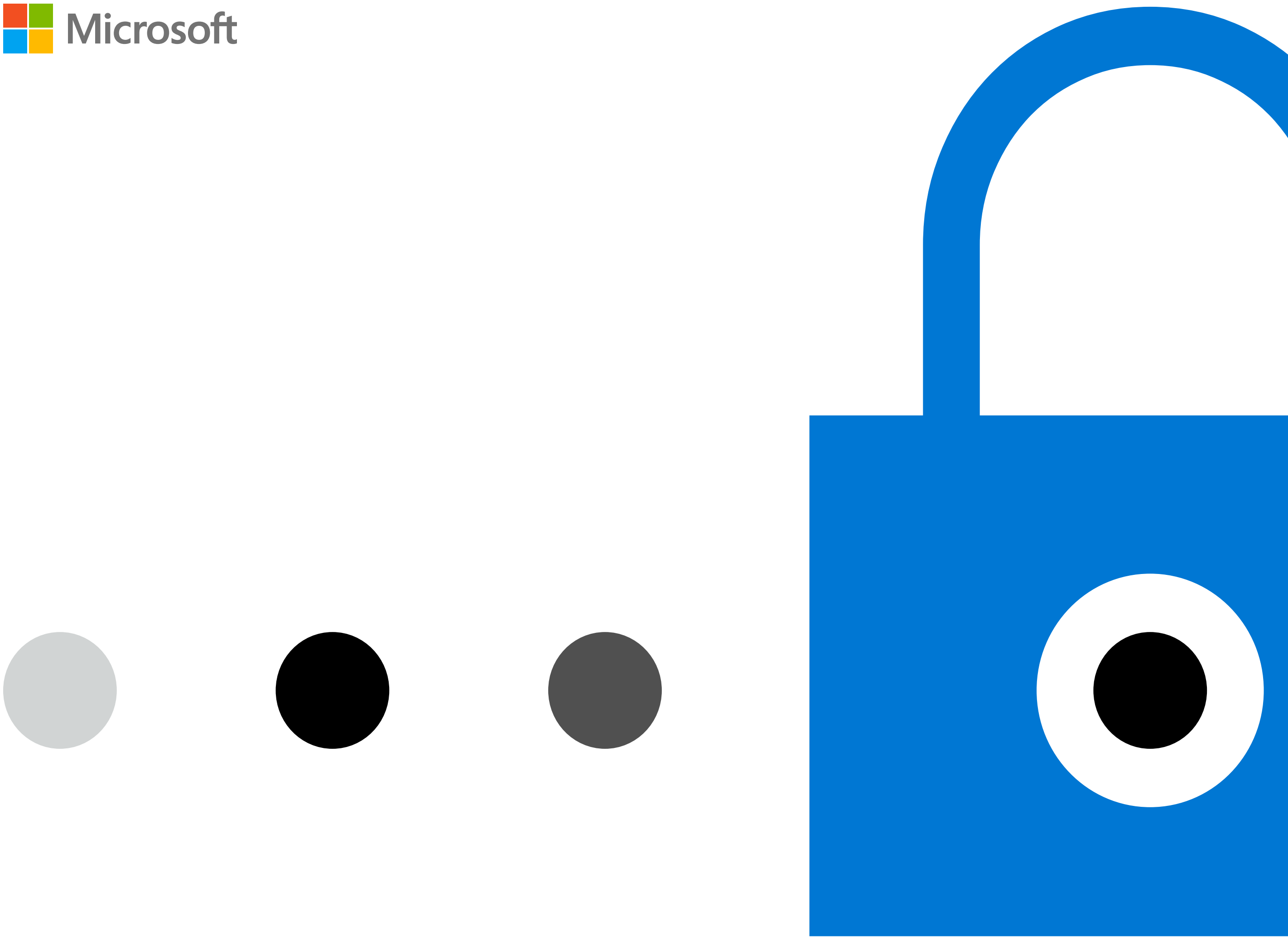


Examining Zero Trust

An executive roundtable discussion

Around the roundtable

On December 1, 2020, Microsoft and Cloud Security Alliance (CSA) hosted a virtual executive roundtable to hold a real-world dialog and extend the vision of Zero Trust security. Ann Johnson, CVP, Security, Compliance, and Identity Business Development at Microsoft, facilitated the roundtable, which was attended by 10 executive security leaders from prominent energy, finance, insurance, and manufacturing companies. These leaders shared their insights as well as lessons learned on the journey toward Zero Trust.

Key insights

During the roundtable, leaders discussed the importance of information security to digital transformation. They shared their own experiences and real-life examples of building a strategic approach to information security, as well as adopting the fundamental elements of Zero Trust to improve their overall information security postures.

Within this context, attendees focused on the following topics:

- Thinking beyond perimeter security and moving to a holistic security approach.
- Starting small in the Zero Trust adoption journey, addressing—and then building on—discrete aspects of information security.
- Improving the adoption of Zero Trust security across an entire organization.

The Zero Trust strategy for modern security

Zero Trust security is not a product or solution.

It is a broader strategy for modern security that adapts to the complexity of today’s business environment, embraces the mobile workforce, and protects people, devices, apps, and data wherever they’re located. Unlike traditional approaches that attempt to force all assets onto a “secure and compliant” network, Zero Trust focuses on the security and compliance of assets regardless of their physical or network location.

It replaces the belief that everything behind the corporate firewall is safe, instead assuming breach and verifying each request as though it originates from an uncontrolled network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches the importance of “never trust, always verify.”

A Zero Trust strategy must first deliver on fundamental principles and threat protection, and then provide secondary benefits like simplification.

Foundational benefits	
Better contains security breaches	32%
Increases the speed of threat detection and remediation	30%
Better protects customers' data	29%

Source: Microsoft Zero Trust Survey 2020

Everything from the user’s identity to the application’s hosting environment is used to prevent breach. Micro-segmentation and least privilege access principles are applied to minimize lateral movement while rich intelligence and analytics help to improve visibility, drive threat detection, and enhance defense by identifying what happened, what was compromised, and how to prevent recurrence.

Elements that drive Zero Trust adoption

A Zero Trust framework requires implementing controls and technologies across all foundational elements: identities, devices, applications, data, infrastructure, and networks. Each of these elements is a source of signal, a control plane for enforcement, and a critical resource to be defended. As such, each is also an important area to focus investments.

Consider identity the new perimeter

In the course of the conversation, the roundtable surfaced an essential realization: Organizations must first focus on strengthening their user authentication and identity verification, as most security breaches involve the theft of credentials.

Because lapses in cyber hygiene amplify risk for individual employees and the entire organization, comprehensive identity management is essential for helping to ensure only authorized users can access business data.

Consider identity the new perimeter

Use identities to control access

Identities—representing people, services, and IoT devices—are the common denominator across networks, endpoints, and applications. In a Zero Trust security model, they function as a powerful, flexible, and granular way to control access to data. When any identity attempts to access any resource, the management process should:

- Verify the identity with strong authentication.
- Ensure access is compliant and typical for the identity.
- Confirm the identity follows least privilege access principles.

> One participant emphasized that by starting with strong identity and access management: "We lost the perimeter. The new perimeter is identity, and you need a strong identity that is validated....That is where the project started; since you can't do access management manually, it has to be an automated process. Have good automation and good logins to make sure it's working as it should be."

Consider identity the new perimeter

Elevate authentication

You can substantially improve your organization's information security posture simply by incorporating multifactor authentication (MFA) or continuous authentication into your identity management strategy. Emphasizing the power of this approach, one roundtable participant noted that by extending identity management with continuous authentication profiles, their organization can now validate identity even when a user's IP address or routine behavior pattern changes.

In relation to establishing identity with field operational technology, one participant was asked which is the more critical identity to address: humans or machines? He answered: "Both. You need humans, especially technicians, to go out into the field and enable multifactor authentication. In the past, it was difficult to do, but it is much easier now. Then the biggest issue is machine-to-machine authentication. How do you have the second factor when you don't have a human to challenge [it]?"

Consider identity the new perimeter

Incorporate passwordless authentication

As Zero Trust evolves, it's becoming more common to use biometrics and other innovations as part of a modern approach to information security. Another form of MFA, passwordless authentication replaces the traditional password with a secure alternative. This type of authentication requires two or more verification factors that are secured with a cryptographic key pair. When registered, the device creates a public and private key. The private key can only be unlocked using a local gesture, such as a PIN or biometric authentication. Users have the option to sign in directly through biometric recognition—such as fingerprint scan, facial recognition, or iris scan—or with a PIN that's locked and secured on the device.

When asked about the impact of passwordless authentication on the effectiveness of Zero Trust, one participant responded: "I think it increases it. After a year of Microsoft Windows Hello proof of concept, we are now rolling out corporate-wide. Zero Trust will only work if it is transparent to the end user. You have to make it easy and transparent. If you want to authenticate every five minutes or every second, that's fine, as long as the end user doesn't have to do anything—as long as you can validate through other methods. For example, the endpoint can be one of the factors for MFA."

Segment your corporate network

Network segmentation was a topic of intense discussion during the roundtable. One participant shared the belief that when you do a lot of segmentation, things start to break. When you start designing various parts and segmenting the perimeter network, you no longer have a flat IT network. This is a pain point for business IT because firewalls represent early segmentation, and this results in inherent difficulties with development and testing. Ultimately, the IT team becomes more reliant on security teams to fix networking, connectivity, and access issues.

Yet, in a mobile- and cloud-first world, all business-critical data is accessed over network infrastructure. Networking controls provide critical functionality to enhance visibility and help prevent attackers from moving laterally across the network. This means organizations should continue to segment networks and conduct deeper in-network micro-segmentation, in addition to deploying real-time threat protection, end-to-end encryption, monitoring, and analytics.

> One participant noted: "We began with micro- and macro-segmentation of our network. We started in the datacenters and offices, which led to application segmentation with the capability to restrict users to a given app stack as they are coming over in VDI or VPN. So, we can segment [users] in a way that they do not get access to carte blanche once they land on our VPN."

Further in the discussion about segmentation, participants were asked if the Zero Trust framework can extend to on-premises assets, as well, or if it's better just for cloud environments. In response, one participant shared their experience as follows: "For us, it started with on-premises and will still be there since we need it for the micro-segmentation for lateral movement protection, and so on. Those things are not changing; we are just stretching it out to the cloud now. For financial services, we are never going to have it all on the cloud; we'll always have a mix of on-premises and cloud....[We're] going to have to figure out how to tend all the various perimeters and get the paradigm stretched across the board."

Another participant stated: "I started with more micro-segmentation and NAC, as well. I really didn't trust the next VLAN. You had to hop through a firewall; if you weren't authorized, you couldn't get there. Now we had to really make sure they could go through segment to segment, and they could go bidirectionally, unidirectionally. That's where it really started."

Secure your devices

While most would agree that modern organizations must navigate an incredible diversity of endpoints accessing data, one roundtable participant voiced a concern that devices, themselves, have been largely ignored. Not all endpoints are managed or even owned by the organization, leading to different device configurations and software patch levels. As previously noted, Zero Trust adheres to the principle of "never trust, always verify." In terms of endpoints, this means always verify all endpoints—including not only contractor, partner, and guest devices, but also apps and devices employees use to access work data, regardless of device ownership.

With the Zero Trust model, the same security policies are applied whether the device is corporate owned or personally owned, and whether the device is fully managed by IT or only the apps and data are secured. The policies apply to all endpoints—PC, Mac, smartphone, tablet, wearable, or IoT device—wherever they are connected, be it the secure corporate network, home broadband, or public internet.

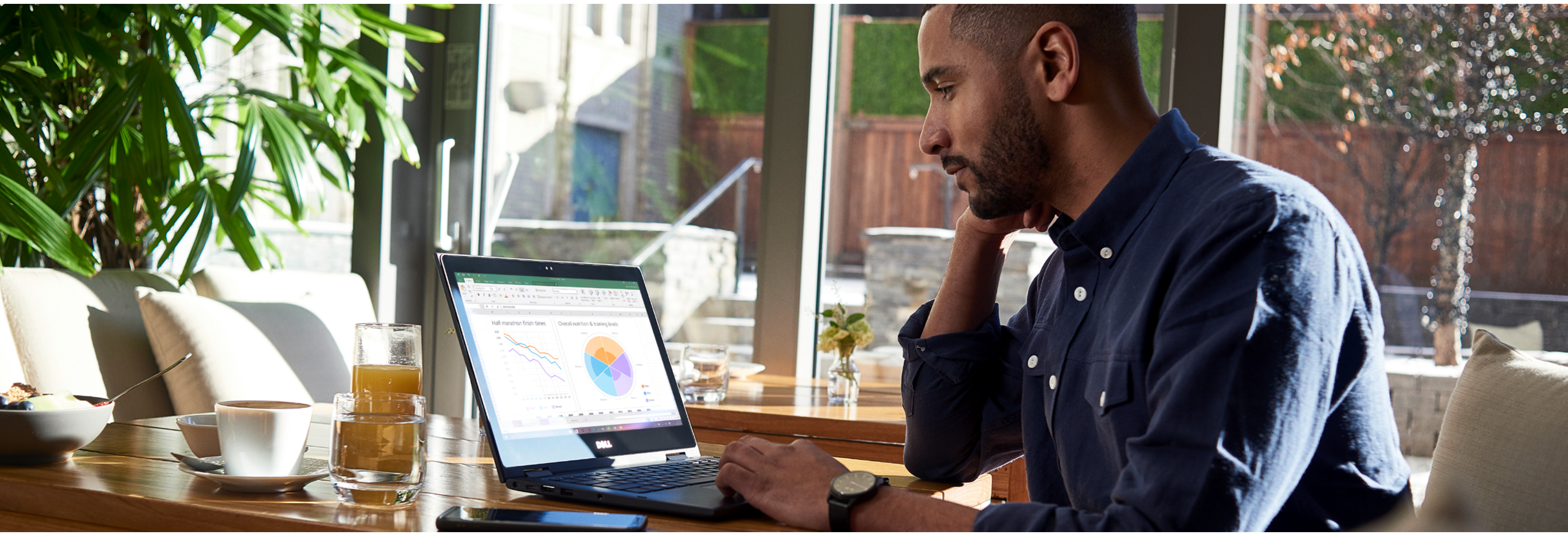
In the conversation about device security, one participant provided an especially cogent example: "In a BYOD world, the device is the explosive piece. If you allow unpatched devices to connect to your network, it is, in essence, walking into your base with live ordinance, and it can go bad quickly. Why wouldn't you test outside to begin with? Over time, people get used to being prompted to make things secure (like patch devices), and it becomes an expectation. The user will become better at expecting those reminders and securing the device."

Segment your applications

Of particular note, some roundtable participants drove the conversation specifically to their concerns about application-level security. They stressed that having right-sized access to applications, whether through SaaS or in datacenters, plays a crucial role in the successful implementation of a Zero Trust strategy.

Indeed, to get the full benefit of cloud apps and services, organizations must find the right balance between providing access and maintaining control to ensure that apps, and the data they contain, are protected. Controls and technologies should be applied to discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, restrict user actions, and validate secure configuration options.

> While discussing the journey toward Zero Trust, one participant shared their thoughts around application security: “It is becoming easier and more achievable to have segmentation between the applications. Being able to provide excessive privileges/role-based access is becoming part of the policy engine. The application piece of the puzzle seems to be solving itself more intelligently as time goes on. This approach gets validated every time I hear an end user is able to dial in on the problem.”

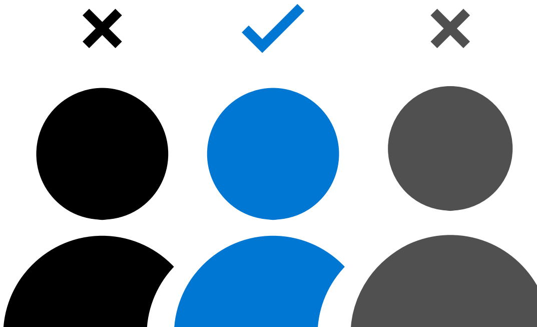


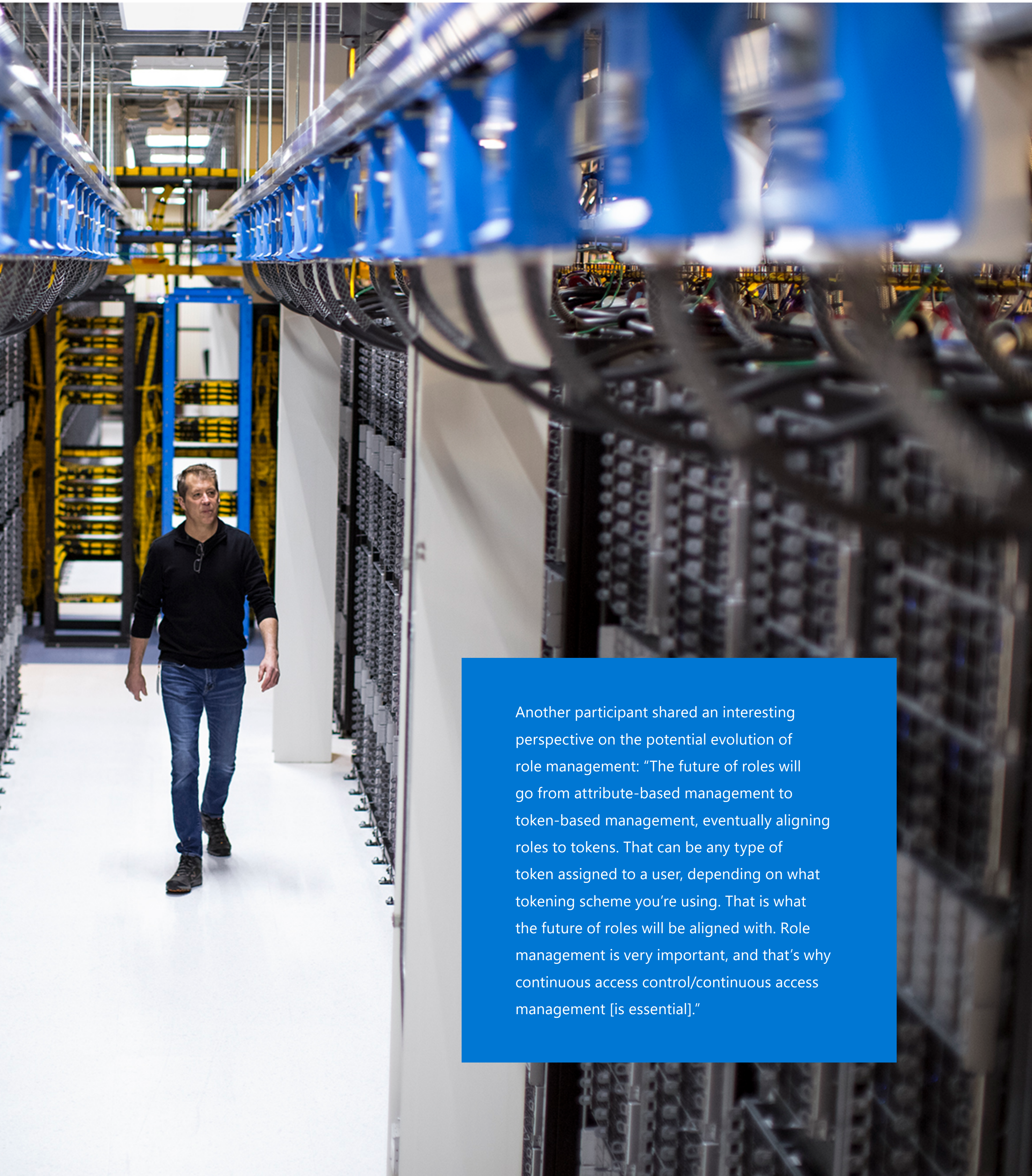
Define roles and access controls

Tackling today's most immediate issues, the roundtable spent time considering the rapid rise of remote work. With most employees now working remotely, organizations must consider alternate ways of achieving modern security controls. One participant focused squarely on operations, stating that managing user roles with policies is a key piece of the information security puzzle. This idea was then extended to include the necessity of effective role management—and tying roles to policy as part of authorization, single sign-on (SSO), passwordless access, segmentation, and so on.

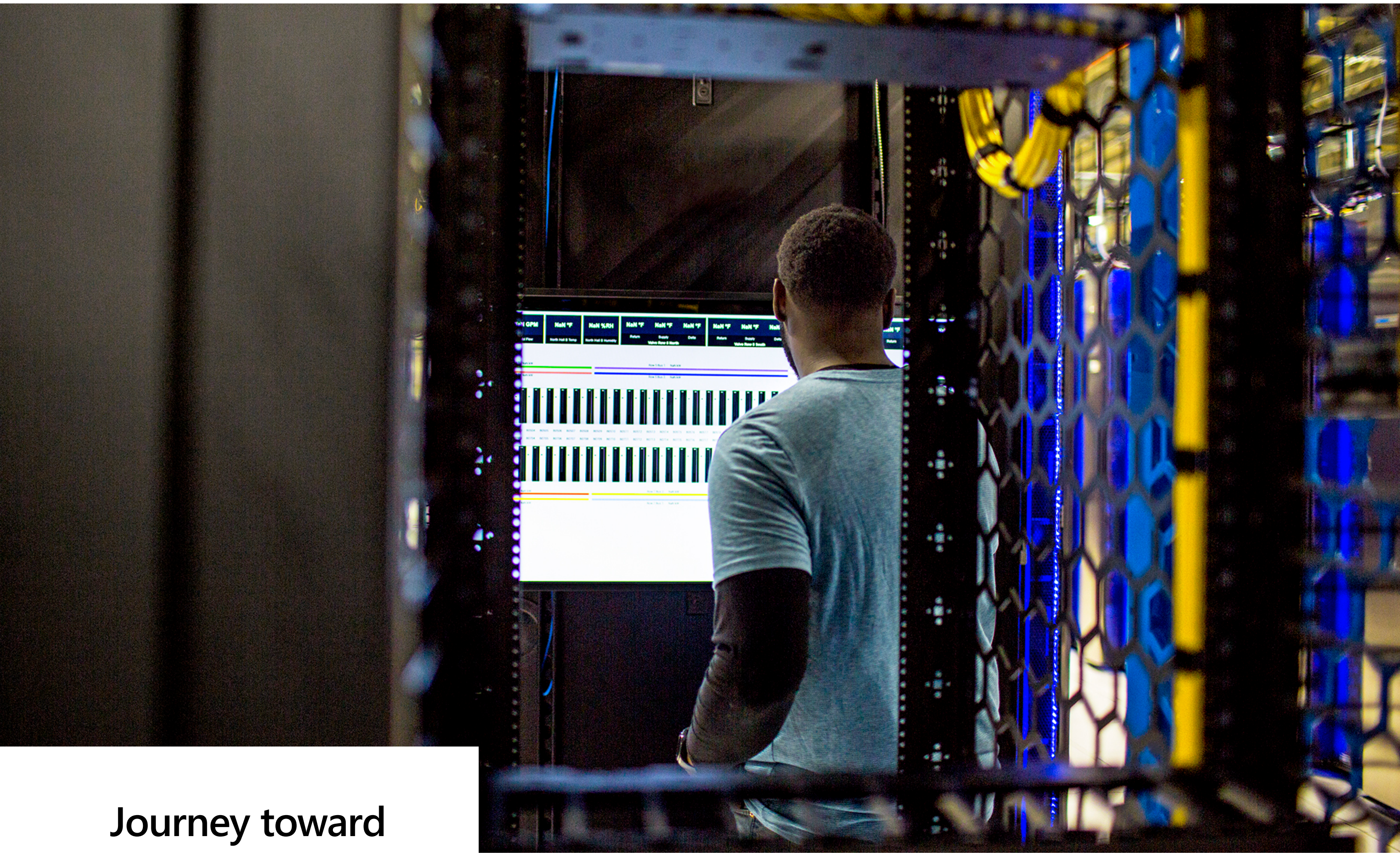
The outstanding question, then, is this: How effective is it to manage roles at the operations level and tie them to policy management? According to one participant, it's actually essential to operationalize roles because to enable SSO and passwordless capabilities, the right roles have to be defined. This participant also advocated caution, however, and warned against having too many roles. Every role defined must be managed now and in the future, which can create sprawl and risk, as roles may be left unmonitored or have more privileges than needed.

On defining roles effectively, one participant offered: "You want to be super granular with authorization, but at the end of the day, if you create a thousand roles in your organization to be that granular, you will have problems with management down the road. You're going to end up with massive amounts of accounts that are not updated, and that's where you have breaches—like if I move to another part of the organization and take those privileges [that I no longer need] with me into that new role."





Another participant shared an interesting perspective on the potential evolution of role management: “The future of roles will go from attribute-based management to token-based management, eventually aligning roles to tokens. That can be any type of token assigned to a user, depending on what tokening scheme you’re using. That is what the future of roles will be aligned with. Role management is very important, and that’s why continuous access control/continuous access management [is essential].”



Journey toward Zero Trust

As participants in the roundtable discussed their Zero Trust experiences—both how they started and where they are in the journey—several shared patterns emerged. A top concern was the necessity of understanding the scope of information security and identifying a starting point. Some participants had started their Zero Trust journey with user identity and access management, while others began with network macro- and micro-segmentations, and still others considered application sides. Eventually, all moved toward Zero Trust maturity by not trusting anyone or anything—inside or outside the wall, on the endpoint, on the server, in the cloud, and so on. They concurred that as Zero Trust evolves, so, too, does the realization that there is no destination, and this is all a journey.

One participant shared that they started their journey toward Zero Trust security with identity management. They wanted to implement SSO capabilities and realized these can be extended to work from home.

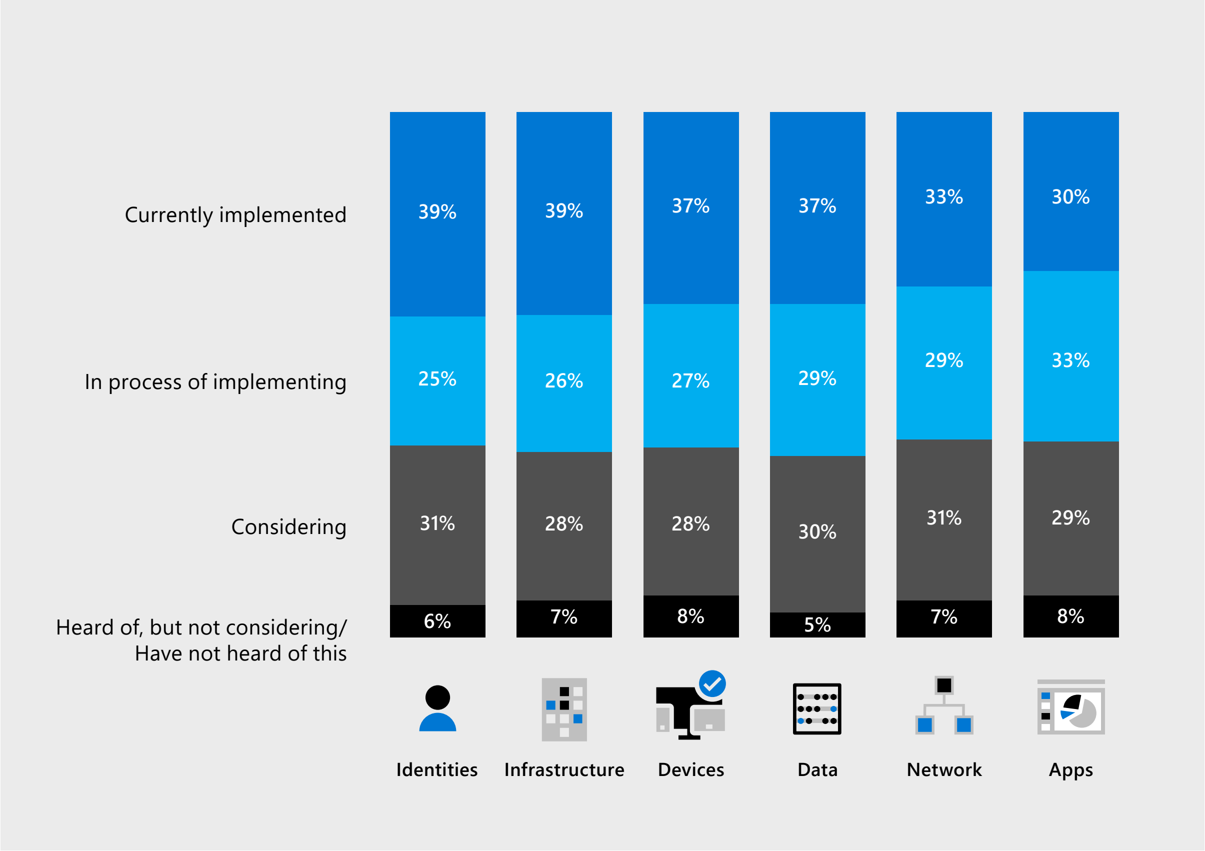
Developing a holistic strategy to address Zero Trust is critical. To define and execute a successful journey toward Zero Trust, an organization must consider corporate priorities, technologies, processes, and even the impact of change.

The roundtable agreed:

Start small, build confidence, and then roll out Zero Trust across the organization for optimal protection.

Zero Trust is an end-to-end strategy with implementation across all pillars

Current state of Zero Trust activities
Total (n=300)



Source: Microsoft Zero Trust Survey 2020

Start small and build confidence

Organizational requirements, existing technologies, and security stages all affect the planning for a Zero Trust implementation. While Zero Trust security is most effective when integrated across the entire digital estate, many organizations will need to take a phased approach that targets specific areas based on their Zero Trust maturity, available resources, and priorities. Each investment must be carefully considered and aligned with current business needs. The first step in the journey does not have to be a large lift and shift to cloud-based security tools.

Likewise, starting with Zero Trust doesn't require a complete reinvention of infrastructure. The most successful solutions should layer on top of and support a hybrid environment without entirely replacing existing investments.

No matter the size of the organization, deploying Zero Trust should start with the small pieces, as trying to complete multiple larger changes simultaneously often isn't feasible. Success is usually achieved by either starting with a new greenfield project in the cloud or experimenting in a dev and test environment.

One participant highlighted their opinion about starting small by saying: "You need to start with the crown jewels, but don't try to do everything. Trying to deploy Zero Trust and trying to do multiple other things simultaneously is not possible."

Another participant shared a real-life experience about convincing a large organization to start small with Zero Trust: "I did a workshop with a major bank and said they should start small. Their response was, 'We'll start small with 5,000.' From their perspective, that was small, but my response was, 'Start with 50.' The bank didn't agree and started with roughly 2,500. About eight weeks later, the bank came back wanting to re-evaluate their scope and what the pilot plan would look like. The bank restarted with 25 individuals. Now they're two years in, and they've progressed."

Extend to the full stack

After the first steps are taken and confidence is established, the Zero Trust model should be extended throughout the entire digital estate, while also serving as an integrated security philosophy and end-to-end strategy. When a Zero Trust strategy is applied to the full stack, it must cover the complete security posture.

Every access request should be strongly inspected for anomalies before granting access. Everything from the user's identity to the application's hosting environment should be authenticated and authorized using micro-segmentation and least privilege access principles to minimize lateral movement.

In short, to implement a Zero Trust security model consistently and comprehensively, organizations should consider all foundational elements, including identity, devices, applications, data, infrastructure, and network. In addition, the following considerations should be addressed:

- All users and devices attempting to access resources should be validated as trustworthy enough to access the target resource (based on sensitivity of target resource).
- A single Zero Trust policy engine should be used to consistently apply organizational policies to all resources (versus multiple engines whose configuration could diverge).
- The more measurements reflecting normal behavior included in a trust decision, the more difficult and expensive it is for attackers to mimic legitimate sign-in attempts and activities, deterring or degrading an attacker's ability to inflict damage.
- System operations should always stay in a safe state, even after a failed or incorrect decision (for example, preserve life/safety and business value via confidentiality, integrity, and availability assurances).
- Staying in a safe state is particularly important for organizations that rely on legacy or static controls that cannot dynamically measure and enforce trustworthiness of inbound access attempts (for example, static network controls for legacy applications, servers, or devices).

Assessing Zero Trust readiness

Organizations beginning to assess their Zero Trust readiness and plan improved protection across their digital estate should consider the following key investments, which will help drive a smooth and effective Zero Trust implementation.

Strong authentication: Ensure strong MFA and session risk detection as the backbone of any access strategy to minimize the risk of identity compromise.

Policy-based adaptive access: Define acceptable access policies for resources and enforce them with a consistent security policy engine that provides both governance and insight into variances.

Micro-segmentation: Move beyond a simple centralized network-based perimeter to comprehensive and distributed segmentation using software-defined micro-perimeters.

Automation: Invest in automated alerting and remediation to reduce the mean time to respond to attacks.

Intelligence and AI: Use cloud intelligence and all available signals to detect and respond to access anomalies in real time.

Data classification and protection: Discover, classify, protect, and monitor sensitive data to minimize exposure from malicious or accidental exfiltration.

Source: Microsoft Zero Trust Maturity Model

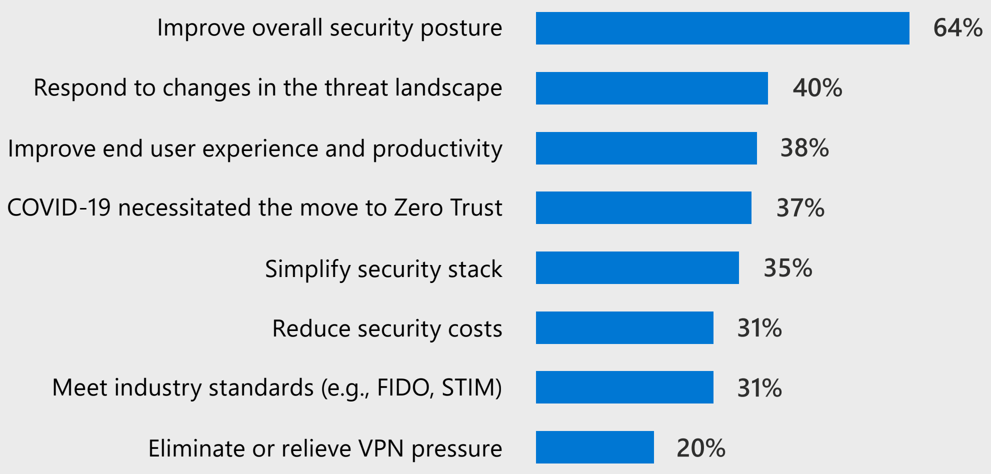
Sharing their organization's experience about growing in Zero Trust maturity, one participant commented:

> "[We started] off with a basic journey of manually doing micro-segmentation (before there was SDP), and then implementing NAC. From there, with the introduction of IoT and cloud and the thinning of the line of internal and external perimeters, it continues to evolve into the other aspects of Zero Trust—for example, application segmentation, network segmentation, identity federation, continuous authorization, and multifactor authentication—and has grown into a full-blown ecosystem."

Improving overall security posture is the biggest motivator to adopt a Zero Trust strategy, followed by evolving security threats

Zero Trust motivators

Total (n=300)



Source: Microsoft Zero Trust Survey 2020

Never trust, always verify

The Zero Trust security model establishes effective controls for business-critical information and systems, ensuring the right people have access to the right data at the right time. Based on the principle of “never trust, always verify,” Zero Trust helps secure corporate resources by eliminating unknown and unmanaged devices and limiting lateral movement. As Zero Trust delivers end-to-end strategy across the full stack—including identity, infrastructure, devices, data, applications, and network—implementing a true Zero Trust model requires all these elements to be validated and proven trustworthy.

While a Zero Trust model can be challenging to achieve, it’s an essential element of any long-term modernization plan. Any organization wanting to adopt Zero Trust should start by applying security controls on small pieces rather than trying to enforce multiple, larger controls simultaneously. Once security controls are successfully applied in a phased approach, Zero Trust security can be extended throughout the entire digital estate. An ideal Zero Trust environment includes strong identity authentication, devices enrolled in device management, least privilege user rights, and verified health of service.

Learn more

Discover Zero Trust security

Assess where you are on your Zero Trust journey

Microsoft Zero Trust Deployment Center