IDENTITY IS THE ZERO TRUST KEYSTONE
A Global Survey of Security and IT Professionals

October 2021
Introduction

This paper reviews key findings from a global primary research survey focused on understanding how the security perimeter has changed due to work from home trends, anywhere operations and what companies are most concerned with protecting. The research specifically investigated what capabilities are in place to control access to these critical resources.

The research also focused on capturing a real world view of Zero Trust adoption. The report covers which solutions have typically been deployed, current level of success, benefits received, top challenges encountered and what is preventing some companies from even starting a Zero Trust security model.

Executive Summary

This research finds that work from home (WFH) trends have changed the security threat landscape with increased risk on employee devices, endpoints, and data. Companies remain keenly focused on protecting business applications, but findings indicate that supply chains and business applications that rely on bots or partners are high risk due to poor access management practices. In fact, more than 5 out of 10 surveyed said their identity access controls strategy relies on manual processes, which contributes to less than half of companies knowing who has access to cloud resources, endpoint devices, and unstructured data.

Anywhere operations, increased cloud use, and growing security attacks are leading 92% of companies to incorporate a Zero Trust security model. Zero trust is expected to deliver improved visibility, earlier threat detection, fewer incidents, and improved remediation. Those benefits have led to 42% of companies already deploying Zero Trust solutions backed by significant budget allocation as a majority have dedicated 25% or more of their security budget to Zero Trust. Nearly all (97%) agree identity is a foundational component of a Zero Trust security model. 99% of those deploying Zero Trust stated it is already improving their security effectiveness. The top technical challenge during implementation is integration of the solutions which form their Zero Trust defense. Zero Trust expertise is also in short supply and was the leading reason companies haven’t started Zero Trust. The way businesses work has changed, and that is reflected in the security landscape both from new threats and new defenses needed. Zero trust is an excellent security addition but companies need expertise and solutions that integrate more easily.
IDENTITY IS THE ZERO TRUST KEystone
A Global Survey of Security and IT Professionals

Key Findings

- **Shifting Work Patterns Result in New Risks Old Approaches Can’t Defend**
  - Work from home results in risk shift to employee devices, numerous locations, and data
  - 55% still rely on manual processes to adjust access when IT environments change
  - Less than half of companies know who has access to cloud resources and unstructured data

- **Zero Trust being Rapidly Adopted with Early Success**
  - 92% of companies planning on Zero Trust with 45% having already started
  - 97% state identity is a foundational component of a Zero Trust security model
  - 99% of Zero Trust initiatives are already successful at improving security

- **Early Days for Zero Trust, and Companies Looking for Expertise**
  - Less than 40% of companies have all key solutions to form an effective Zero Trust security defense
  - Zero Trust top implementation challenge is integrating solutions
  - Lack of expertise leads barriers to Zero Trust adoption
Detailed Findings
Work from Home Results in Risk Shift

The rapid migration of the work from home (WFH) employee was a forced reaction to the pandemic. However, WFH model will continue to be pervasive going forward and notes a key inflection point for businesses. This shift in worker location has also had a direct impact on company’s security risk landscape. When security and IT professionals were asked what resources were most at risk, WFH employee devices topped the list at 64%. End point devices (55%) followed indicating risk not only for devices at home but IoT devices as well. Now that employees are out of the office, traditional access to data stores has changed not only due to WFH employees but from anywhere operations, providing yet another risk vector. The quantity of devices that now extend the network outside of traditional company facilities is staggering.

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>At Risk Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work from home employee devices</td>
<td>64%</td>
</tr>
<tr>
<td>Endpoint devices (IoT)</td>
<td>55%</td>
</tr>
<tr>
<td>Data stores (SharePoint, network drives, etc.)</td>
<td>53%</td>
</tr>
<tr>
<td>Corporate network</td>
<td>51%</td>
</tr>
<tr>
<td>Collaboration portals (Zoom, WebEx, MS Teams, Slack, etc.)</td>
<td>39%</td>
</tr>
<tr>
<td>Corporate applications (ERP, CRM, SFA, etc.)</td>
<td>38%</td>
</tr>
<tr>
<td>SaaS applications</td>
<td>30%</td>
</tr>
<tr>
<td>IaaS/PaaS environments</td>
<td>29%</td>
</tr>
</tbody>
</table>
IDENTITY IS THE ZERO TRUST KEYSONE
A Global Survey of Security and IT Professionals

Dimensional Research    |    October 2021

Business Applications Remain the Top Focus for Security and Access

Among the resources organizations are most concerned with protecting access to, critical business applications were at the top of the list at 75%. Structured data stores (60%), often feeding the critical business applications, took the second spot. Then, as discussed previously, WFH devices (58%) and the data they access (44%) represent the next set of resources that are critical to control access to. Cloud environments filled out the next two spots with SaaS at 44% and IaaS/PaaS at 43%. And endpoint devices (40%) takes the last spot. This chart represents the huge diversity of resource types and locations that require strict access control is challenging.

SailPoint Zero Trust Solution

SailPoint Identity Security helps organizations adopt Zero Trust by enabling you to easily discover, manage and secure all identities and their access to technology resources. Gain a 360-degree view of ALL user access, their entitlements and attributes in real time, enabling you to make accurate decisions about who should have access to which resources — and when. As workers join, change roles, or leave the organization, access is automatically granted, updated or revoked.

SailPoint also enables you to enforce the rule of “least privilege” with automated role management, permissions and access policy logic. Grant exactly the right amount of access for every single role and prevent toxic access combinations that lead to fraud or theft of data.

Additionally, SailPoint keeps your Zero Trust security profile strong, by giving you the ability to continuously monitor, analyze and proactively respond to changes – or new risks – faster than ever. Get deeper visibility into user access including access trends, access approvals, roles and relationships with AI-driven insights. Adjust access controls as your business evolves or as new threats emerge. Measure the efficacy of your access controls; and leverage custom workflows, APIs, and event triggers to integrate identity events seamlessly with other Zero Trust security solutions. To learn more, visit sailpoint.com/solutions/zero-trust.
Companies Lack Access Control for Key Users

With such stringent requirements to protect numerous critical resources, it is not surprising to see 99% of companies managing access by user types. Perhaps expected, 84% of companies can manage workforce access followed by controls for software (68%) and closely followed by contractors (67%). A common effect of the pandemic is increased reliance on the supply chain, but this leads to the surprising finding that barely over half of companies (55%) can control access to supply chain apps which often integrate directly into key business applications. Also alarming is that only a quarter of companies (25%) control access by bots. While bots can be the instruments of AI/ML, if a malicious attack utilized bots, 3 out of 4 companies would be completely vulnerable.
Companies Rely on Manual Processes When IT Environments Change

When considering the number of employees, devices, applications, services, bots, and cloud environments, it can be daunting to keep control of it all. And the reality is most IT environments are in constant change, exacerbating the challenge. Technology professionals were asked about automated solutions that are used to manage the tremendous volume of change. While it was positive to see 69% of companies with some automatic solutions for managing access policies, it was shocking to see manual processes (55%) were in the second spot. This is clearly setting the stage for a scaling problem and the ability to miss necessary changes and updates needed to ensure enterprise security.
Most Companies Operating in the Dark with Access Privileges

While the previous question focused on access control, the research turned to simply asking if companies know “who has access to what.” This question revealed some understanding of how their access is actively managed - not only who is being granted access rights, but who has which privileges and who is having them removed. Barely over half of the companies could definitively identify who had access to critical business applications (69%) and their corresponding data (53%). Surprisingly, less than half of companies accurately know who has access to cloud environments: SaaS (49%) and IaaS/PaaS (46%). Earlier in this report end points were identified as the 2nd most at-risk item, yet barely over a third of companies actually know who has access to them. These findings are starting to paint a disturbing security picture of inconsistencies as companies articulate key risk resources but lack controls for access and often don’t know who already has access.
Most Companies Turning to Zero Trust

Given the preceding access disconnects and the growing number of critical resources that are outside the traditional data center and network, fueled by the WFH employee, it is not surprising that Zero Trust is being heavily adopted by 92% of security and IT professionals. In fact, 45% of the companies surveyed already are using a Zero Trust security approach today.

Anywhere Operations and Growing Threats Lead Companies to Zero Trust

Zero Trust adoption is being driven by increasing security threats (75%), which are likely attributed to hackers looking for easy entry with WFH employees having access to key applications and data. This risk is seen as highly related to anywhere operations (68%) not only driven by WFH employees but growing public cloud reliance. In fact, the rapid adoption of the cloud came in third (56%) as another key reason technology professionals are looking to Zero Trust to add more control and security. Also tied at 56% is the need to manage new types of identities introduced by IoT devices, bots, and more, which we have already found in this report to create access problems for most companies.
IDENTITY IS THE ZERO TRUST KEYSTONE
A Global Survey of Security and IT Professionals

97% State Identity Is Critical Component of Zero Trust
A question from another Dimensional Research project in 2021, titled “Trends in Digital Security Identities,” asked Security and IT professionals specifically about Identity Management’s role within the Zero Trust security model. 97% of those surveyed stated that identity is a key part of Zero Trust. This provides more evidence of why Zero Trust is being rapidly adopted to not only provide increased security but to also deliver automated identity access management, governance, and control.

Zero Trust Initiatives Already Successful at Improving Security
Adoption of Zero Trust may have been thrust forward in popularity due to the pandemic and WFH employees, so the research sought to cut through the hype and directly inquire if Zero Trust is actually delivering business value. Overwhelming, 99% of companies indicate that Zero Trust has been successful already and is delivering increased security for their business.
Most Companies Have an Immature Zero Trust Security Defense

While companies report already receiving benefits from Zero Trust, security and IT professionals were asked what solutions have been deployed thus far to gain insight into the maturity of current Zero Trust deployments. While the chart below provides the list of solutions deployed, perhaps the key takeaway is that less than 40% of companies have all key solutions deployed that are typically associated with a fully mature Zero Trust security model. While initial security improvements have been overwhelmingly positive, a large majority of companies still have additional tasks and associated benefits ahead of them.

![Chart showing the percentage of companies implementing various Zero Trust solutions](chart.png)
Integration, Culture Change and Expertise Shortage Impede Zero Trust

Given the majority of companies were still working to deploy all the key solutions of a Zero Trust security model, the research focused on understanding which hurdles were impeding companies. Leading the list of challenges was difficulty integrating the different solutions (69%) and is perhaps the most compelling finding of why customer’s Zero Trust initiatives were still lacking key solutions. But just in second spot, at 65%, was the need to change culture and habits. This trend was touched on earlier in this report where key resources were at risk, yet identity controls were not aligned or properly managed. Given this new world of WFH, driving Zero Trust adoption, it is no surprise that 51% of companies lack the necessary expertise. Noted earlier in this report, identities often are manually updated which leads 49% to say they have to validate whether identities are actually accurate. Rounding out the findings were the usual suspects: lack of budget (46%), time consuming (45%), and lack of best practices (39%).

![Bar Chart: In your experience, what are the challenges with implementing a Zero Trust security model?]

- Integrating the different solutions: 69%
- Changing our culture (habits, thinking, etc.): 65%
- Lack of expertise: 51%
- Ensuring user identities are accurate: 49%
- Budget: 46%
- Time consuming: 45%
- Lack of industry best practices: 39%
- There are no challenges to implementing a zero trust security model: 2%
Advanced Features Significantly Improve Meeting Productivity

For those 8% who indicated their company is not implementing a zero trust model, we asked them why not. Leading the top reasons is lack of expertise, which was noted previously and a legitimate concern and reason to delay or seek assistance. The second leading reason represents an opinion that it is just another overhyped technology fad, even though the earlier findings of 99% indicating improved security clearly provides evidence that is not the case. Rounding out the top 3 is lack of budget (28%). Tied at 4th at 24% are perceived solution immaturity and that Zero Trust is a complicated security model. At the bottom (20%) is perhaps the most rational business reason that their business model just doesn’t warrant that level of security. However, most of these objections be could addressed by seeking experience.
Conclusion

This research finds that the operate anywhere and WFH models have driven a significant change in the security landscape and often place key resources outside the data center, work facilities or traditional network. This makes protecting key applications, devices, and data more challenging. While companies have employed some access controls, they remain misaligned on their critical resources and lack clearly comprehensive controls for all identities that have access to them. Furthermore, many access polices are updated manually, leaving access privileges out of date and thus resources at risk.

These challenges have led most companies to adopt a Zero Trust security model which is founded on proper access and identity management. While essentially all (99%) companies have already enjoyed success with their initial Zero Trust deployments, most remain fairly immature, needing to implement other solutions to build out a comprehensive security model. Standing in their way is difficulty integrating solutions and needing an experienced guide to not only create culture change but to help establish processes based on best practices. In fact, those challenges are the top reasons why some companies have delayed their adoption of Zero Trust.

The reality is the security landscape has been forever altered and is significantly more complex, often by thousands or tens of thousands of new devices which have to be protected and assigned proper access. It’s not going to get easier, and it’s not going to get simpler. Appropriate access needs to be granted or redacted when situations change and this needs to be automatic, not just for employees but for consultants, supply channels, partners, bots, services, and other applications. Often security experts say the biggest exposure is simply not following their own rules and enforcing their own processes and policies, and this is where a fully implemented Zero Trust model shines.

Survey Methodology

Security and IT professionals at enterprise companies representing all seniority levels were invited to participate in a survey on their company’s security and identity practices and as well Zero Trust model adoption.

A total of 315 qualified participants completed the survey. All participants were responsible for security, identity, or IT operations. Participants were from 5 continents balancing North America, Europe and Middle East, and Asia Pacific regions. The survey was administered electronically, and participants were offered a token compensation for their participation.
About Dimensional Research
Dimensional Research provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business.

For more information, visit www.dimensionalresearch.com.

About SailPoint
SailPoint is the leader in identity security for the modern enterprise. Harnessing the power of AI and machine learning, SailPoint automates the management and control of access, delivering only the required access to the right identities and technology resources at the right time. Our sophisticated identity platform seamlessly integrates with existing systems and workflows, providing the singular view into all identities and their access. We meet customers where they are with an intelligent identity solution that matches the scale, velocity and environmental needs of the modern enterprise. SailPoint empowers the most complex enterprises worldwide to build a security foundation grounded in identity security.