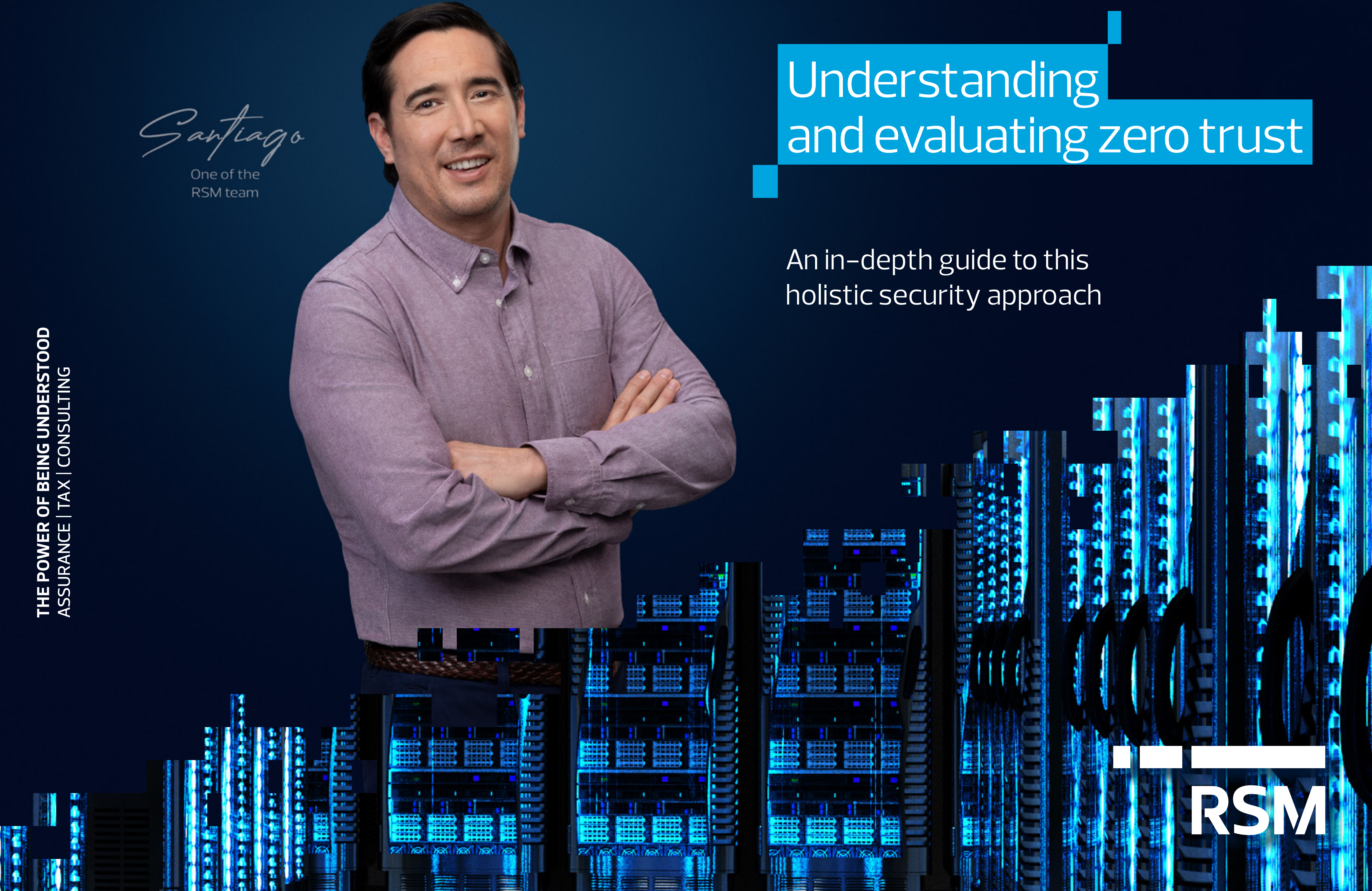
Understanding and evaluating zero trust

An in-depth guide to this holistic security approach



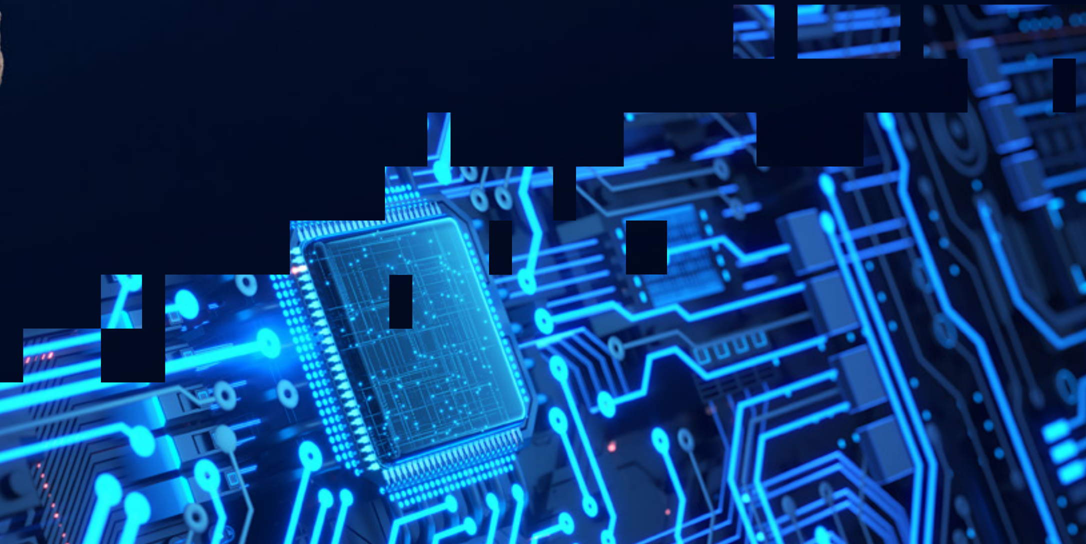
THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

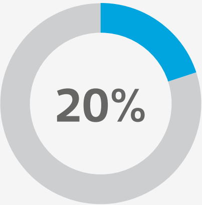
Table of contents

What zero trust is and why it's needed

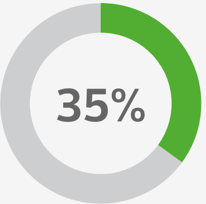
Cybersecurity is undergoing a radical transformation. Remote work arrangements, multiple cloud services, mobile devices, extended supply chains and interconnected and highly intertwined data streams have dramatically redefined what constitutes a network and what's needed to secure it. Cybersecurity risks are already high, and attacks have become incredibly sophisticated—and more menacing by the day.



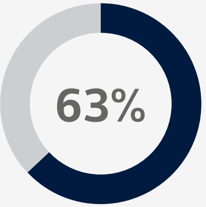
Consider what RSM found when it surveyed businesses for its 2023 Cybersecurity Special Report:



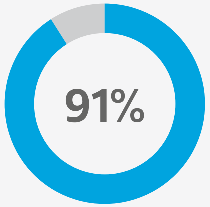
of middle market executives claimed their company experienced a data breach in 2022.



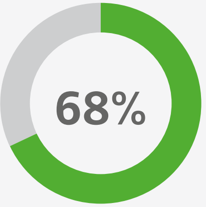
of middle market executives have been forced to deal with a ransomware attack.



expect to become a ransomware target moving forward.



said they have moved data to the cloud because they believe it is more secure there.



of business leaders believe that unauthorized users will attempt to access their data and systems.

What does this data tell us? A traditional approach to security based on borders, boundaries and perimeters no longer works, and most companies haven't yet adapted to this new reality. Today, every person is an insider—and everyone is a potential threat. To maximize security, organizations must start from the position that no person, device or system can be inherently trusted—outside, or even inside, the organization's perceived secure perimeter.

Instead, every person, device and system must be continuously authenticated, verified and monitored. It's critical to ensure that everyone and everything that touches the network is legitimately authorized to access and use it along with all the associated resources.

Zero trust is a multilayered security framework that meets this need. **Although many definitions of zero trust exist, the basic premise is "never trust, always verify" anything that touches a client environment, whether that be the physical network, public cloud or software-as-a-service (SaaS) applications.** And while the underlying concept of zero trust is easy to grasp, executing this security strategy is difficult because there's no single template to deliver a viable and sustainable zero trust framework. Every company's business model, IT infrastructure and risks are unique.

To achieve zero trust, companies must weave a tapestry of security tools and technologies into a unified fabric. The overall effectiveness of this framework depends on how well all the pieces of the security puzzle are assembled in the real world. Zero trust can involve entirely different technology vendors and disparate types of tools. As a result, there's typically a need to rethink and rewire processes, practices and workflows.

In this guide, you will find valuable information on zero trust, how to successfully put it to work in your organization and how to navigate the consulting and vendor selection process.

Zero trust myths

1.

Various security tools and controls embedded in a zero trust environment will interfere with business.

Best-in-class zero trust starts with the idea that trade-offs are unnecessary—and even undesirable. The goal is to frustrate attackers, not users. The reality is that zero trust can enable a more agile and efficient enterprise.

2.

Zero trust is too costly. It's something for large enterprises.

Nothing could be further from the truth. An upfront investment in zero trust can save money down the line. According to IBM, the cost for organizations with fewer than 500 employees is $3.31 million; the average cost per breached record is $164. Zero trust simplifies security by automating processes and greatly reduces the risk of a breach or ransomware attack. The right zero trust framework can help your organization align security with critical key performance indicators and metrics.

3.

Zero trust is a plug-in solution.

Zero trust requires experience and careful analysis to determine what works best for each organization. Every business is different and every zero trust framework is unique. As a result, a zero trust provider must have a broad set of industry partnerships with leading providers like Microsoft, Cisco, Palo Alto Networks and others. The provider must also be able to tie all the components together and provide visibility through a single pane of glass.

4.

Zero trust can wait. Strong identity management and multilayered security can keep us safe.

Identity and access management (IAM) is at the center of effective zero trust. Yet, there are numerous tools, technologies and approaches that orbit IAM. It's critical to map out the entire network topography—and understand how application programming interfaces (APIs) and other connections work in the real world, and on your network. Only then will your organization be able to assemble the right protections and configure them optimally.

What a zero trust model looks like

There are three primary pillars of a best-in-class cybersecurity framework:

- ✓ **Verify activity explicitly.**
  An organization must always authenticate network users and authorize access based on all available data points, including user identity, location, device health, data classification and anomalies.

- ✓ **Take a least-privileged approach.**
  A business must control user access with just-in-time and just-enough access (JIT/JEA), along with risk-based adaptive polices and robust data protection methods.

- ✓ **Adopt a breach-first mentality.**
  It's crucial to focus on methods that minimize the damage from a breach. This includes using segmentation to prevent lateral movement via a network, user, devices and application. Among other things, it's critical to verify that all sessions are encrypted end to end and tap analytics that support visibility and threat detection.

What makes a zero trust environment so powerful is the ability to operate in a coordinated way across multiple levels and layers within an environment—and beyond. For example, if a malicious actor compromises a user's device or credentials, a zero trust framework can detect the transgression through an IAM system directly, through behavioral analysis software or dynamic analytics that look at activity in a broader way.

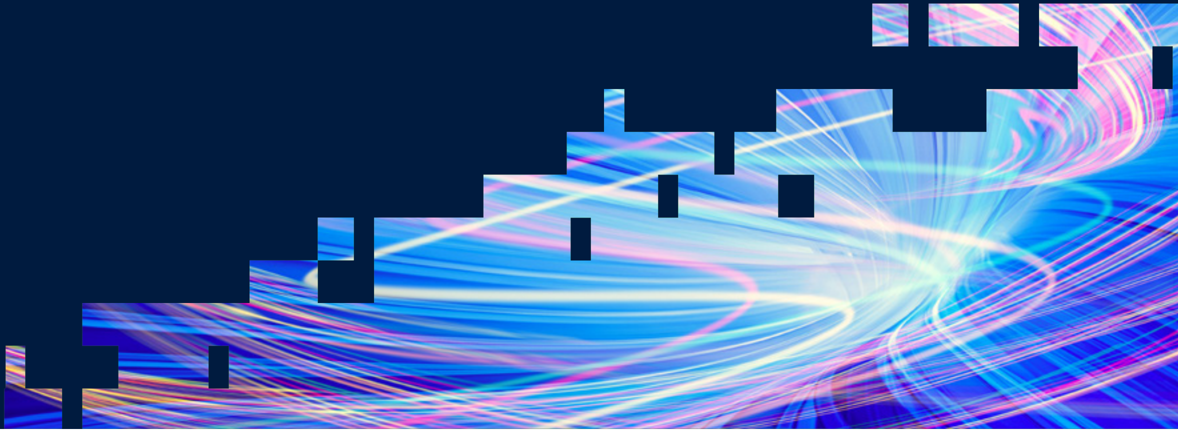
A zero trust system can then issue a security alert or temporarily block access to the network, depending on the importance of the data and other factors. It can also hone in on risks and point additional resources in that direction. With a context-level view, fine-grained controls and continuous monitoring and risk assessment, an organization evolves from reactive to proactive. In short, zero trust connects people, processes and monitoring in a more practical way.

Tools, technologies and products that establish zero trust

Some of the key technologies that comprise a zero trust security framework include:

- Identity and access management (IAM)
- Multi-factor authentication (MFA)
- Single sign-on (SSO)
- Directory services to manage permissions
- Network segmentation
- Firewalls
- Virtual private networks (VPNs)
- Software-defined networking (SDN)
- Data loss prevention (DLP)
- Endpoint security, including malware and spam detection software (EDR)
- Security orchestration, automation and response (SOAR)
- Encryption at rest and in transit
- Behavioral analysis software
- Application security, including static and dynamic scanning
- Risk management analysis software
- Data masking
- Penetration testing

The principles of zero trust



Secure the new identity perimeter

Most organizations today no longer house a single data center inside their corporate headquarters. Instead, most networks now typically consist of a combination of on-premises equipment, cloud services, mobile devices, SaaS solutions and other systems that in-house employees, remote workers, third-party vendors and partners, and others use to get work done. Because of this, identity (e.g., username/password or access credentials) has become the new network perimeter that must be secured.

Centralize and verify identity; manage access

Zero trust relies on a user's identity and least-privileged access principles to determine if a person can access a network or not, and what applications and data they can use while they are on the network. Zero trust establishes a clear baseline of trust, enforces trust-based access, continuously verifies trust and responds to any change in trust. It handles these tasks by establishing definitive rules for what people should and shouldn't do when they are accessing and using the network—and what access is acceptable and not acceptable.

These adaptive controls are based on contextual policies and attributes, including location, role, device type and other factors. Zero trust also incorporates a flexible set of MFA tools, such as push, calls, SMS, biometrics, wearables, passwordless and tokens. In this way, it's powerful yet flexible enough to suit different users, needs and situations without compromising protection.

User trust

Whenever someone logs into a network, zero trust authenticates and validates that the person is who they say they are and makes the decision whether or not to authorize and grant the user access to any applications or data.

Device trust

Zero trust operates on a closed-access default model with access on a per-app basis. If a user's device appears to be compromised, an organization can temporarily revoke network access. An analyst can investigate the potential breach and depending on the outcome, clear the user and device or permanently block it. For instance, a scanner might detect malware or a login from an IP address in a different country than where the person resides and act accordingly.

Zero trust also introduces onboarding and offboarding protocols with baked-in rules, so that former users and zombie devices don't continue to have access for days, weeks or months after they were supposed to be offboarded or decommissioned. In this way, an organization achieves frictionless, consistent yet secure access—for any application, using any browser, app or device—across legacy, hybrid and multi-cloud environments. This approach eliminates or scales down high-risk protocols and provides device posture assessments for unmanaged devices.

Applications

With strong MFA and insight into users and devices across a network, it's possible to establish highly secure access and granular controls across a wide array of applications, services and platforms—residing in both legacy environments and in the cloud. These capabilities extend across guest accounts and representational state transfer (REST) APIs. This makes it far more difficult for an imposter to gain access to critical assets—and plant malware or steal data.

Network traffic

In business and in cybersecurity, many events are situational, so having the ability to continuously monitor conditions and detect anomalies is paramount. Highly integrated zero trust systems share signals to quickly detect any change in risk. This extends from legacy systems to the cloud; from operational technology to internet of things (IoT) devices. Best-in-class zero trust accomplishes this by continuously scanning and examining connected devices, device posture, disabled security features, the state of patches and security updates, and other factors. It also integrates and coordinates features across vendors and third-party applications.

As a result, whenever a suspicious event does occur or an unauthorized "bring your own device" event pops up, an enterprise can immediately pinpoint it, quickly identify the scope of the incident and take steps to resolve it. Ultimately, an accelerated and appropriate response (one that is in line with the actual threat and risk) establishes better safeguards while streamlining data visibility, aggregation and correlation across the enterprise.

This approach not only trims manual work and technical debt, but also frees help desks and security teams from the need to constantly put out fires. Instead, they can focus on strategic issues.

Data

Zero trust provides numerous protections for data. Today, a vast array of structured and unstructured data types exist—and databases, files and documents are spread across legacy systems, clouds, home offices and even devices. This points to the need for strong data governance, encryption of data at rest and in motion, advanced firewalls and VPNs, and more. Zero trust provides a way to tie all these tools, technologies and components together in a uniform way—and ensure that an organization is consistently enforcing data policies.

Workloads

The point of zero trust is to secure access across all applications and environments, from any user, device and location. Rather than attempting to establish protection through silos of disconnected security, the protection is embedded in workflows. That way, with visibility across systems, an enterprise can continuously monitor for risks and apply the right protections to a workforce, workloads and workplace—including across multi-cloud environments, APIs and out to the IoT and edge computing spaces.

Gain visibility into devices

The capacity to view devices and users in real-time—and manage their level of access—is a foundational component of zero trust. Centralized cloud controls make this possible. Rather than handling security from different systems, applications and silos—and attempting to string everything together—it all occurs in the same place. With live, centralized monitoring, an unauthorized connection or event is highly unlikely.

Enforce access policies

Zero trust continually applies and enforces an organization's access policies. With centralized cloud controls in place, security teams can also enforce endpoint security, device configuration, app protection, device compliance and overall risk levels. Zero trust and the cloud ensure that devices are securely provisioned, properly configured and up to date. This high level of uniformity and consistency greatly simplifies security—while dramatically improving it.

The steps to achieving zero trust

Zero trust is both a program and an ongoing journey. Achieving a best-practice framework takes time and effort. It's critical to identify gaps as well as opportunities across devices, networks, applications, workflows and data. Key questions include:

- Which applications rely on implicit trust?
- What is our organization's budget and timeline?
- Does the current IT environment support the necessary changes?
- Do we have the required internal knowledge and bandwidth needed to tackle zero trust, or should we tap outside resources to design a custom zero trust framework?
- Are we equipped to execute the plan?

Developing a strategy and establishing a path to zero trust is essential. It's possible to approach a platform in different ways and with different vendors and tools.

Here are five critical steps:

Step 1:
Analyze your existing security environment. Work with a trusted consultant or managed services provider that has the experience to understand your business, conduct a detailed assessment and match your organization's processes with the right security tools, technologies and solutions.

Step 2:
Analyze what you need to achieve zero trust. Conduct an in-depth analysis of existing security protections and evaluate what is lacking. This gap analysis process must extend across the various pillars of zero trust security, including users, devices, applications and workflows, the network, and data.

Step 3:
Begin the search for solutions. Focus on solutions that rely on open standards so you have maximum flexibility to connect systems and adapt as conditions change. Items to look for include open API frameworks, low-code integration and management features, strong reporting tools, AI and automation tools, and functionality across the entire enterprise, including IoT components and multi-cloud environments.

Step 4:
Advance to the implementation phase. Identify the specific zero trust security tools, technologies and products that best fit your organization's needs. At the same time, identify skill gaps and infrastructure gaps that could undermine results. It's critical to address these issues before switching on new security solutions.

Step 5:
Undergo regular reviews. Ideally, an organization should continue to work with a trusted provider over time to assess and review tools, products and performance—and identify new issues and possible gaps. Today's cybersecurity environment changes quickly, and organizations must shift and adapt accordingly. Both risks and solutions are in a steady state of flux.

What to look for in a zero trust solution

★★★ GOOD

★★★★★ BETTER

Application and workload controls

★★★

- Most mission-critical applications available over public networks to authorized users
- Protections exist across all application workflows, with context-based access controls
- Coordinated teams exist for development, security and operations

★★★★★

- Applications available over public networks and include continuous authorized access controls
- Protections exist for all types of sophisticated attacks within all workflows
- Support for immutable workloads with security testing integrated throughout the application and workload life cycle

Data controls

★★★

- Automated data inventory and tracking
- Consistent, tiered and targeted categorization and labeling of data
- Redundant and highly available data stores
- Static DLP
- Automated and context-based access controls
- Data encrypted at rest

★★★★★

- Data inventories take place on a continuous basis
- Automated data categorization and enterprise-wide labeling
- Optimized data availability
- Dynamic access controls
- Data fully encrypted in motion

Device controls

★★★

- The ability to track nearly all physical and virtual assets
- Enforced compliance that's tied directly to threat risk
- Device posture determines initial resource access

★★★★★

- Continuous physical and virtual asset analysis, including automated supply chain risk management that's integrated with threat protections
- Access to resources based on real-time device risk analysis

Network controls

★★★

- Expanded isolation and resilience mechanisms
- The ability to adapt configurations through automation
- Network-level data encryption

★★★★★

- Micro-perimeters with just-in-time and just-enough access controls
- Proportional resilience
- Configurations that evolve to meet application-specific needs
- An ability to integrate best practices for cryptographic agility

Identity controls

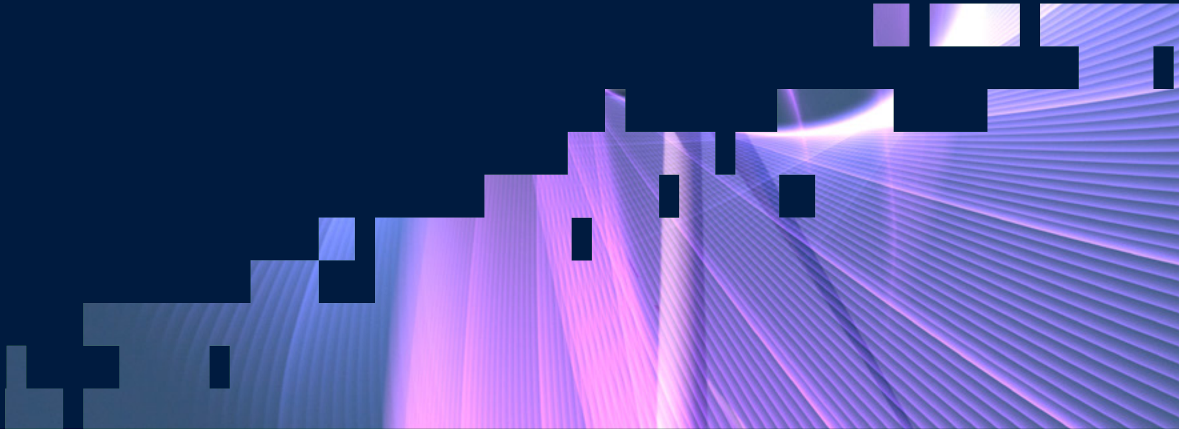
★★★

- Strong MFA that's phishing resistant
- Consolidated and securely integrated identity stores
- Automated identity risk assessments
- Granular, session-based access controls

★★★★★

- Continuous validation and risk analysis
- Enterprise-wide identity integration
- Granular, tailored and automated access

How RSM delivers on the promise of zero trust



RSM builds knowledge, experience and industry perspective into a proven zero trust methodology. This includes insight into products, compliance requirements, data privacy issues, technical considerations and business requirements. In addition, RSM has strategic relationships in place with leading technology providers, including Cisco, Microsoft and Palo Alto Networks. All of this means that RSM can devise a zero trust framework based on the unique needs of your organization and connect performance to the metrics and KPIs that matter most to your business.

RSM's zero trust methodology

RSM's cybersecurity advisors have developed a best-in-class framework for navigating zero trust. It's based on seven critical factors:

- Minimizing disruption
- Optimizing costs
- Reducing complexity
- Managing legacy technologies
- Balancing security, business performance and user experience
- Developing skills and knowledge
- Continuous monitoring adaptation

Conclusion

Zero trust is central to protecting your organization's business today. It's a multilayered security framework designed for a borderless world of computing and interaction. But it's important to remember that it isn't a template, product or plug-and-play solution. It's a strategic framework that requires broad and deep analysis—and a plan that fits the unique needs of your organization. The right advisor can guide you to zero trust success—and strengthen and simplify your organization's security.

Take your organization's security protections to a higher level through RSM's zero trust framework. Contact us today to get a free two-hour consultation.

CONTACT US

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.