Enterprise Strategy Group™ by TechTarget

Considerations for Implementing Zero Trust for the Workforce

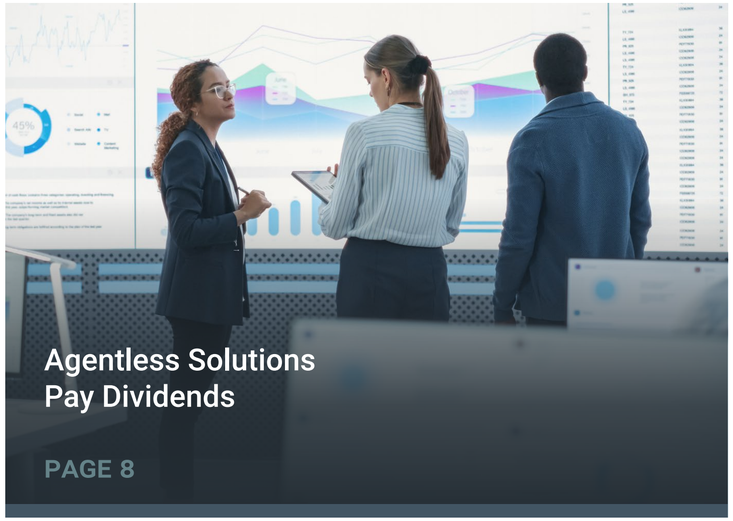
Moving Beyond VPNs to Ensure Consistent, Secure Access

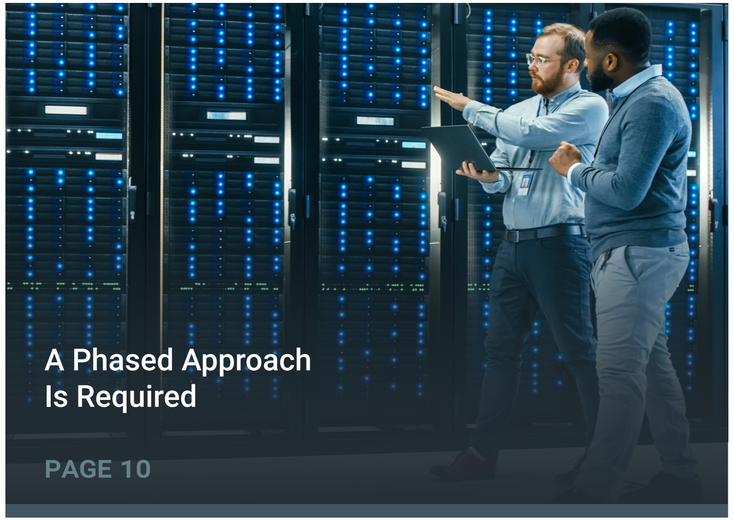
John Grady | Principal Analyst, Cybersecurity

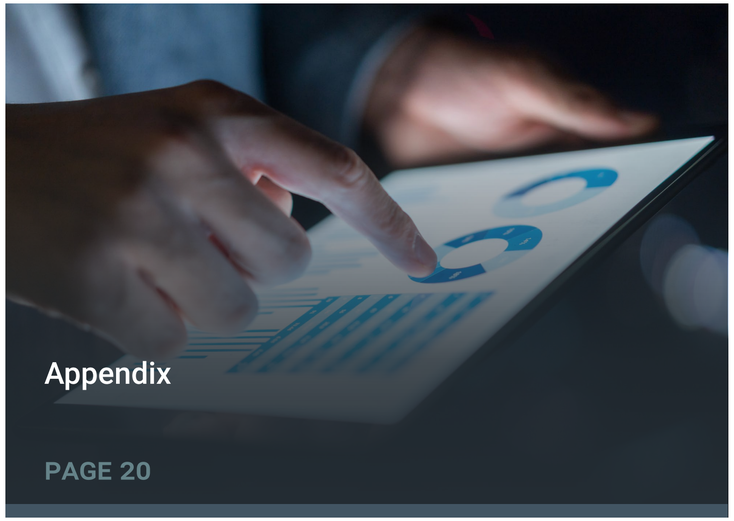
ENTERPRISE STRATEGY GROUP

JULY 2024

TABLE OF CONTENTS







The Need for Secure Access Leads to ZTNA

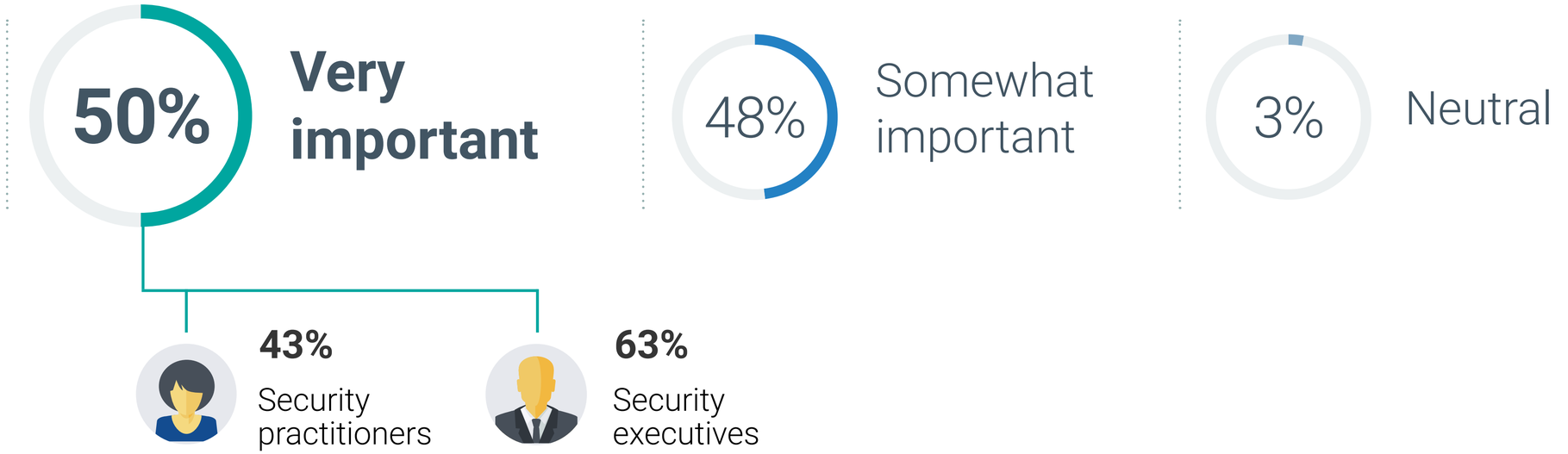
Ensuring Consistent, Secure Access Is More Critical Than Ever

Enterprise environments are much more complex than just a few years ago. The proliferation of apps and devices—coupled with changing work habits and the increasing velocity of business—make ensuring users have secure access to the internal resources they need both more important and more complex than ever.

On average, organizations estimate that ~44% of their FTEs are hybrid or remote users, while ~27% of the users accessing internal resources are third parties, and ~50% of employees access internal resources from an unmanaged device.

As a result, many organizations have recognized the importance of applying zero-trust principles to the workforce. Specifically, this means connecting users to applications rather than the broader network. In total, 98% of Enterprise Strategy Group research respondents say this practice is important. As attackers continue to exploit traditional VPNs to launch attacks, embracing a zero-trust approach for the workforce becomes even more important.

Importance of directly connecting users to applications rather than to the broader network.



98%
of Enterprise Strategy Group research respondents say **this practice is important.**

John Grady,
Principal Analyst, Cybersecurity

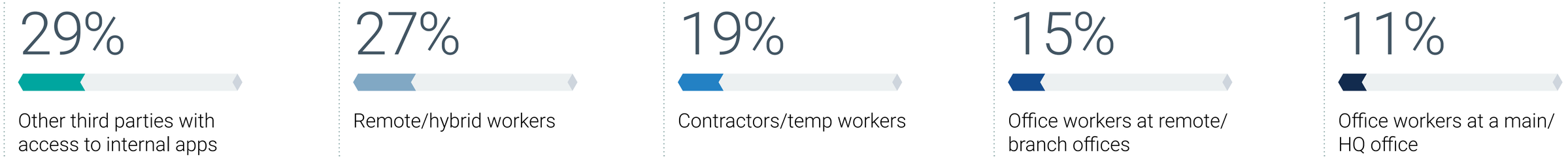
Non-office Users Are Considered the Greatest Risk

Many organizations are still trying to adequately address these new workforce realities, a fact evidenced by how our research respondents view different user groups with regard to risk.

Respondents considered groups that would be viewed as more traditional as the least risky to the organization, including office workers at headquarters (11%) and remote/branch offices (15%) as well as contractors or temporary workers (19%).

Conversely, remote and hybrid workers (27%) and other third parties (29%) top the list of the most risky user groups. These groups are most likely to access resources from outside corporate locations and/or use unmanaged devices. These factors put additional stress on traditional secure access approaches.

User groups with the greatest risk.



BACK TO CONTENTS

Shorten Time and Reduce Costs by Accelerating IT Integration to Enable Business Initiatives

Adding to the complexity is the integration required across identity, applications, and networks to securely provide the right level of access to the right user. The continued migration to cloud as well as merger and acquisition (M&A) activity are specific trends that highlight this issue. More than three-quarters of research respondents agree that these trends drive the need to accelerate integrations.

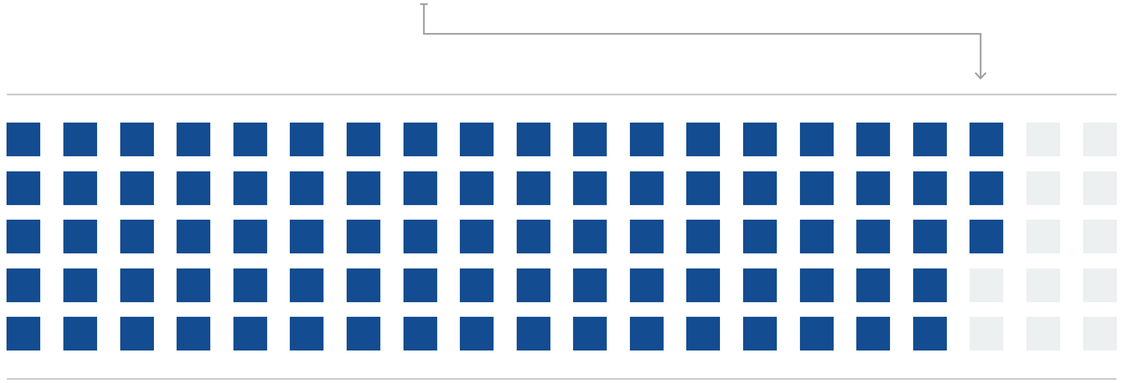
In the case of M&A, it takes time to fully integrate disparate identity management systems and network architectures. However, key users such as executives, finance teams, and sales personnel may need immediate access to critical systems before this can occur. VPNs and IP-based policies were not designed to effectively or efficiently enable access in these situations.

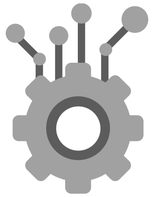
An aggregation layer that more simply secures access across any identity or application and network location—irrespective of device—can help organizations enable business initiatives quicker and more effectively.

The need for integration.

88%

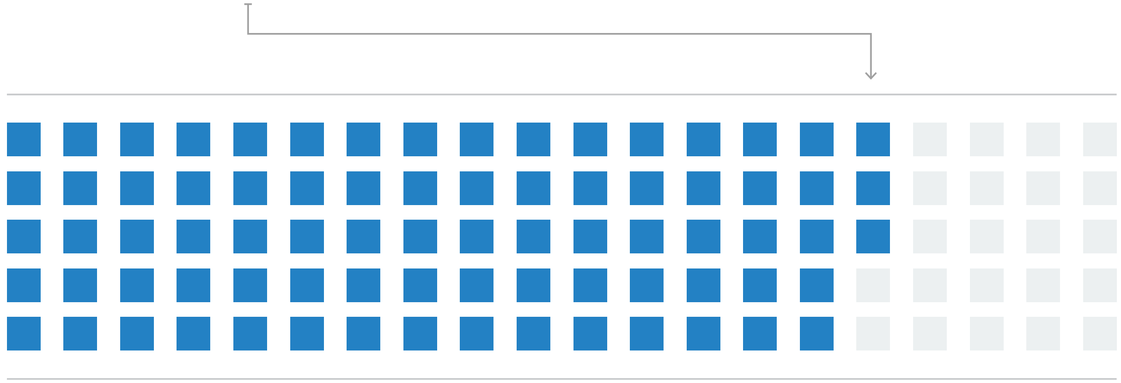
Cloud migration drives the need to accelerate IT integrations across multiple identity and app locations





78%

M&A activity is driving the need to accelerate IT integration across multiple identity providers and networks



BACK TO CONTENTS

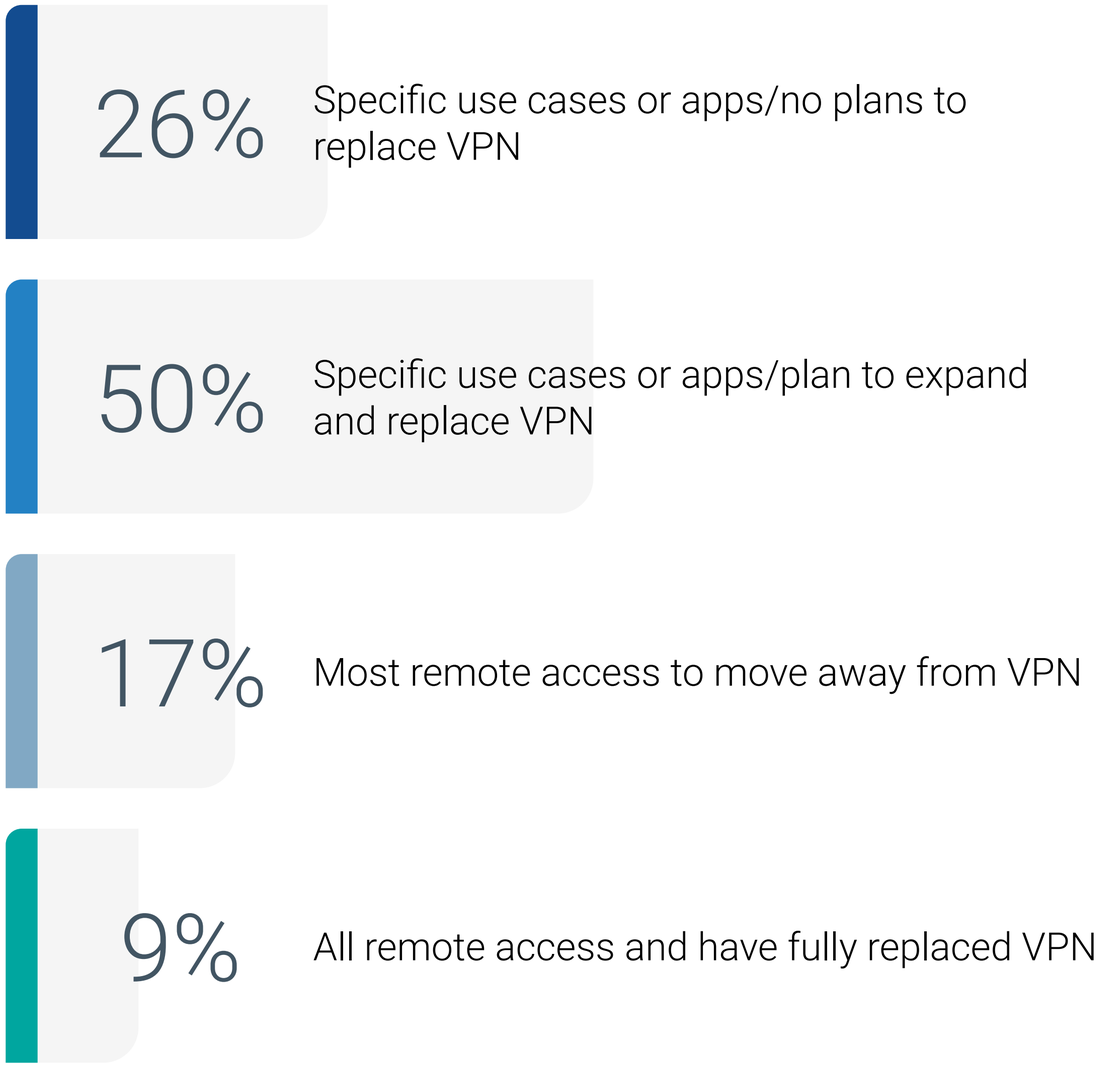
“76% of organizations **have or will replace VPN with ZTNA.”**

ZTNA Plays a Big Role, but VPN Replacement Doesn’t Occur Overnight

Zero-trust network access (ZTNA) has gotten tremendous attention in recent years as a way to address many of these issues, reduce the reliance on hardware solutions, and help security teams implement zero trust for their workforce. While only 9% of organizations surveyed say they have replaced VPN with ZTNA, an additional 67% that use ZTNA in some capacity are planning to expand usage away from VPN. In addition to better security, the cloud-delivered architecture ZTNA provides offers better scalability and flexibility compared to hardware-based VPNs.

Finally, while 26% say they do not plan to fully replace their VPN, that may ultimately change over time. Some may use a VPN plus ZTNA architecture for a period and, over time, decide to move forward with full replacement.

How organizations use ZTNA



BACK TO CONTENTS

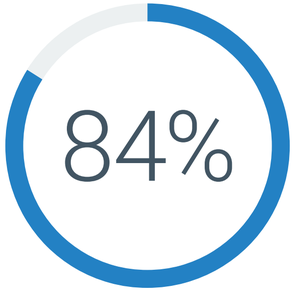
Agentless Solutions Pay Dividends

Strong Agreement That Agentless ZTNA Accelerates Zero-trust Adoption

Nearly three-quarters (71%) of respondents say that their current ZTNA tools support agentless deployment. More importantly, these organizations are seeing important benefits due to their agentless architecture. Perhaps most importantly, 84% said their agentless ZTNA deployment helped them significantly accelerate zero-trust adoption. This is critical because the faster zero trust is implemented, the more quickly risk can be reduced and value realized, building momentum to expand the initiative. Further, 85% of respondents noted that agentless ZTNA effectively addresses the use cases, users, and applications they want to cover, meaning they are able to expand coverage without deploying additional tools that use agents.

Benefits realized from agentless deployment.

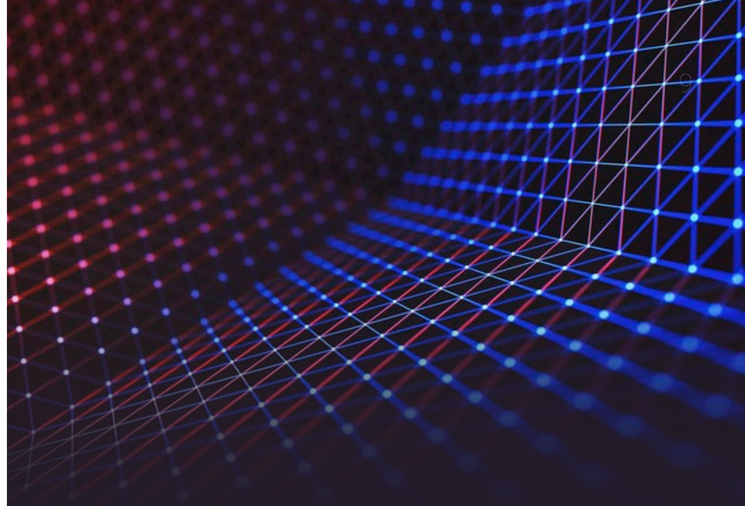
Simplified deployment, reduced admin burden & potential points of failure



Significantly accelerated zero-trust adoption

Easier scalability by eliminating individual agent installs on every device

Effectively meets our use cases and scale for desired number of users and apps



“Nearly three-quarters (71%) of respondents say that their **current ZTNA tools support agentless deployment.”**

BACK TO CONTENTS

A Phased Approach Is Required

Taking a Phased Approach to Zero Trust for Workforce Implementation

Average time expected in each phase:

The breadth of types of users, applications, and ZTNA functionality makes implementing zero trust for the workforce a journey best broken down into phases. While every organization and implementation is different, the high-level structure of each phase should remain roughly the same.

- **Phase 1,** or "Initial Rollout," would typically support a limited set of use cases and/or functionality, with the organization identifying the key priorities it wants to solve for and address these before a broader rollout.
- **In Phase 2,** or "Expansion," coverage is expanded, which could mean rolling availability out to a broader set of employees, increasing coverage across a wider set of applications, or taking advantage of additional features or capabilities.
- **In Phase 3,** or "Advancement," the initiative continues to advance, which could mean becoming broadly deployed with coverage across most employees and applications, advanced capabilities being used, and/or the project now meeting the overall goals established during planning.

On average, respondents expected it to take roughly 11 months to complete Phase 1, 15 months to complete Phase 2, and 16 months to complete Phase 3. It is important to note that many of these respondents were sharing their expectations with Phases 2 and 3, not experiences. These perceptions might be based on the use of first-generation ZTNA tools from over four years ago, before the pandemic, that did not prioritize scalability and expansion. As noted earlier, agentless ZTNA solutions can accelerate adoption and help organizations move through these phases more quickly.

BACK TO CONTENTS

Top Focus Areas for Phase 1

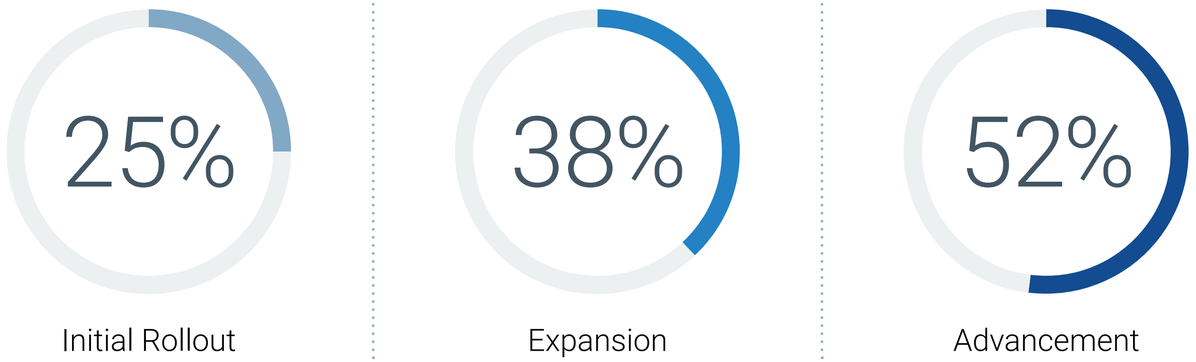
Phase 1 is arguably the most important in this process. Organizations should be focused not only on their top priorities, but also where time to value is low to help build momentum and consensus to keep the project moving forward. While starting small is important, on average, respondents indicate they will include 25% of their applications and users in Phase 1. This will grow to 38% in Phase 2 and 52% in Phase 3.

From a user perspective, sales, IT, and C-level executives are the most common focus in Phase 1. Meanwhile ERP, communication and collaboration, and file storage and sharing are the most common applications covered. This does not necessarily mean every organization should start with these users and applications, but it does provide a view into the areas many are identifying and seeing success with.

Average percentage of users and apps covered by phase.

MOST COMMON USERS:
- Sales
- IT
- C-suite

MOST COMMON APPS:
- ERP
- Communication and collaboration
- File storage and sharing



Finally, the fact that, on average, organizations expect to cover 52% of users and applications in Phase 3 again reflects where the market is overall. Very few organizations have fully replaced their VPNs at this point and may find it difficult to visualize that milestone. And many may have reached phase 3 before the pandemic increased the percentage of users and apps where remote access is applicable. Identifying vendors that have helped customers achieve this end-state can help generate buy-in on the process and final goals.

BACK TO CONTENTS

How Organizations Prioritize Types of Applications, User Groups, and Capabilities

Project Focus by Adoption Stage

Initial Rollout	Expansion	Advancement
1. **Enforce ZTAA for SaaS apps**	1. **Address specific use cases**	1. **Replace VPN fully**
2. ZTNA for private apps	2. ZTNA for private apps	2. Enforce ZTAA for SaaS apps
3. Address specific use cases	3. Unify ZTNA, SWG, CASB, etc.	3. Unify ZTNA, SWG, CASB, etc.
4. Unify ZTNA, SWG, CASB, etc.	4. Replace VPN fully	4. ZTNA for private apps
5. Replace VPN fully	5. Enforce ZTAA for SaaS apps	5. Address specific use cases

ZTNA for private apps is the #1 priority for public sector organizations.

Overall, most organizations start with a specific application focus with either zero-trust application access (ZTAA) for SaaS applications or ZTNA for private applications, expand to additional use cases, and then mature toward full VPN replacement and broader SASE/SSE implementations. It should be noted that while ZTNA is often associated with private applications, SaaS applications were the top priority in Phase 1. Zero trust can mean different things to different people, and some may consider tools such as secure web gateway (SWG) or cloud access security broker (CASB) implementing identity- and context-based access controls to SaaS applications as zero trust. But consistency is critical, which makes it important to consider vendors that can unify and reuse zero-trust access policies across any type of application.

Also noteworthy is the fact that traditional organizations (i.e., not digital natives) were more likely to unify ZTNA, SWG, and CASB in earlier stages than their counterparts. This might be because they are less likely to have migrated tools to the cloud and look at this as an opportunity to start that process or because they have acquired more individual tools and recognize this can slow down their adoption of zero trust.

BACK TO CONTENTS

Capability Focus by Adoption Stage

= Average number of capabilities added in each stage

	Initial Rollout	Expansion	Advancement
Digital-native Orgs	1.1 1. **MFA** 2. Device posture checks 2. UEBA (user risk scores) 4. DLP 5. Data control policies 5. Geolocation/time of day	2.1 1. **DLP** 2. **Data control policies** 2. Geolocation/time of day 2. MFA 3. UEBA (user risk scores) 5. Device posture checks	2.4 1. **Device posture checks** 2. **Geolocation/time of day** 3. Data control policies 4. UEBA (user risk scores) 5. DLP 6. MFA
Public Sector Orgs	1.1 1. **Device posture checks** 2. Geolocation/time of day 2. UEBA (user risk scores) 4. DLP 5. Data control policies 5. MFA	2.6 1. **MFA** 2. **Geolocation/time of day** 2. **Device posture checks** 4. Data control policies 5. UEBA (user risk scores) 5. DLP	2.2 1. **Device posture checks** 1. **Geolocation/time of day** 3. Data control policies 3. UEBA (user risk scores) 5. DLP 6. MFA

Zero trust for the workforce requires solution capabilities that organizations have not traditionally used. Just as with users or applications, security teams must consider the best order in which to implement capabilities. On average, respondents have or will add 1.4 capabilities in the Initial Rollout phase, 2.4 in the Expansion phase, and 2.1 during Advancement. While there are differences based on the type of organization (in this case, digital-native and public sector), more fundamental capabilities such as multifactor authentication and device posture checks are prioritized early on, while data loss prevention (DLP) and other data control functionality are added in later phases.

BACK TO CONTENTS

Application Types by Adoption Stage

= Average number of application types added in each stage

Initial Rollout	Expansion	Advancement
2.3	4.4	3.9
1. ERP	**1. CRM**	**1. Communication and collaboration**
2. Communication and collaboration	**2. Financial management**	**2. DevOps CI/CD workflows**
3. File storage and sharing	**2. DevOps CI/CD workflows**	**3. Project management**
3. Sales enablement	**4. Development and collaboration**	**4. File storage and sharing**
5. IT operations	5. HRM	5. IT operations
6. HRM	6. Project management	5. Sales enablement
6. Development and collaboration	7. IT operations	7. Financial management
8. Project management	8. ERP	7. Development and collaboration
9. CRM	8. File storage and sharing	7. HRM
9. Financial management	10. Sales enablement	10. CRM
11. DevOps CI/CD workflows	11. Communication and collaboration	11. ERP

Project management was the #1 application for public sector organizations.

There are a variety of application types organizations must consider on their zero-trust journey. A list with examples of each is available in Appendix II. On average, respondents expect to address 2.3 application types in Stage 1; 4.4 in Stage 2; and 3.9 in Stage 3. Among respondents, business-critical and widely used applications such as ERP, communications and collaboration, and file storage and sharing applications are most common during the Initial Rollout phase. They then expanded to applications such as CRM, financial management, and application development in Phase 2.

There were nuances across geography and organization type as well. In the UK, CRM and file storage and sharing did not enter the top five application types until the Advancement phase. While in the public sector, project management was the #1 application during Initial Rollout. It should be emphasized that this list does not imply an aggregate stack-ranking that should be adopted by most organizations, but that—as IT teams plan out their journey for which apps to take off the VPN—they should consider application ownership and other structural nuances across the organization.

BACK TO CONTENTS

Employee Groups by Adoption Stage

= Average number of employee groups added in each stage

Initial Rollout	Expansion	Advancement
2	3.8	3.7
1. Sales	**1. Legal/compliance**	**1. Information security**
1. IT	**2. Manufacturing/logistics**	**2. Finance and accounting**
1. C-suite	**2. Marketing**	**3. IT**
4. R&D Teams	**4. R&D Teams**	**4. App dev & software engineering**
5. Information security	5. App dev & software engineering	5. Marketing
5. App dev & software engineering	6. Sales	5. C-suite
7. Legal/compliance	6. C-suite	7. R&D Teams
8. Marketing	8. Finance and accounting	8. Sales
8. Finance and accounting	9. IT	8. Manufacturing/logistics
10. Manufacturing/logistics	10. Information security	10. Legal/compliance

Marketing was the #1 employee group for digital-native organizations.

With regard to user groups, respondents, on average, expect to address 2 user groups during Initial Rollout, 3.8 during Expansion, and 3.7 during the Advancement phase. Many of the groups prioritized have access to applications with sensitive internal or customer information, making zero-trust access a priority. Sales, IT, and executive teams can all be targeted by phishing and other threats as attackers seek to gain initial entry, making their focus in Phase 1 logical. The groups prioritized during Expansion (legal, manufacturing, and R&D teams) often have access to applications with sensitive proprietary information. Digital-native respondents were a bit different, with marketing taking the #1 spot in the Initial Rollout phase. Again, each organization is different and should prioritize based on their own needs, with our respondents showing what that order could look like.

BACK TO CONTENTS

User Personas by Adoption Stage

Initial Rollout	Expansion	Advancement
1. Developers or IT admins with privileged system access 2. Contractors or third parties on unmanaged devices 3. Contractors or third parties on managed devices 4. Employees on unmanaged devices	1. Employees on unmanaged devices 2. Contractors or third parties on managed devices 3. Developers or IT admins with privileged system access 4. Contractors or third parties on unmanaged devices	1. Contractors or third parties on unmanaged devices 2. Contractors or third parties on managed devices 3. Developers or IT admins with privileged system access 4. Employees on unmanaged devices

Contractors on unmanaged devices was the #1 user type for digital-native organizations.

Organizations also must consider the riskiest user personas, including third parties and employees on unmanaged devices. But at the top of the list among our respondents were developers or IT admins with privileged access. This makes sense, as these users are more likely to be using SSH, RDP, or other protocols—which grant a much deeper level of system access—as well as the secret management risks that come with these roles. When unmanaged devices come into play, provisioning VPN client software can lengthen onboarding and still leave the organization open to risk. Similarly, adding third-party users to identify providers requires extra work that takes time. In all these areas, agentless ZTNA solutions can simultaneously help reduce risk and shorten the time needed to provide secure access to these user personas.

BACK TO CONTENTS

Conclusion

Organizations have high expectations when it comes to implementing zero trust. Reducing incidents and data breaches as well as improving the efficiency of security operation centers rate highly, but reducing costs and improving employee productivity and satisfaction are also top of mind. Organizations clearly need solutions that can deliver these benefits—strong security and a seamless experience for users—but they must focus on shortening time to value through risk and cost reduction. Agentless ZTNA solutions provide this by helping security teams more efficiently and effectively roll out coverage across different users and applications. Further, organizations seeking to implement zero trust for the workforce should consider vendors that can help prioritize the projects, capabilities, application types, employee groups, and user types to focus on in each phase.

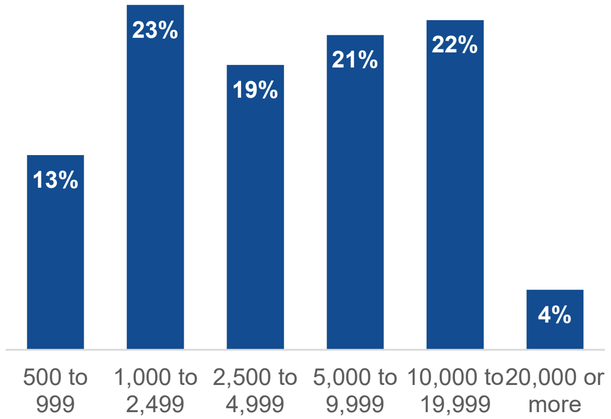
APPENDIX I: RESEARCH METHODOLOGY AND RESPONDENT DEMOGRAPHICS

To gather data for this report, Cloudflare commissioned Enterprise Strategy Group to conduct a comprehensive online survey of 200 senior IT security decision-makers knowledgeable about their organization's approach to securing user access to corporate applications and resources. Organizations represented span traditional, digital-native, and public-sector organizations across North America (U.S. and Canada), and Europe (United Kingdom). The survey was fielded between March 6, 2024, and April 3, 2024.

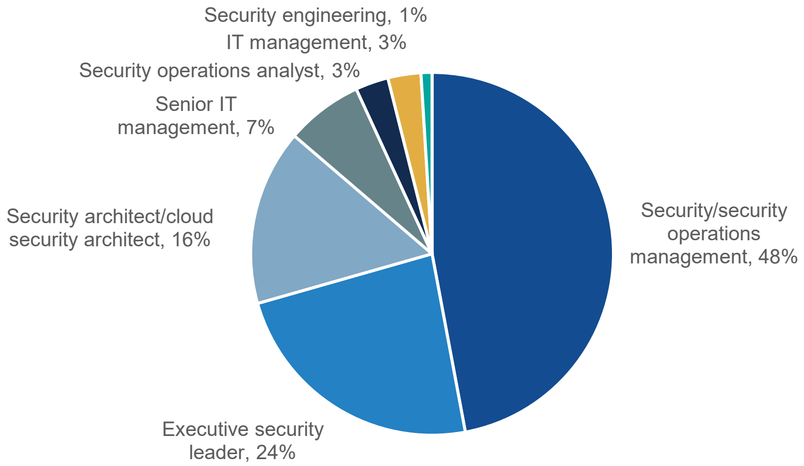
All respondents were offered an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding, and the margin of error for this sample size at the 95% confidence level is + or - 7 percentage points.

The following figures detail the demographics and firmographics of the respondent base.

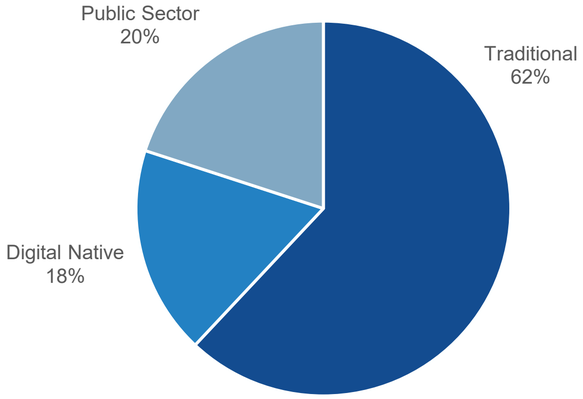
Respondents by Number of Knowledge Workers



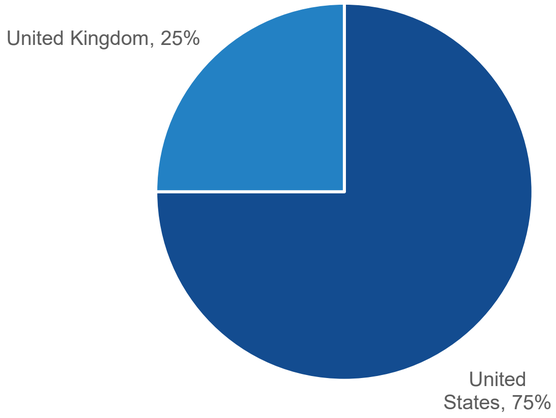
Respondents by Job Title/Level



Respondents by Org Type



Respondents by Country



BACK TO CONTENTS

APPENDIX II: GLOSSARY OF APPLICATION TYPES AND EXAMPLES

Communication and collaboration
- Microsoft 365
- Slack

CRM
- Hubspot
- Salesforce

ERP
- Infor
- SAP

Development and collaboration
- Asana
- Trello

DevOps CI/CD workflows
- Jenkins
- Jira

Financial management
- Expensify
- QuickBooks

File storage and sharing
- Box
- Dropbox

HRM
- Insperity
- Workday

IT operations
- ServiceNow
- Zendesk

Project management
- Monday
- Smartsheet

Sales enablement
- Highspot
- Seismic

BACK TO CONTENTS

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.