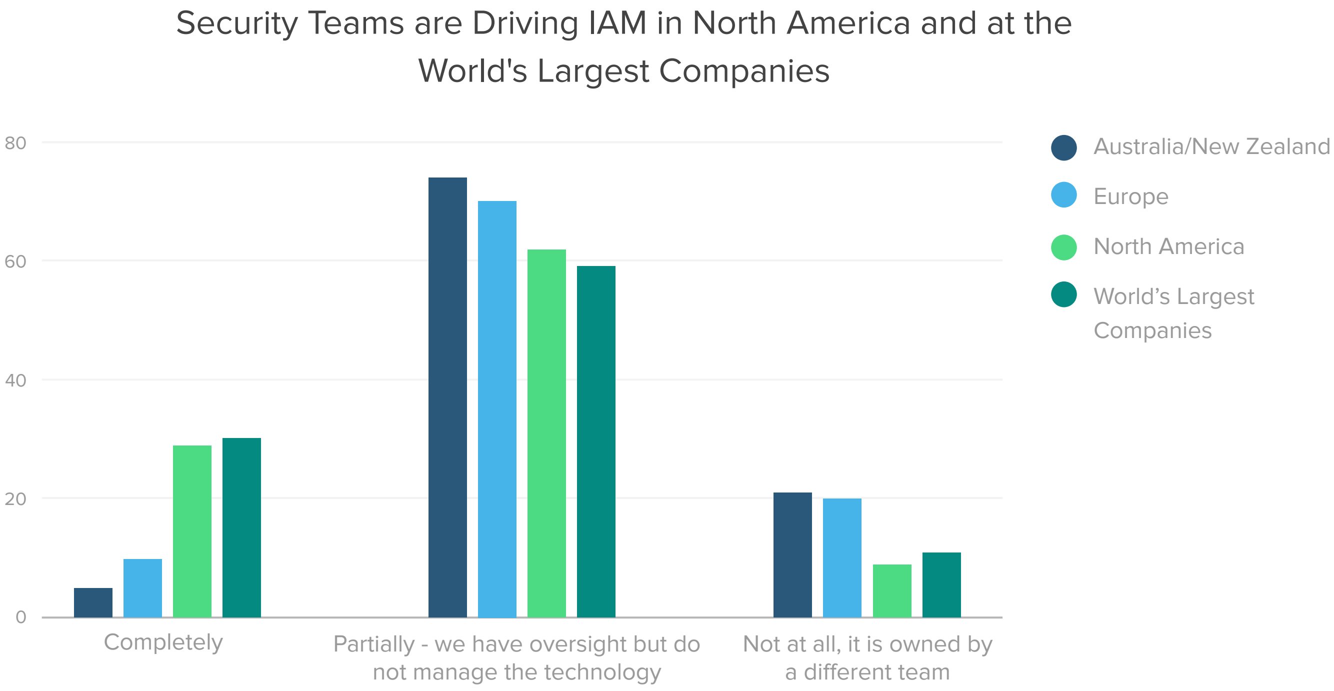
When we look into specific industries, we find that those which commonly store large amounts of sensitive data tend to prioritize zero trust more heavily. Security leaders in finance, healthcare, and manufacturing know it's crucial to be prepared because their organizations are top targets for threat actors.

However, fewer professional services firms seem to recognize their risk level, with less than 40% confirming defined zero trust initiatives. This is problematic, since Verizon's 2019 Data Breach Investigations Report found that the professional services industry deals with more security incidents than any other industry.



Are identity and security peas in a pod?

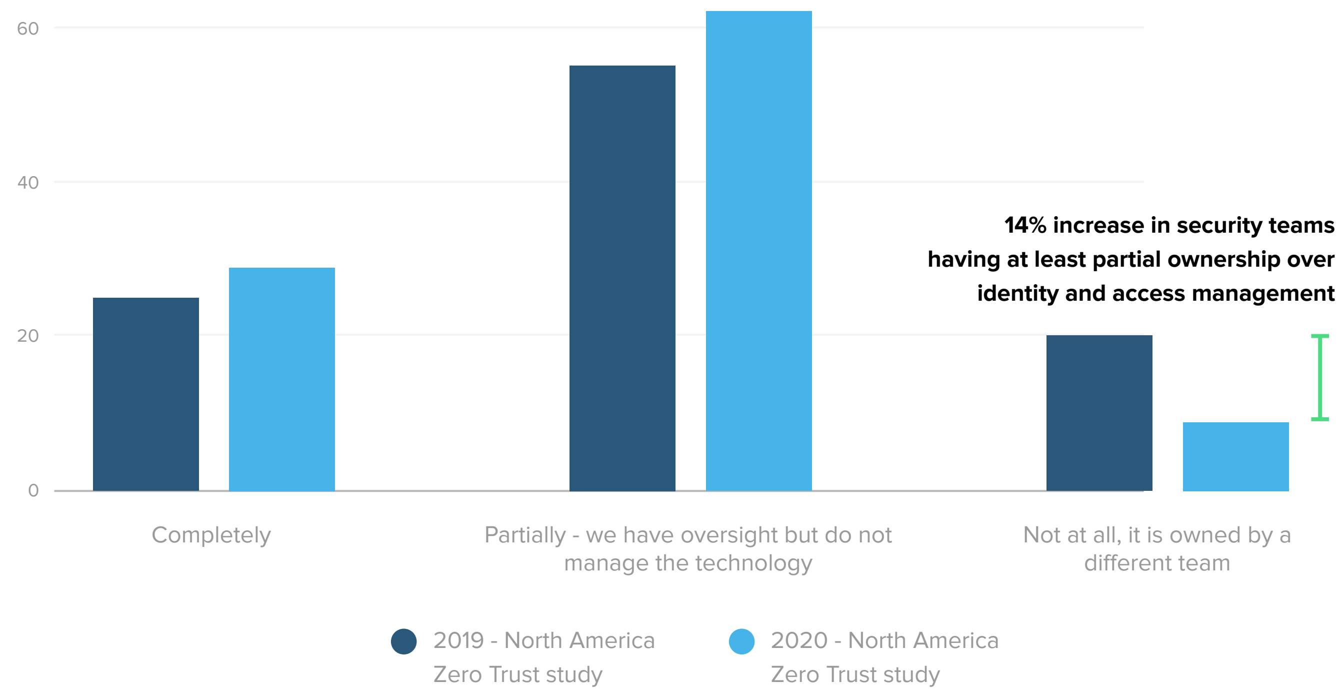
Many zero trust technologies require tight partnership between IT and security teams to be truly successful. In particular, identity solutions have traditionally been owned by the IT department, so we wondered how the move towards zero trust is impacting that relationship.



It turns out that IAM technologies — which for many organizations form the foundation of their zero trust strategy — are almost 3X more likely to be owned by security teams in North America and at the World's Largest Companies (defined here as organizations on the latest Forbes Global 2000 list) than in other segments. In healthcare, over 40% of respondents say their security team completely owns IAM, double the percentage in any other industry.

When we dig further into our year-over-year North American data, we learn that security's partial or complete IAM ownership levels have gone up 14% since 2019 (today with 91% of security leaders reporting complete or partial ownership of identity and access management solutions, up from 80% the year prior), indicating that security leaders are taking an increasingly larger role in managing the IAM technologies at their organizations.

Security Teams' Ownership of IAM is on the Rise in North America

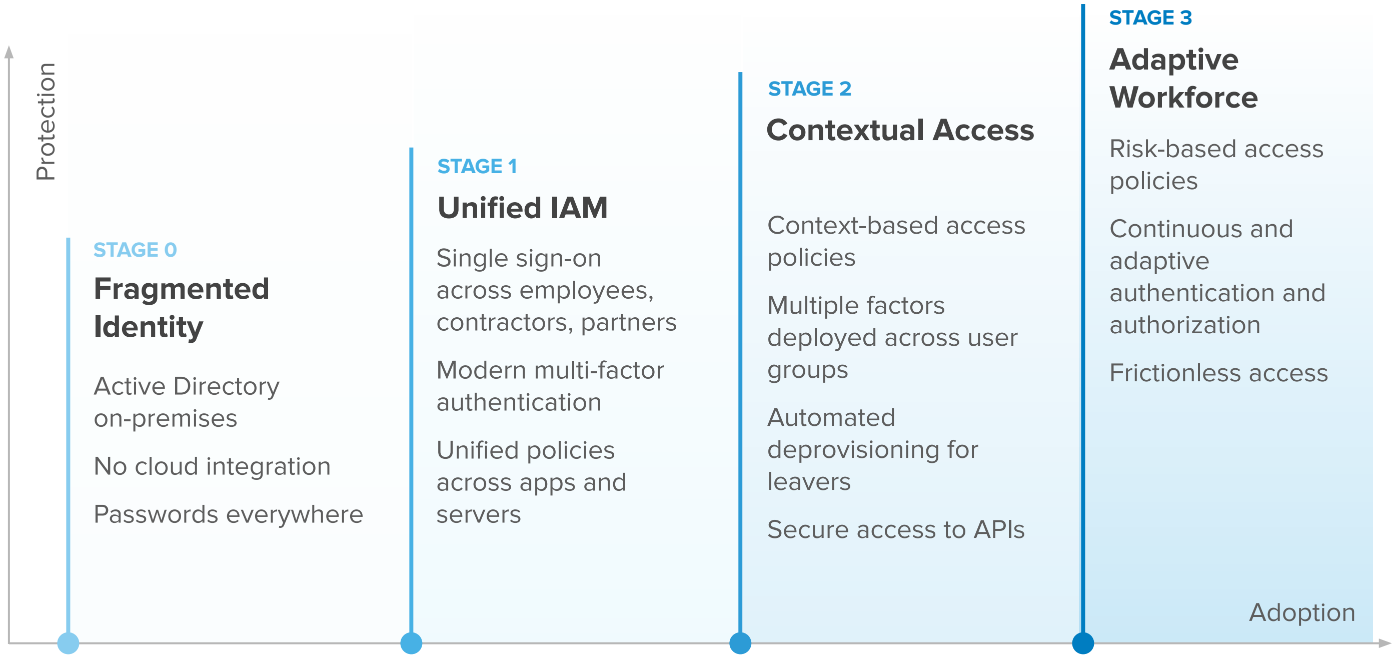


14% increase in security teams having at least partial ownership over identity and access management

Zero Trust Maturity

Now that we've established the lay of the land, let's explore what zero trust initiatives actually entail, through the lens of Okta's identity and access management maturity curve. As organizations work to implement a zero trust architecture built around identity-driven security practices, we find they roughly follow four primary stages of maturity:

Identity and Access Maturity Curve



STAGE 0

Fragmented Identity

Active Directory on-premises

No cloud integration

Passwords everywhere

STAGE 1

Unified IAM

Single sign-on across employees, contractors, partners

Modern multi-factor authentication

Unified policies across apps and servers

STAGE 2

Contextual Access

Context-based access policies

Multiple factors deployed across user groups

Automated deprovisioning for leavers

Secure access to APIs

STAGE 3

Adaptive Workforce

Risk-based access policies

Continuous and adaptive authentication and authorization

Frictionless access

These aspects of zero trust span everything from the type of resources an organization manages, to how they provision and deprovision users, which authentication methods they deploy, and more. Companies with a fragmented approach to identity really haven’t started down the path yet. During Stage 0, they might begin to embrace cloud technologies, but don’t yet integrate those solutions with an IAM platform or on-premise resources. At Stage 1, teams start wrapping their arms around a unified IAM ecosystem through projects like eliminating poor password hygiene by implementing single sign-on (SSO) and multi-factor authentication (MFA) for employees to access key resources.

Moving into Stage 2, businesses adopt additional security best practices by extending access controls to other resources such as their APIs, and also using rich context and diverse factors to better inform authentication decisions. It’s worth noting that API protection is especially critical at this stage, since Gartner has found that, "By 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the user interface, up from 40% in 2019." Once companies reach Stage 3, they’ve successfully adopted a full risk-based authentication approach to zero trust, with passwordless and continuous access solutions.

These aspects of zero trust span everything from the type of resources an organization manages, to how they provision and deprovision users, which authentication methods they deploy, and more. Companies with a fragmented approach to identity really haven’t started down the path yet. During Stage 0, they might begin to embrace cloud technologies, but don’t yet integrate those solutions with an IAM platform or on-premise resources. At Stage 1, teams start wrapping their arms around a unified IAM ecosystem through projects like eliminating poor password hygiene by implementing single sign-on (SSO) and multi-factor authentication (MFA) for employees to access key resources.

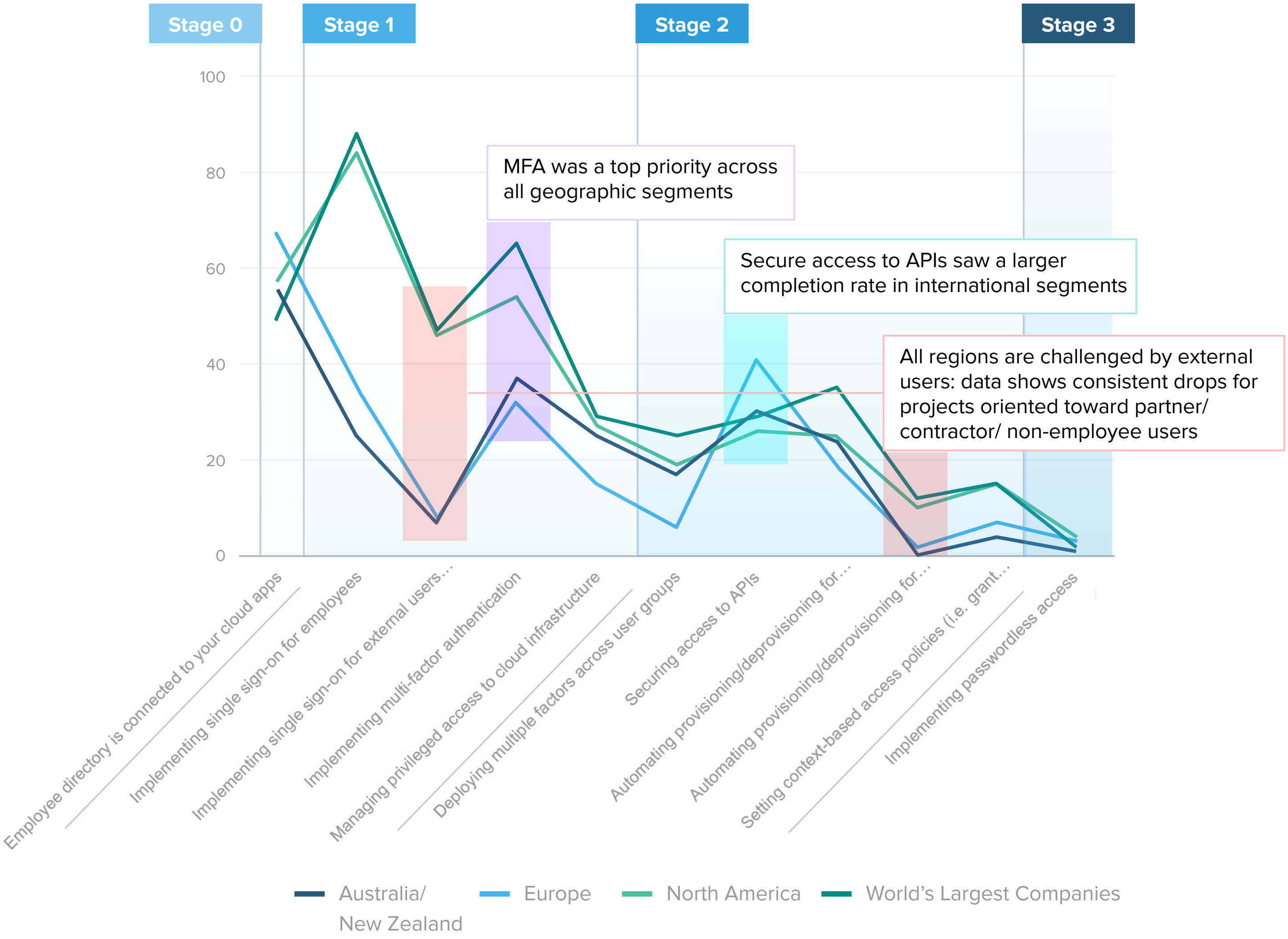
Moving into Stage 2, businesses adopt additional security best practices by extending access controls to other resources such as their APIs, and also using rich context and diverse factors to better inform authentication decisions. It's worth noting that API protection is especially critical at this stage

> *"By 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the user interface, up from 40% in 2019."*
>
> *— Gartner*

Where we are today

We asked respondents what projects they've completed or have in the works so we could figure out who's ahead of the curve, and identify opportunities for further progress.

North America, World's Largest Companies Are Most Advanced in Overall IAM Projects; International Organizations Lead in API Security



MFA was a top priority across all geographic segments

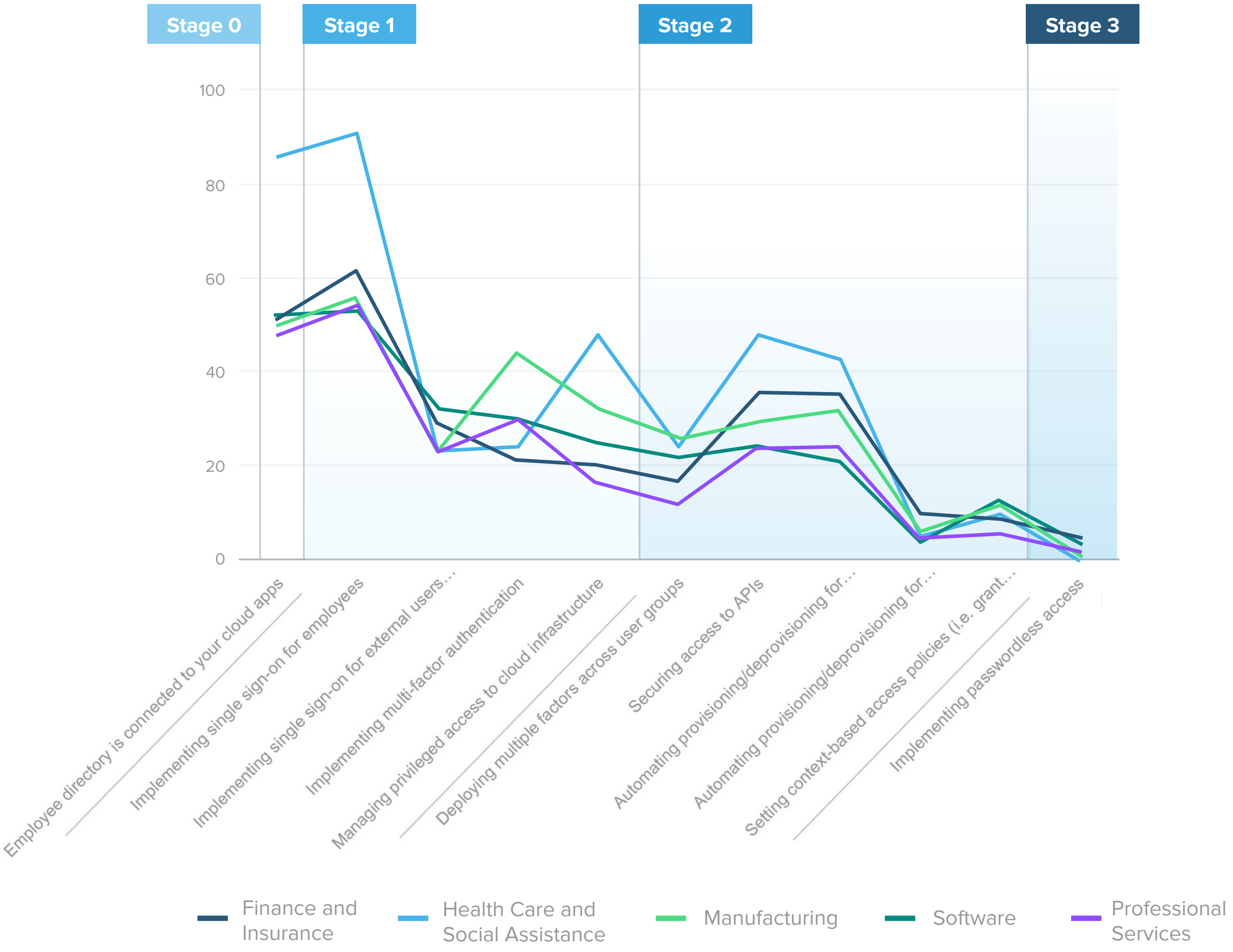
Secure access to APIs saw a larger completion rate in international segments

All regions are challenged by external users: data shows consistent drops for projects oriented toward partner/ contractor/ non-employee users

When considering global averages for each of the individual stages outlined above, it’s clear that the vast majority of companies are still in Stage 0 or Stage 1 of their zero trust journey. Looking more closely, we start to see a divergence between applying strong authentication and risk tools for employees versus the full extended workforce, including contractors and partners. Many organizations are still behind on eliminating password sprawl via SSO for these external users, especially outside of North America. Similarly, most businesses haven’t yet taken the step to automate provisioning for external users, however they’re placing higher priority on API security and context-based access policies.

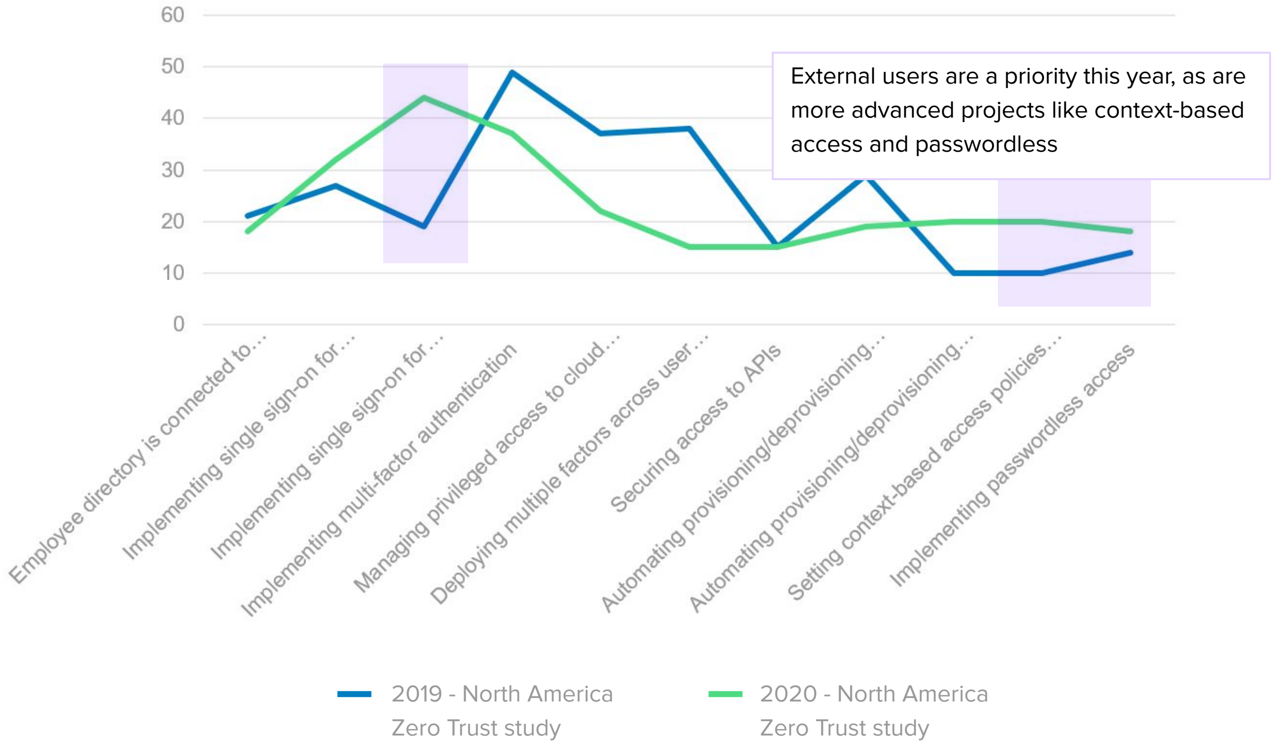
Healthcare organizations top the industry list for nearly every type of zero trust initiative, both in their current and planned projects. 90% of providers have already implemented SSO for employees, and over 43% plan to implement SSO for external users in the next year or so. However, when it comes to more advanced Stage 3 capabilities, such as automating provisioning and deprovisioning for external users (6%), setting context-based access policies (10%), or implementing passwordless access (0%), healthcare security lags behind the manufacturing and software industries, which are prioritizing those projects slightly higher.

Healthcare Leads the Pack in Majority of IAM Zero Trust Projects



It's also interesting to note how zero trust maturity evolved in North America over the past year. The biggest increase came with SSO protections for external users — up to 46% from 16% of organizations in 2019 — although employee SSO implementations also saw a nice bump from 65% to 85%. Because it's been a growing trend in recent years, many companies have already implemented at least basic MFA for their core employees — up to 54% from 44% — so fewer teams are planning MFA projects in the next 12-18 months. Given the gaps mentioned earlier, it doesn't come as a huge surprise that their next goal appears to be rolling out these same technologies for external users.

Planned IAM Projects in North America: 2019 vs. 2020



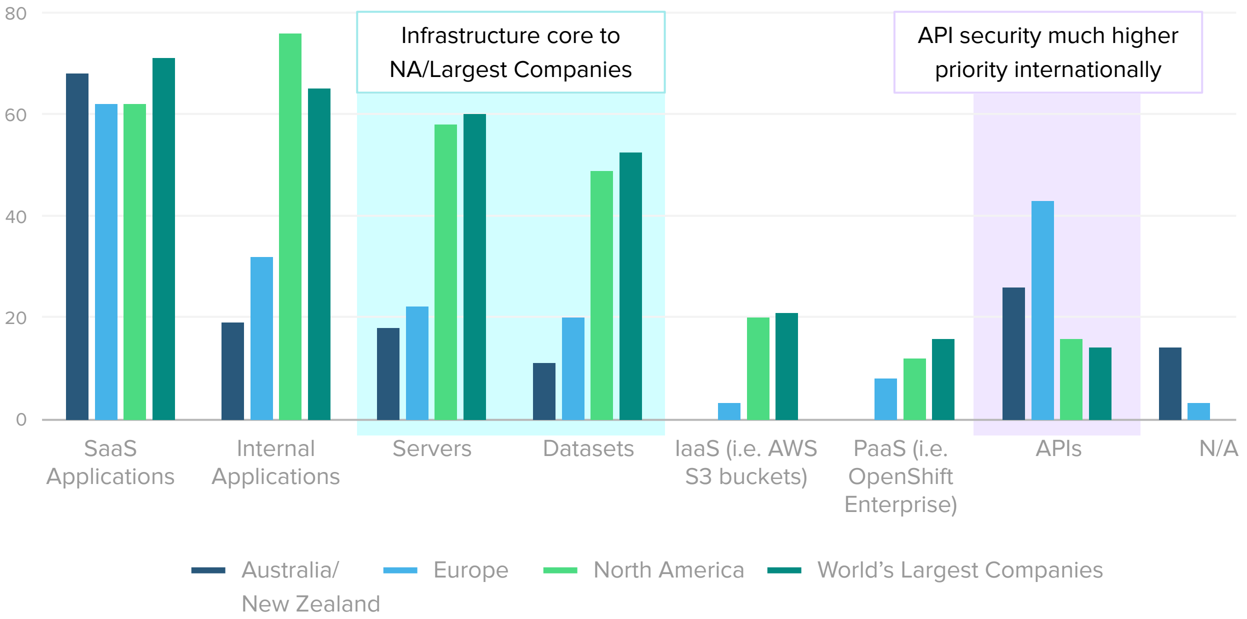
External users are a priority this year, as are more advanced projects like context-based access and passwordless

Stage 1: Unified IAM

To assess progress within the unified IAM stage, we asked whether businesses are requiring SSO for employees or external users, implementing MFA, and/or managing privileged access to cloud infrastructure. By adding multiple layers of security to their authentication mechanisms, Stage 1 organizations ensure users really are who they say they are in order to stop bad actors from accessing their systems.

Looking to the next 12-18 months, we learned that Australia and New Zealand are playing a bit of catch up in these areas, with 52% of respondents still working on implementing SSO for employees, along with many projects surrounding MFA and API security.

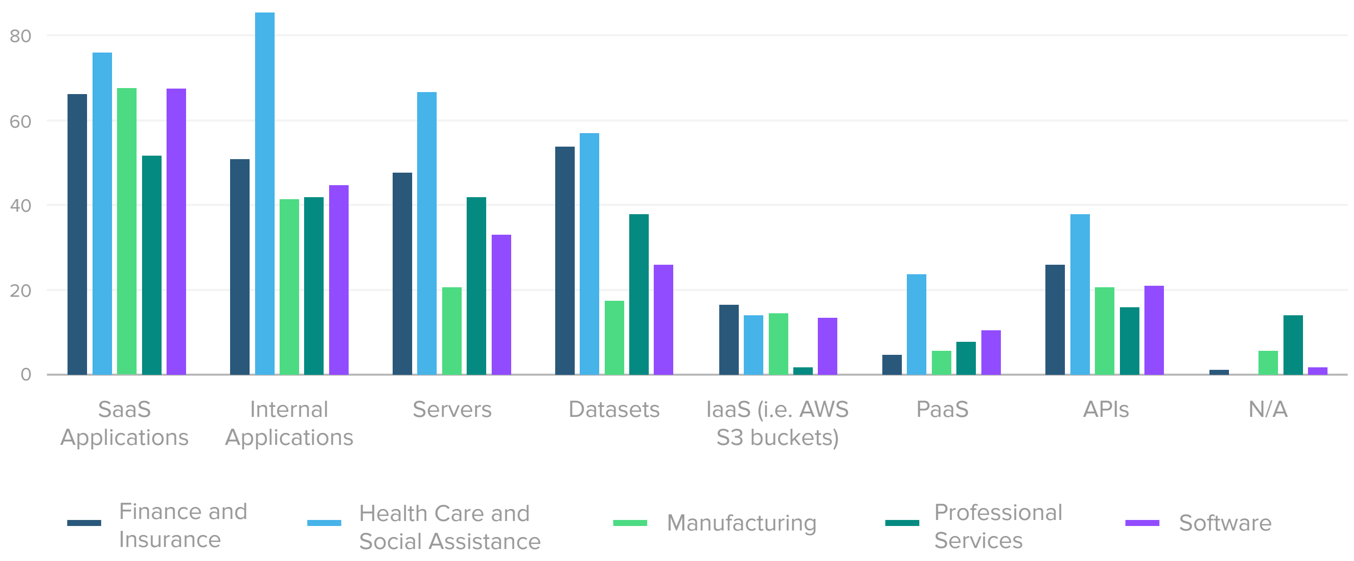
Secure Access to SaaS Apps is a No-Brainer Across Regions



European respondents fell slightly ahead of Australian and New Zealand in terms of current SSO adoption, but while ANZ orgs are prioritizing SSO and MFA for the employees, European security leaders are splitting their priority projects between employees and external users, with just under 30% focused on SSO for each group.

In terms of creating unified access policies by extending SSO and MFA across apps and servers, maturity levels vary across specific resource types. Internationally, organizations focus on access controls for APIs, while in North America (and similarly across the Global 2000), businesses are more concerned with securing access to their infrastructure (i.e., servers and databases).

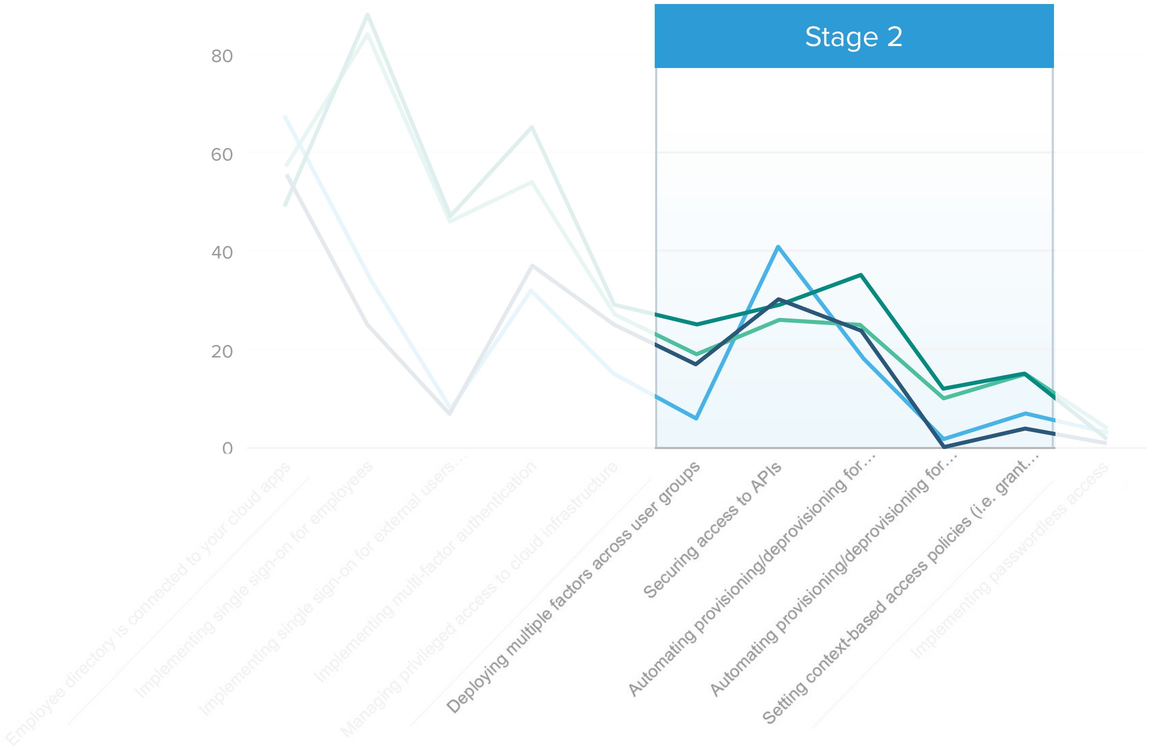
Healthcare and Finance Want It All



Stage 2: Contextual Access

To evaluate Stage 2, we asked respondents whether their organizations deploy safeguards such as multiple factors across user groups, secure access to APIs, automated account provisioning and deprovisioning for employees and/or external users, or context-based access policies. Teams at this stage clearly understand the risks associated with an ever-expanding network perimeter, and have taken big steps toward protecting it.

Average Stage 2 maturity hasn't changed dramatically in the last year, although around twice as many North American organizations have or are planning to implement automated provisioning and deprovisioning for external users, as well as context-based access policies.

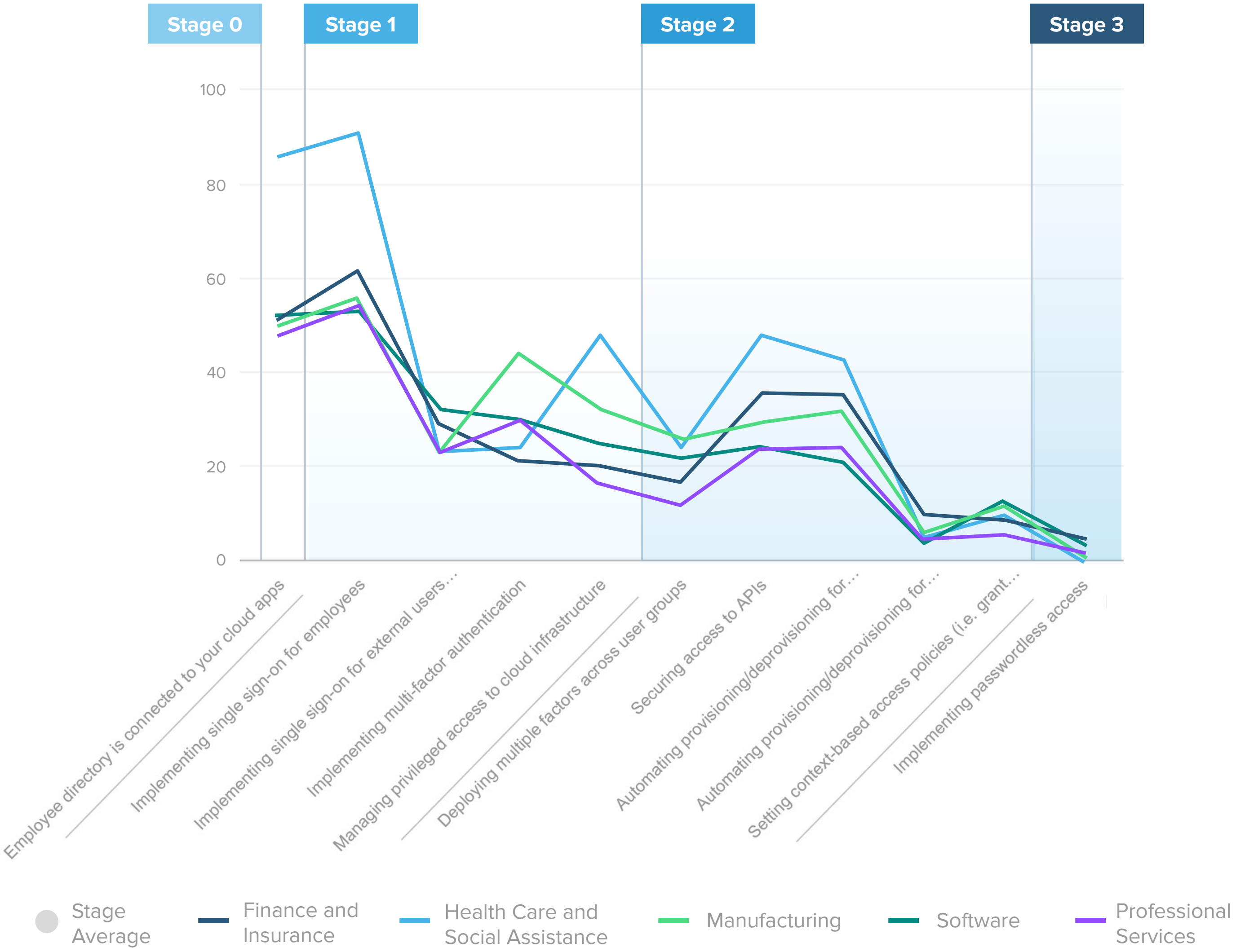


The reality is that most haven't yet taken these steps, however our research found that some segments are starting to more highly prioritize API security and context-based access policies.

Gartner predicts that by 2022, API attacks will be the greatest source of data breaches for enterprise web applications, so it's good to learn that in EMEA, 41% have implemented API security (as compared to only 26% of North American businesses). Our expectation is that this is likely due to Europe's tightening regulatory landscape, with laws surrounding open banking and other models driven by API usage.

New regulations also account for the high percentage of organizations focused on API security in regulated industries, with almost half of healthcare providers (48%) and a third of financial firms (35%) working on securing their APIs. Of course, manufacturing businesses with complex partner ecosystems also have good reason to implement stronger access controls around APIs, leading 29% of them to prioritize this aspect of zero trust.

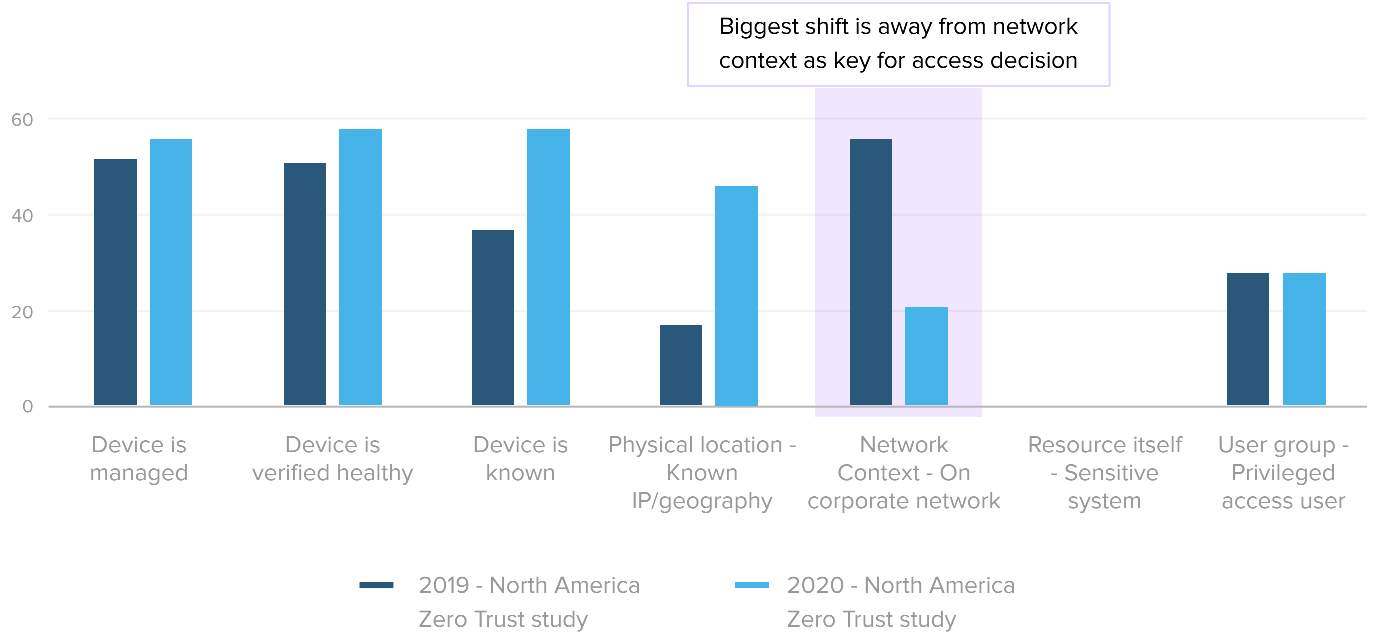
Secure Access to APIs Projects Rise in Regulated Industries



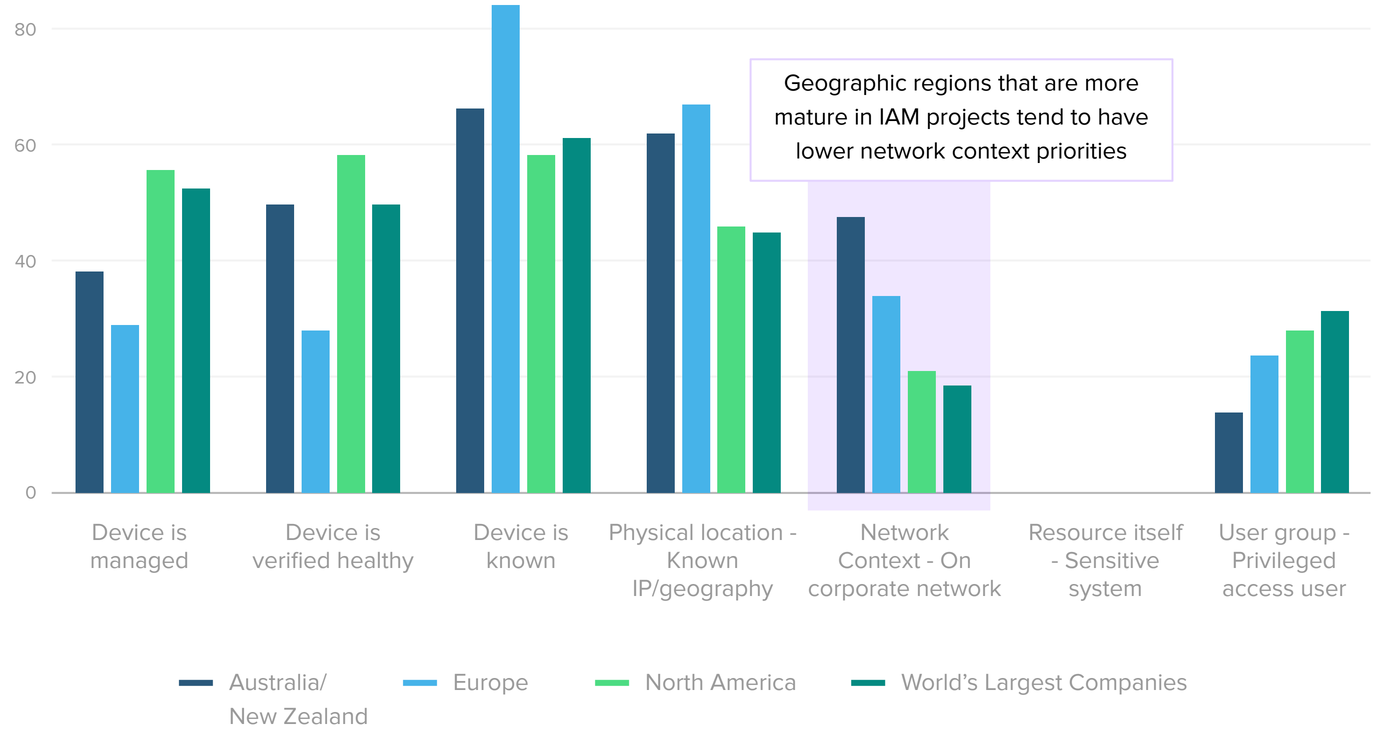
But which context factors do organizations look at when making the decision whether to grant access to a user? Since the core of a zero trust strategy involves shifting away from network perimeter-based security and towards context-based access decisions, we asked how security leaders are making their MFA policies context-aware to better assess users' devices, networks, locations, or the applications they're attempting to access.

The biggest change we noticed over the past year was a move away from making decisions based on whether the user is accessing resources from a corporate network — from 56% listing the network as a top factor in 2019, down to just 21% in 2020. While these surveys took place before the crisis hit, this reflects an increasingly important strategy for businesses to consider in light of this year's sudden global move to remote work during the COVID-19 pandemic, in which the vast majority of employees are now accessing work resources from public networks.

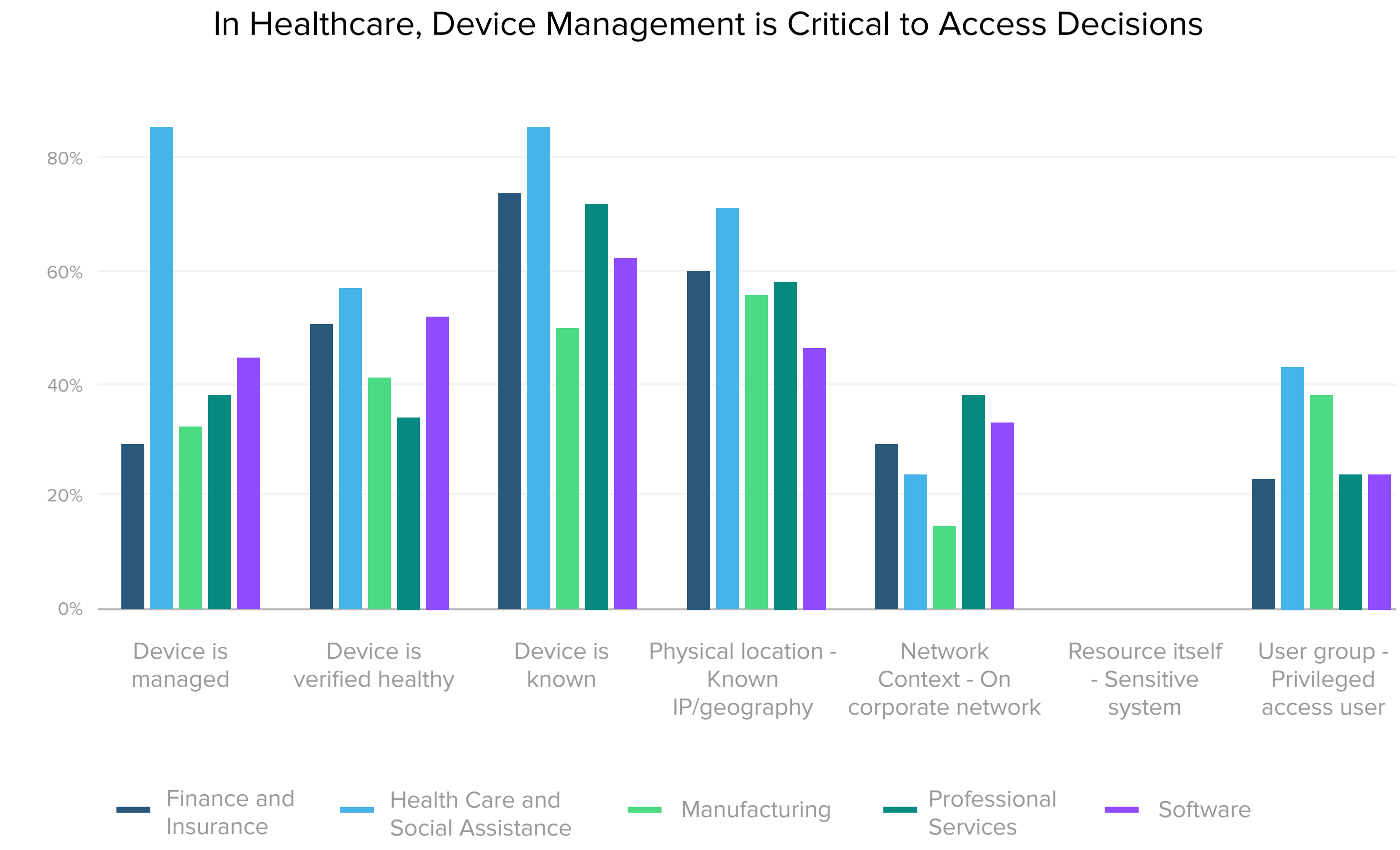
What Matters for Contextual Access Decisions? Device Context Rises, Corporate Network Declines



Network Context Matters Less in More Mature Regions



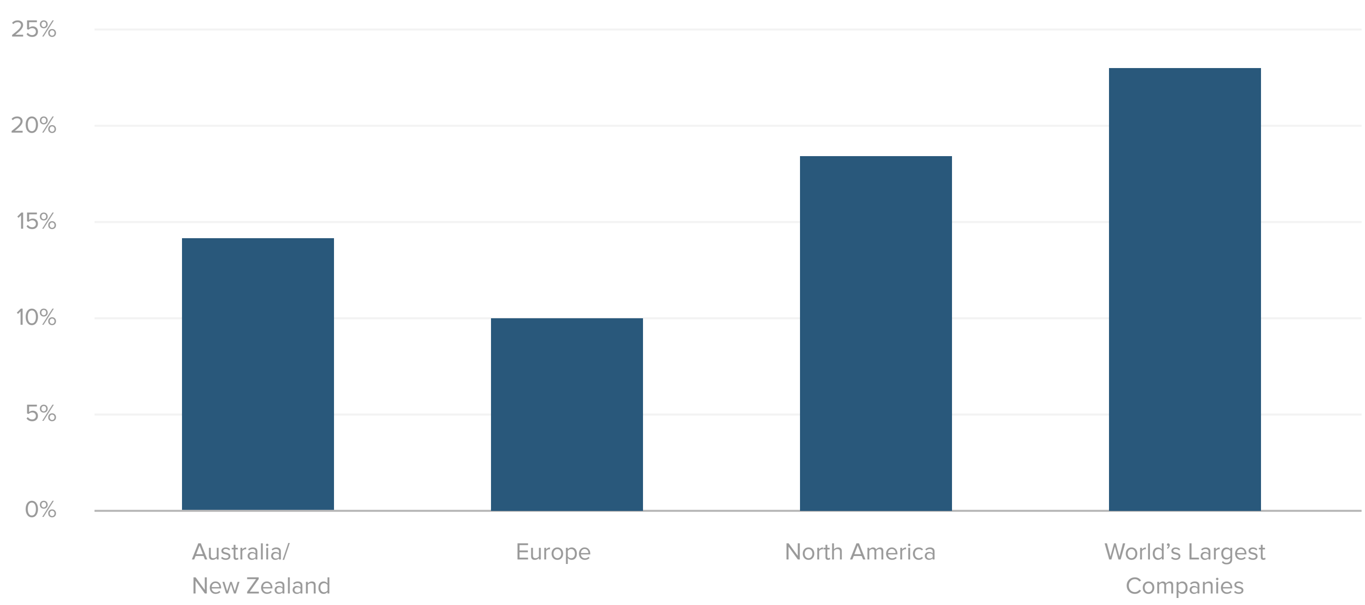
In line with established zero trust best practices, respondents told us that the primary factors they now use in access decisions are related to device posture, such as whether a user's device is known, managed, and/or verified as healthy. This device focus was also reflected in our regional breakdown, which shows that more mature markets (North America and the world's largest organizations) place less emphasis on network context than they do on any other factor. Across both regions and industries, knowing the user's device is generally the most important attribute (with the exception of healthcare, where having a managed device is equally important, likely due to HIPAA compliance).



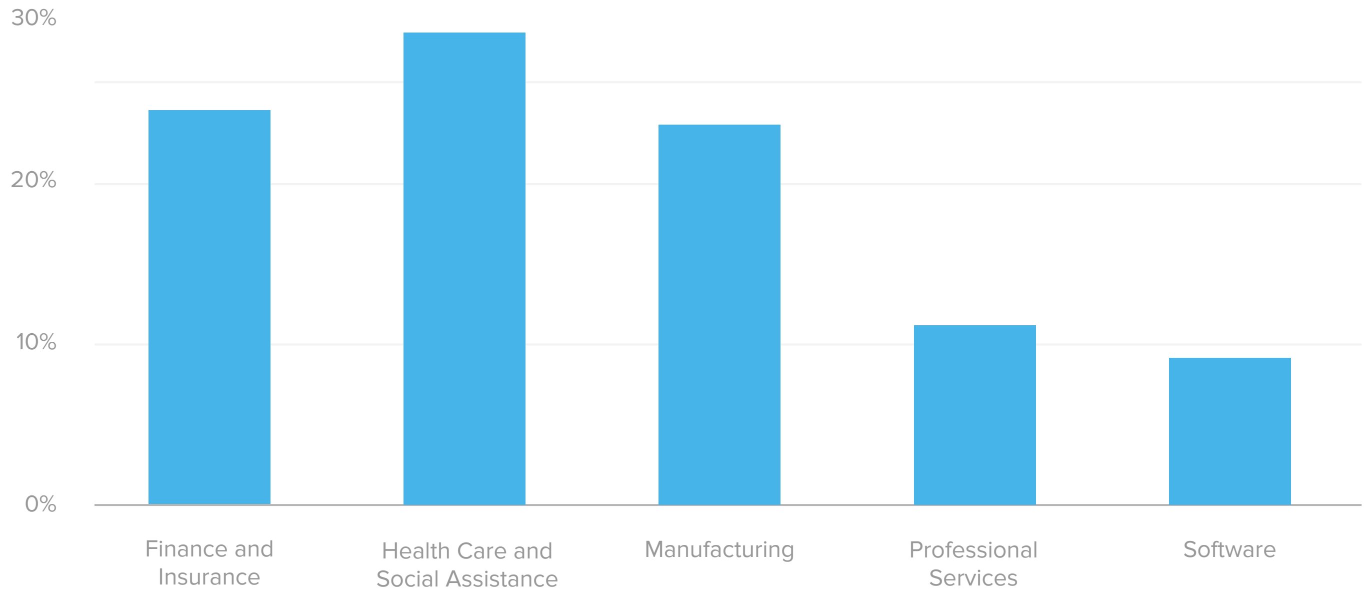
Stage 3: Adaptive Workforce

We all know the inherent insecurity of passwords — particularly since 34% of people use the same login credentials across multiple accounts. Thankfully, new passwordless authentication innovations with factor sequencing, email magic links, biometrics, tokens, and WebAuthn-related methods can help protect businesses from data breaches that compromise user information. While adoption of passwordless solutions is still in its early days, at least 10% of companies across all regions and industries are moving in the passwordless direction, with North America regionally leading the charge (18% of organizations reported planned passwordless projects in the next 12-18 months).

Passwordless Priorities: By Geography



Passwordless Priorities: By Industry



These security teams have a firm understanding of the risks and are leading the way by doing the necessary due diligence to reduce their attack surface and safeguard their organizations against future threats. In addition to implementing sophisticated and adaptive access management policies, they also recognize the benefits of creating a smooth experience for employees, contractors, partners, and customers.

> *“It used to be that security and convenience didn't really go hand-in-hand. We’ve been able to raise our game in terms of cybersecurity and securing our environments, while providing a frictionless and convenient user interface.”*
>
> *— Jamshid Khazenie, Chief Technology Officer for USA TODAY Network*

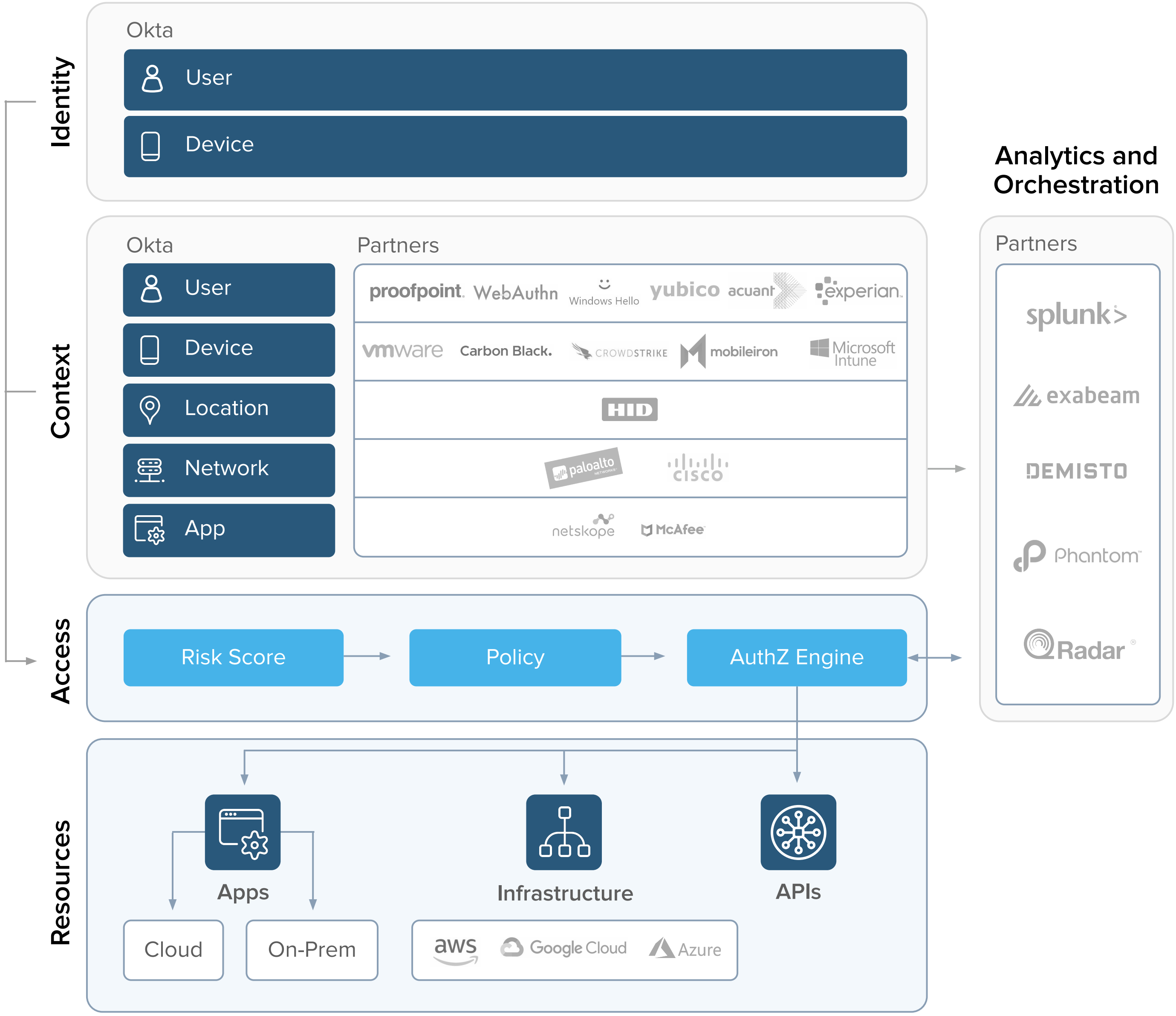
However, zero trust is a marathon, not a sprint. The next challenge in developing a cutting-edge security posture is to maintain this frictionless user experience while evaluating authentication and authorization decisions based on constant, repeated verification of trust, rather than solely at the point of logging in. This continuous component of zero trust is something the entire industry is working to advance.

With the security landscape always evolving, leaders must keep looking to the future of identity and access management. In order to outwit bad actors that are moving targets, it’s important to be aware of new developments in the space and partner with a leader like Okta who’s 100% focused on security and can help you prepare. That way, you’ll be able to continue monitoring the systems you have in place, ensure you’re always up to date on the latest security threats and technologies, and find ongoing ways to automate these tasks so your team can spend their time on strategic priorities.

Building a Powerful Zero Trust Stack

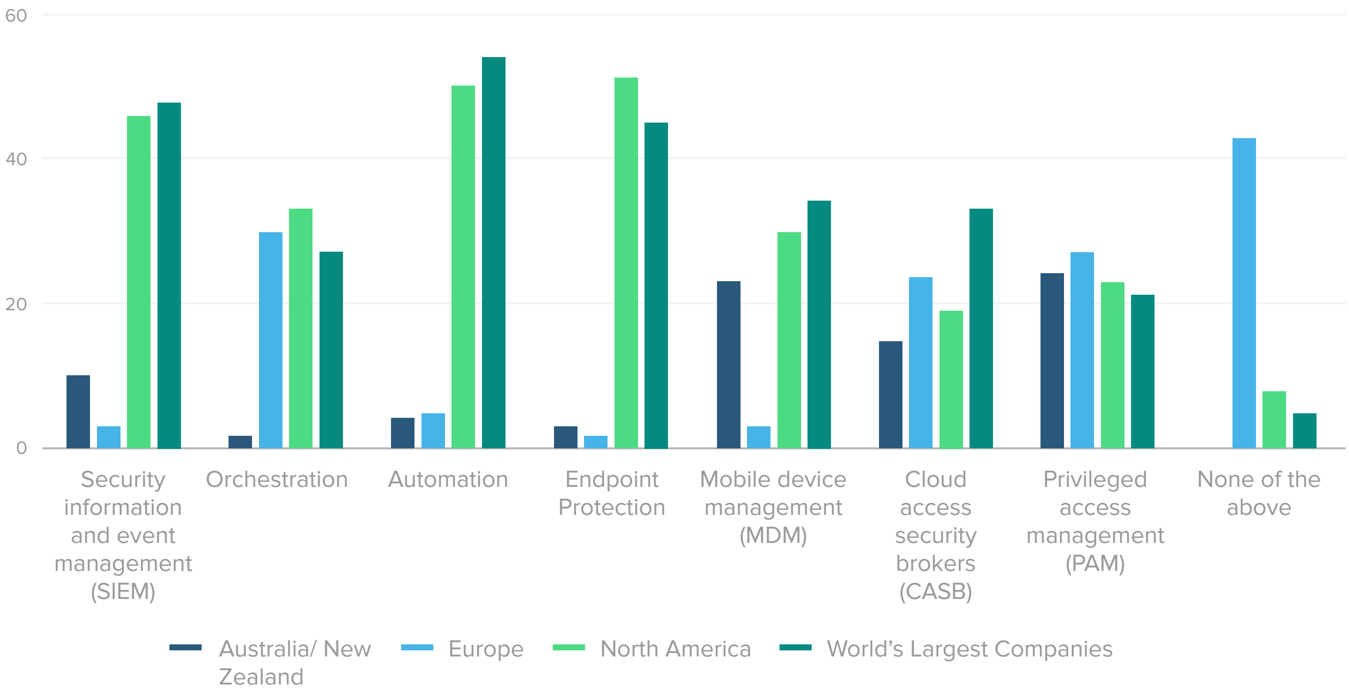
No single solution solves for all aspects of Zero Trust, so another critical best practice is leveraging identity to optimize mitigation across the security stack. Integrating all aspects of a business' security architecture — including security information and event management (SIEM), orchestration and automation, endpoint protection, mobile device management, cloud access security brokers (CASB), and privileged access management (PAM) — with an IAM solution helps establish a holistic, fine-grained approach to zero trust.

With this in mind, we asked security leaders what other tools they have integrated or plan to integrate with their IAM system. As we've seen across the other dimensions analyzed in this report, North American organizations and Global 2000 businesses are further along the road towards broadening their zero trust architecture with platforms such as SIEM, orchestration, automation, and endpoint protection, and plan to continue zero trust integrations across the board.

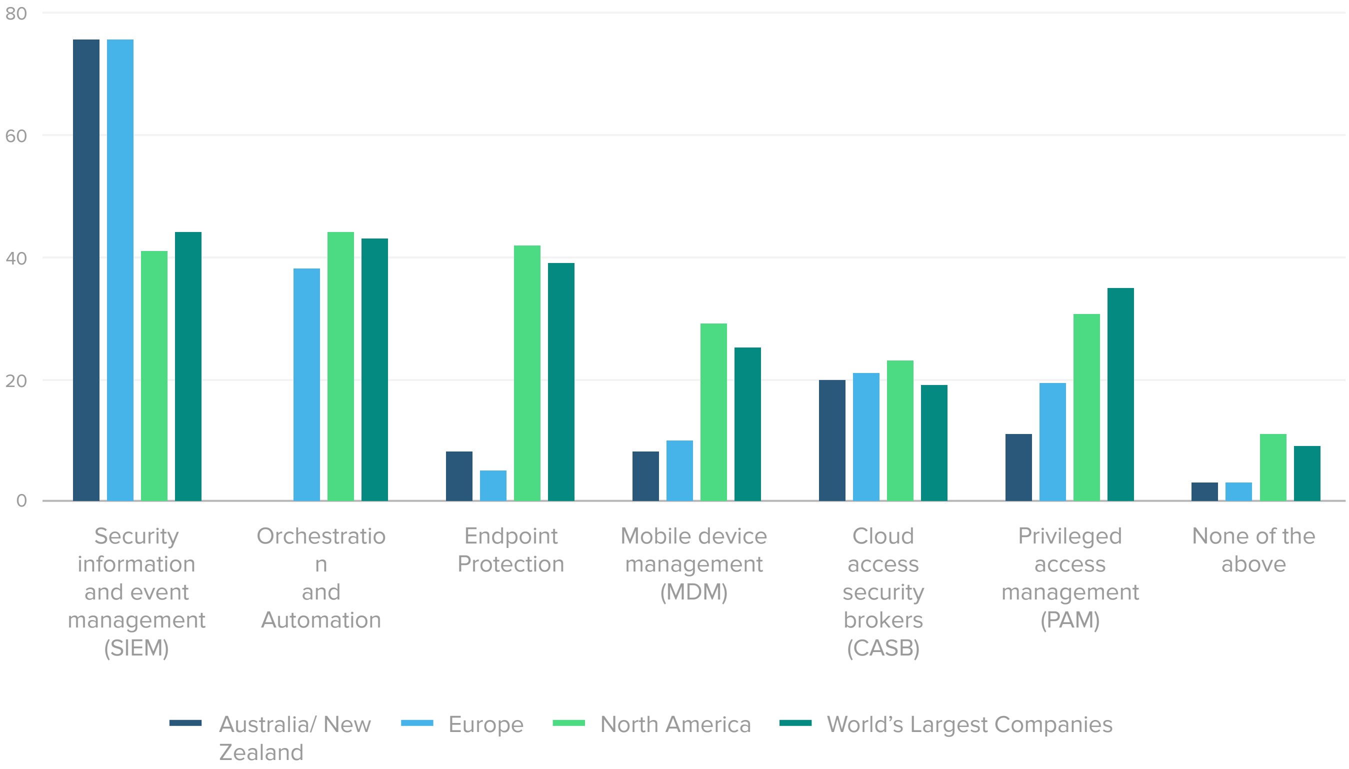


While several European and Australia/New Zealand companies have already connected PAM and CASB tools with IAM, 43% of European organizations haven't yet integrated any of the technologies we asked about. However, that's clearly changing, since 76% of Australia/New Zealand and European businesses plan to invest in SIEMs over the next 12-18 months, as well as continue to grow their CASB and PAM integrations.

IAM Global Integrations: Current Status

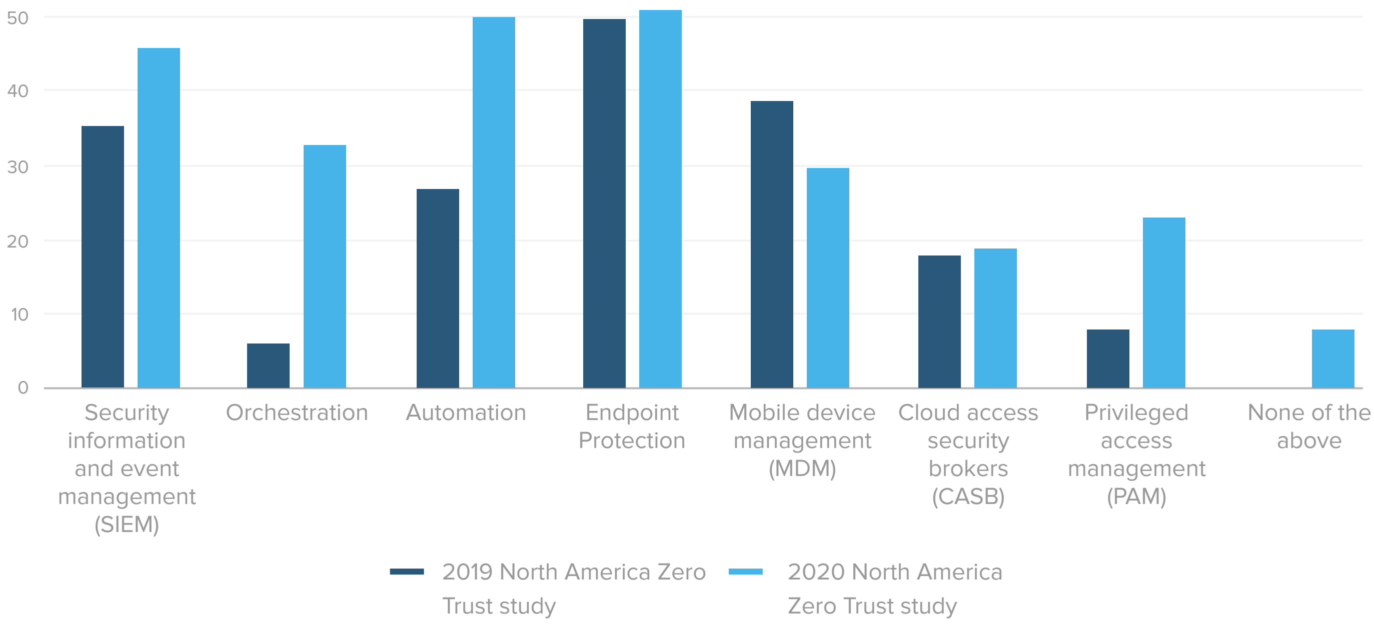


SIEMs Top Future Priority List Internationally

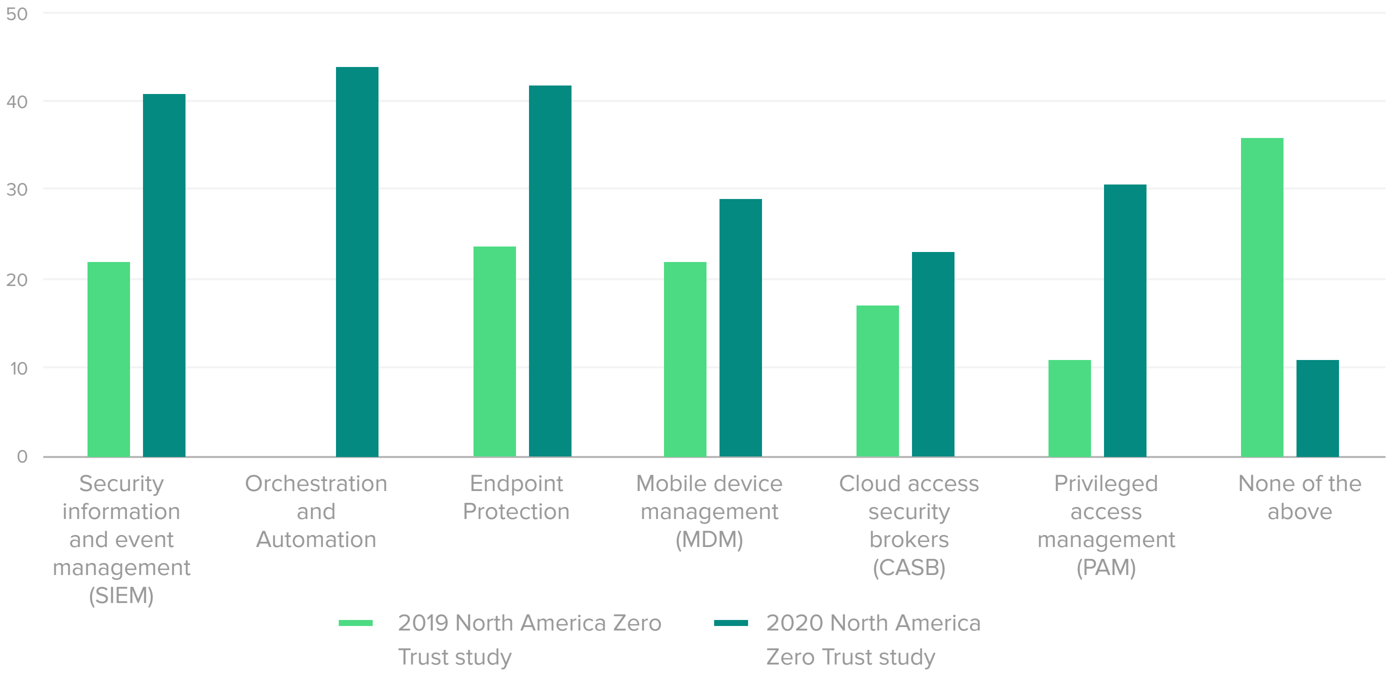


Organizations increasingly recognize the value of placing IAM as the cornerstone of their security stack, where it can work seamlessly with other specialized tools to inch closer to zero trust nirvana. In looking at progress over time, it's worth noting the rising number of current integrations with orchestration (from 6% to 33% of companies) and automation (from 27% to 50%) systems. And the number of teams prioritizing at least some new security integrations with IAM jumped 25% in 2010, with "none of the above" responses dropping from 36% in 2019 to 11% this year.

Current State: Rise in Automation and Orchestration in North America

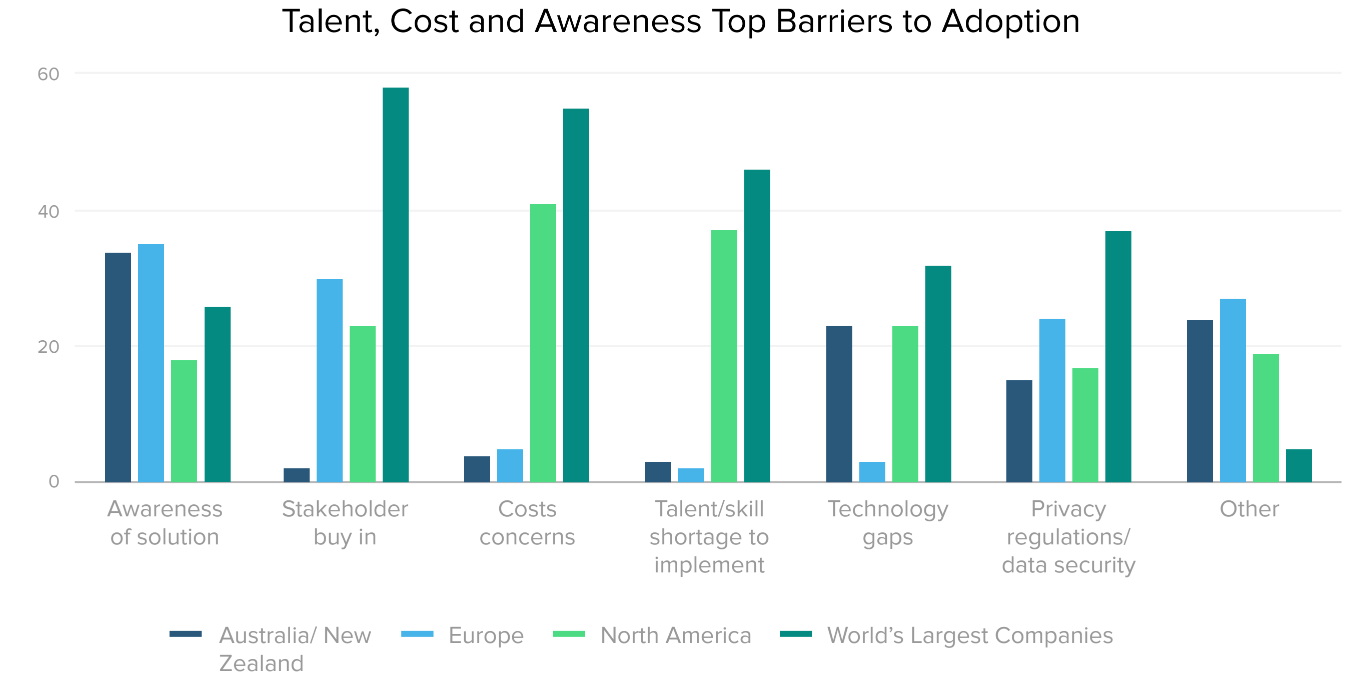


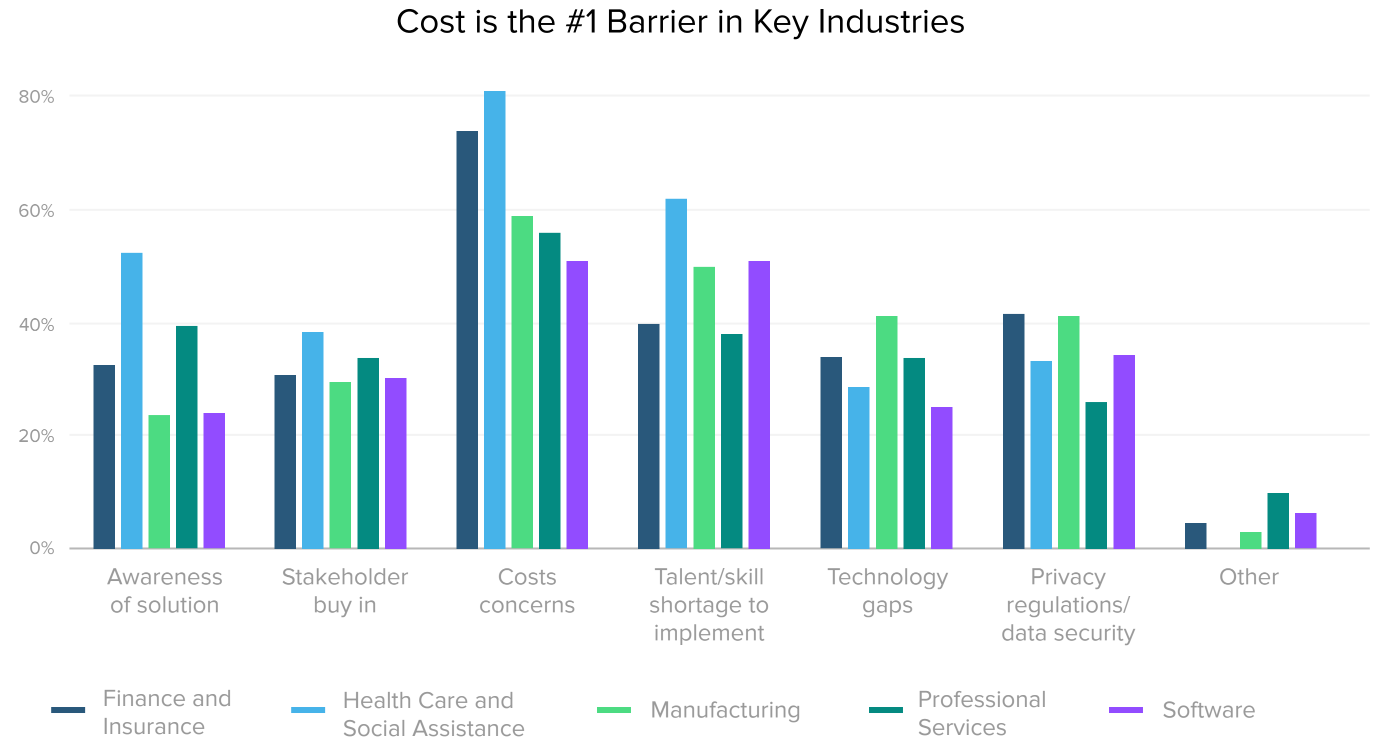
Priority Projects: Integrations Increasing, SIEM, SOAR and Endpoint Lead Pack



Overcoming Common Barriers to Zero Trust

More and more organizations realize the need to adopt a zero trust framework and stay on top of the latest security advancements in order to protect their customers, employees, and shareholders from the headaches and costs of a breach. According to Ponemon Institute's most recent Cost of a Data Breach report, a "mega-breach" of 1 million records could cost a company $42 million, while a loss of 50 million records costs an estimated $388 million.





This risk can't be ignored, since the odds of experiencing a breach are growing (nearly 30% of all companies experience a breach over a two-year period) and the typical lifecycle of a data breach is increasing (the average time to identify and contain a breach is 279 days). Every day that goes by, your business loses money, customer retention suffers, and your teams waste valuable time they could be putting towards mission-focused work.

Given the painful realities of the current threat environment, we asked security leaders what's holding their organizations back when it comes to zero trust. Awareness of zero trust as a solution is still a major barrier in over a third of international companies, while North America's most significant challenges are cost (41%) and talent shortages (37%). Cost and talent are also top concerns across industries, along with 42% of financial companies citing privacy regulations and data security as a key issue, and 52% of healthcare organizations struggling with awareness. The primary barrier for 58% of Global 2000 businesses is stakeholder buy-in.

Implementing zero trust is not easy, and doesn't happen overnight, even for companies with the greatest resources to throw at the problem. However, the digital nature of our modern economy means that security threats will only intensify, so no business can afford to stand still. If your organization is ready to accelerate its zero trust strategy, there are several ways you can make gradual progress by following in the footsteps of Global 2000 companies that are ahead of the game.

For example:

- **Stage 1** — Provide secure access to servers via SSO or MFA, which 60% of the world's largest organizations have implemented, as compared to 40% of respondents overall.
- **Stage 2** — Automate the provisioning and deprovisioning of employee accounts, like 35% of large organizations, as compared to 26% of respondents overall.
- **Stage 3** — Work towards frictionless access, something that 23% of global organizations are planning to implement in the next 12-18 months, as compared to 16% of respondents overall.

As your organization takes steps to ingrain a zero trust mindset and figure out how to bring security best practices to the next level, it can be very helpful to benchmark this work against your peers. Check out Okta's zero trust assessment tool for a prescriptive roadmap to putting zero trust identity and access controls in place. Based on the IAM maturity curve detailed in this report, our assessment will review your identity-driven security practices surrounding everything from the type of resources you manage to how your IT department provisions and deprovisions users. It will also explore which authentication methods you deploy, the policies you have in place, and your future business priorities in order to determine your current maturity and offer actionable recommendations on where you can go from here.

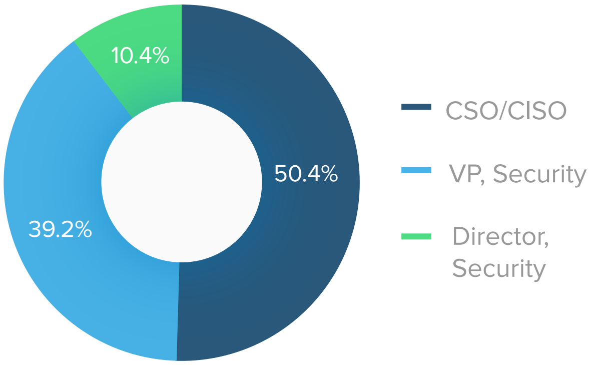
Survey Methodology

Commissioned by Okta, Pulse Q&A conducted a survey of 500 director and above security decision makers at global companies across multiple industries. Decision makers were defined as someone responsible for making technology purchasing decisions, and Pulse collected responses from January 17, 2019, to January 17, 2020. These users may or may not be Okta customers. We refer to this survey as “our survey” and “survey,” and refer to the people who responded as “survey respondents” or “respondents.

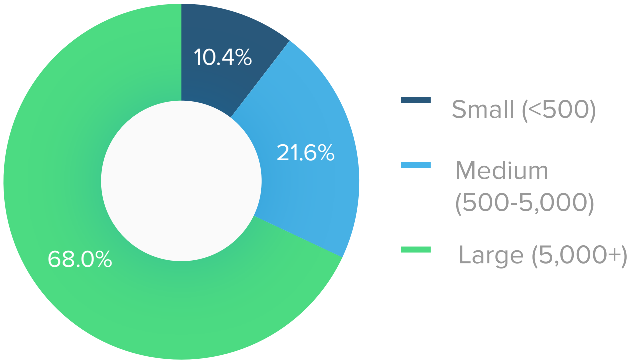
Who took the survey?

Here is a look at the 500 survey respondents and the companies they represent. For industry data, we used percentages within each segment to normalize and compare responses across the top five industries.

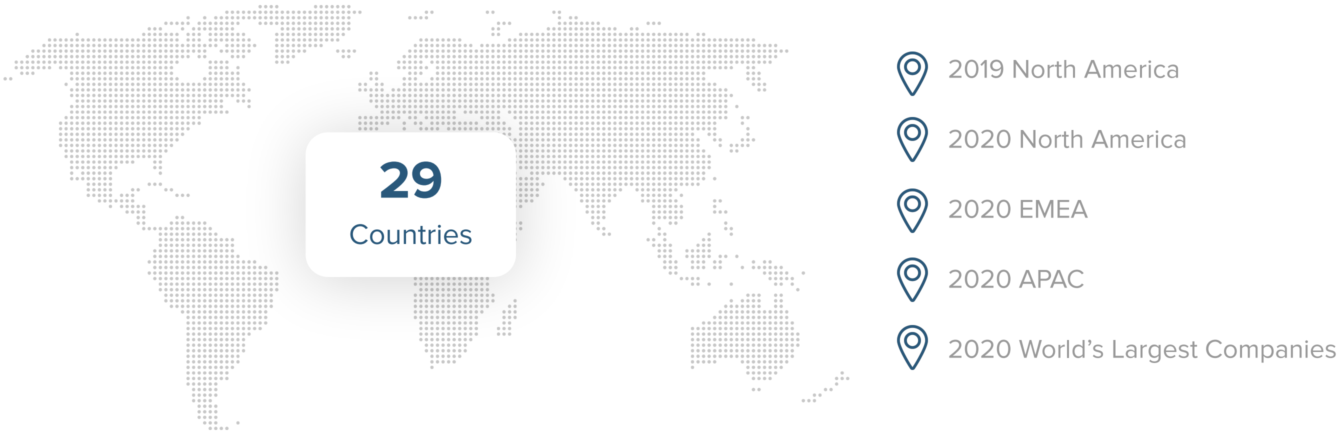
Respondent Roles

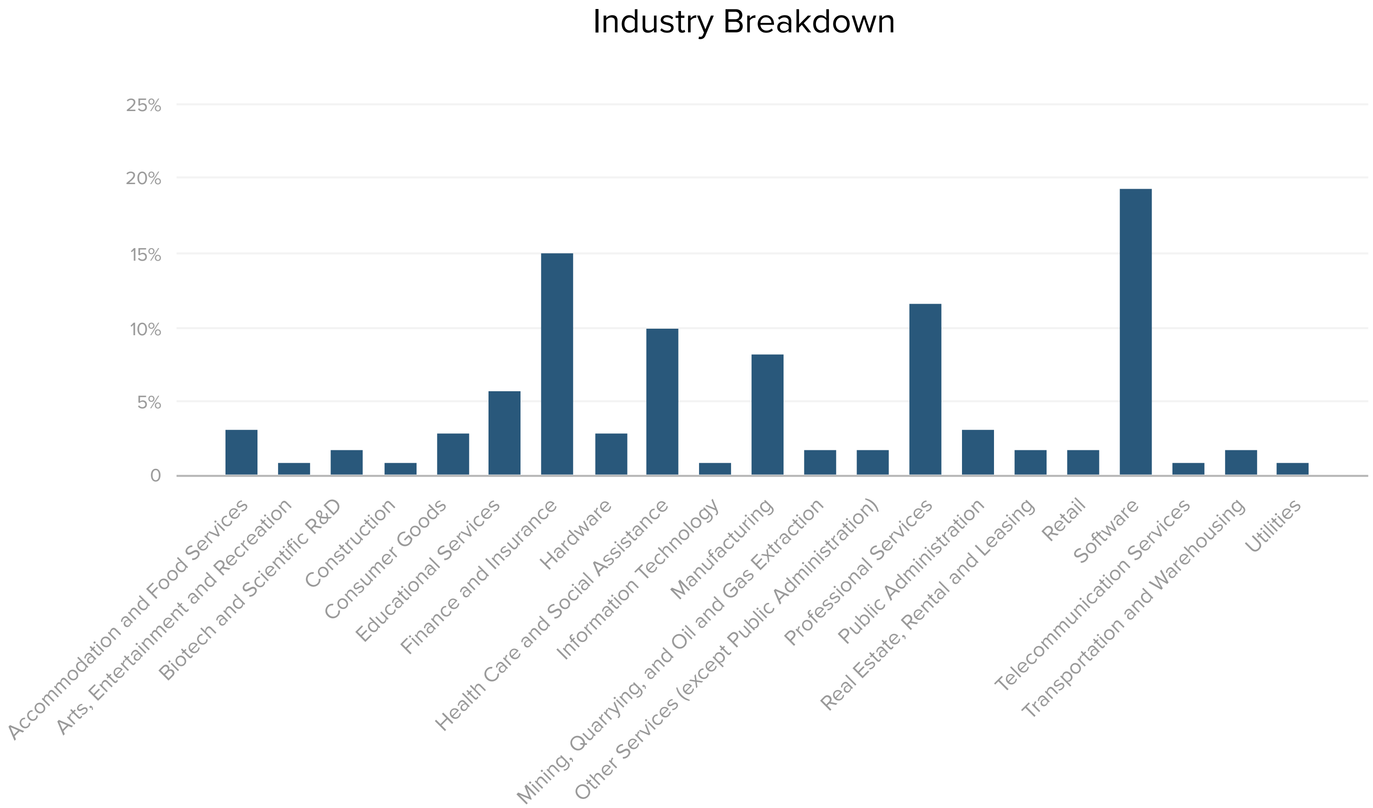


Organization Size



Geographic Breakdown





About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 7,950 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.