CYBERSECURITY

Zero Trust: Your Digital Transformation Requires a Risk Transformation

SEPTEMBER 2022

Table of contents

Introduction 3

Zero trust principles 4

Why zero trust matters 6

Getting started 7

Conclusion 8

Let’s get started 8

Sources 9

Executive summary

Modernizing your technology landscape requires a parallel cybersecurity strategy because your users and data are no longer protected by the corporate firewall. While the cloud provides unsurpassed agility, it also exposes new threat vectors. Your digital transformation must be accompanied by an innovative and comprehensive approach to reduce risk and attack surfaces.

Follow Us:
@NTTDATAServices

Connect With Our Experts:
cybersecurity.sales@nttdata.com

An information cybersecurity framework, zero trust states that an organization shouldn't trust any entity inside or outside its perimeter. It provides the visibility and controls needed to secure, manage and monitor every device, user, application and resource used to access business data.

Zero trust has taken the cybersecurity industry by storm. You can't spend much time looking at cybersecurity solutions, frameworks or products without seeing references to the concept. But is it simply the latest trend sweeping the industry, disguising decades-old approaches as something new and buzz-worthy? Or is it a revolutionary approach to protecting organizations and their users, resources and applications, especially as they embark on their digital transformation journey? The answer, fortunately, is the latter.

Though it's recently caught on across the industry, zero trust dates back over a decade. It's widely attributed to the well-regarded technology analyst firm Forrester, where in 2009 the firm's John Kindervag defined a security mode aligned with the premise that "trust is a vulnerability, and cybersecurity must be designed with the strategy, 'Never trust, always verify.'"[1] But the concept goes back a bit further, having first been coined by Stephen Marsh in his 1994 thesis, "Formalising trust as a computational concept."[2] Marsh sought to mathematically prove the differences between zero trust (or no trust) and distrust, and then apply these concepts to computing, human nature and, more importantly, situational trust.

Together, the work of Marsh and Kindervag paved the way for a revolutionary approach to cybersecurity, forming what's now a widely accepted best practice. Their work indicates you must not simply trust that a person is who they say they are or a machine what it says it is; you always need to verify, and you must look at the context to ascertain that validity is legitimate. Let's unlock what this means.

Zero trust principles

The situations that a computer, server, application or user finds itself in provide part of the context of what each should be allowed to do. This ties directly into the first of the three principles of the modern zero trust framework.[3]

Secure access

Also referred to as explicitly verify, secure access advises that you must authenticate and authorize based on multiple data points (or situations).[3] This information could include user identity, IP address, device health, application, level of access the person is trying to request, location and data classification, along with many other factors. Together, these data points provide context that proves (or disproves) the person is who they claim to be (authentication) and executing a task they're allowed to perform (authorization) on resources or devices they're supposed to be using.

The secure access principle also expresses that these connections must endure the same validation each time the person performs a task. Initially, the connection requests should be considered as external and untrusted, and they must remain so until the validation is completed successfully — every time. User identities are often the victims of compromise, and this practice helps reduce the likelihood of such an occurrence.

Secure access

"Never trust; always verify" — authenticate and verify all access to resources. Treat internal connections the same as external and untrusted connections.

Least privilege

Limit users and devices to the lowest level of access possible. Minimize the attack surface.

Assume breach

Provide strict segmentation and log all activities. Use analytics to inspect data.

Figure 1: The three principles of the modern zero trust framework

Least privilege

This best practice approach to access management is central to the security pillar of Amazon Web Services' Well-Architected Framework.[4] The least privilege model regulates a user or device's access level to the most limited level required to complete the task. This significantly reduces the attack surface, because users, applications and technologies can only access resources they're expressly allowed to access and are limited to the tasks they're permitted to perform.

To put the least privilege model in context, think of your organization's talent recruiter. They need access to the staffing system in your HR portal to open roles, find candidates and facilitate hiring employees for roles in their assigned business division, the marketing team. The recruiter needs an HR talent acquisition user account for the marketing business unit, but they don't need access at an administrator level or access to any other business unit's HR system.

The least privilege model compounds the protection layers the secure access principle sets forth. With secure access, users and resources are authenticated and authorized across contextual data points, which translates to a high likelihood that they are who they say they are. When you layer in least privilege, these users and resources only have access to a workload at a level they absolutely must have to carry out a task they're supposed to perform. When combined, these two principles significantly reduce the attack surface.

Assume breach

This principle isn't a reflection of the adage that cybersecurity professionals are paranoid beyond reason (and one we find good humor in because we've seen how things can unravel). Assume breach serves as a lens to ensure you design and implement controls while continuously verifying that your environment hasn't been subject to a breach. It essentially models cybersecurity best practices to mitigate the likelihood or pervasiveness of the MITRE ATT&CK kill chain, such as lateral movement, defense evasion, and command and control. This principle is an especially relevant consideration within a cloud environment because resources aren't hidden behind the corporate firewall; rather, they're dispersed across different clouds, subscriptions and tenants, each with its own cybersecurity protocols.

The assume breach principle complements governance and control objectives. It's frequently implemented through microsegmentation, session validation, hardened images and encryption, as well as log aggregation and monitoring, along with many other defensive techniques.

Going back to the HR example, where you implemented continuous verification and least privilege, assume breach becomes the third layer of defense. To ensure your talent recruiter is accessing only what they should access in a protected environment, you can implement microsegmentation, so only the app and necessary data are in this area of the virtual data center. You then layer in cloud-native functionality, such as a web application firewall, network security groups (NSGs), policies, network access control lists (NACLs), encryption and other controls, where the recruiting app resides to secure the workload and restrict network ingress and egress. You must also implement continuous monitoring and threat detection to ensure a bad actor hasn't slipped through your gates or infiltrated through a seemingly innocuous system update (like a patch), where it may reside, waiting for an opportunity to strike.

Most technology and cybersecurity providers have different interpretations of and names for these core principles, but they're essentially parallel to each other with the same implications.

Why zero trust matters

The top reason to implement a zero trust approach is attack surface reduction. The three pillars yield a defense-in-depth strategy that mitigates risks and limits vulnerabilities to help avoid exploit potential. Exploits and breaches cost money — often a lot of it.

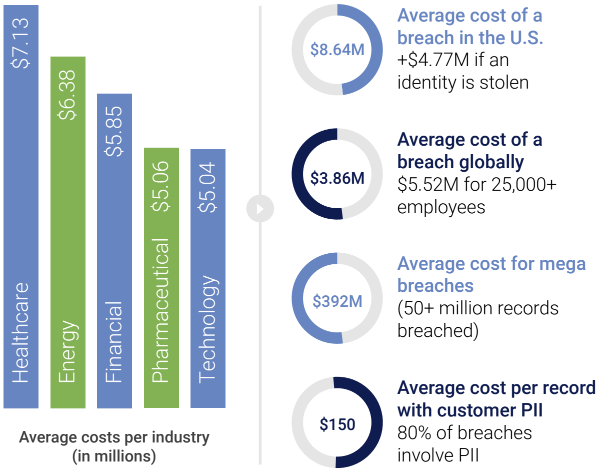


Figure 2: The average cost of exploits and breaches[5]

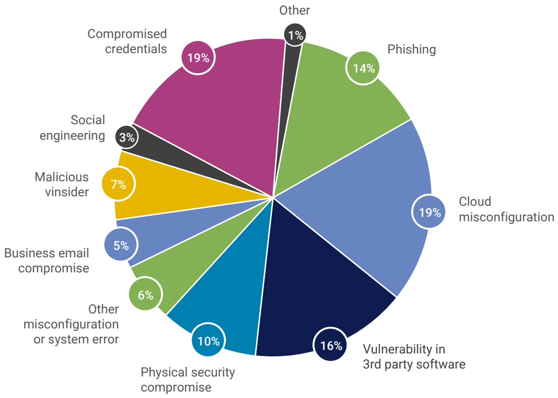
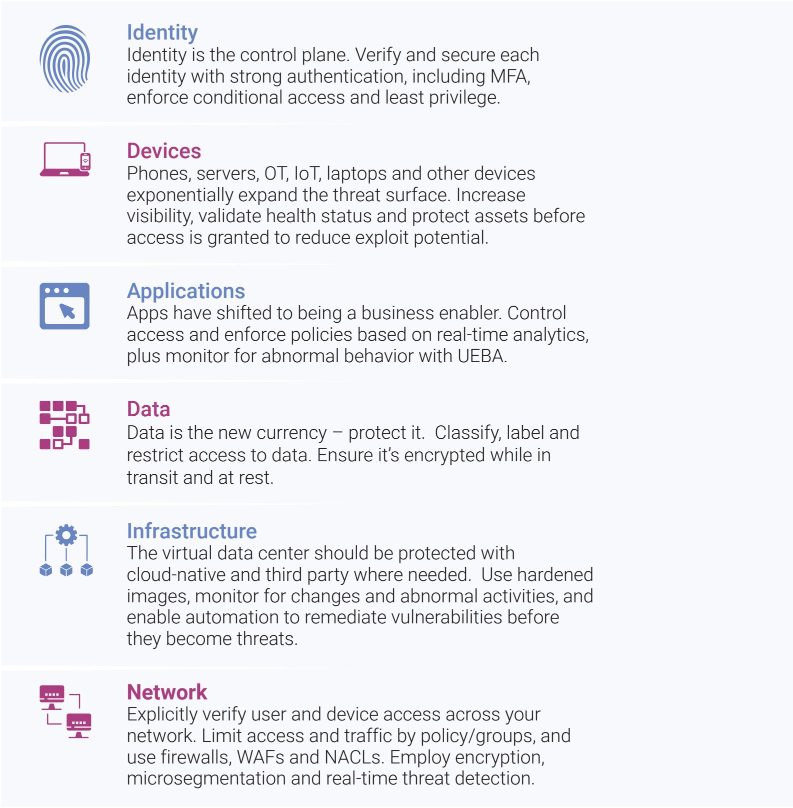


Figure 3: Breakdown of malicious data breach root causes by threat vector[5]

The impact of a breach on brand and reputation is devastating. A simple search for famous breaches uncovers a world of bad actors and terrible events leading to a tremendous loss in customer trust. The zero trust methodology significantly reduces the threat surface and goes a long way to mitigate these risks — when implemented comprehensively.

But it doesn't have to be complicated. The principles need to be applied to and across the core components: identity, devices, applications, data, infrastructure (including infrastructure as a service [IaaS] and platform as a service [PaaS]) and network. Each of these components serves as a control point to defend and protect.



Identity
Identity is the control plane. Verify and secure each identity with strong authentication, including MFA, enforce conditional access and least privilege.

Devices
Phones, servers, OT, IoT, laptops and other devices exponentially expand the threat surface. Increase visibility, validate health status and protect assets before access is granted to reduce exploit potential.

Applications
Apps have shifted to being a business enabler. Control access and enforce policies based on real-time analytics, plus monitor for abnormal behavior with UEBA.

Data
Data is the new currency – protect it. Classify, label and restrict access to data. Ensure it's encrypted while in transit and at rest.

Infrastructure
The virtual data center should be protected with cloud-native and third party where needed. Use hardened images, monitor for changes and abnormal activities, and enable automation to remediate vulnerabilities before they become threats.

Network
Explicitly verify user and device access across your network. Limit access and traffic by policy/groups, and use firewalls, WAFs and NACLs. Employ encryption, microsegmentation and real-time threat detection.

Figure 4: Enabling zero trust approaches reduces vulnerabilities

The generated signals from each component need to be assessed and integrated with policy enforcement mechanisms, which helps fulfill the objectives outlined in the zero trust principles. It's imperative to protect each control plane, (identity, devices, applications, data, infrastructure and network) with secure access, least privilege and assume breach to considerably narrow the vectors that can be compromised. This model demonstrates defense-in-depth strategies that can be applied across your digital or hybrid estate.

A vast body of work exists that notes how to apply zero trust most effectively, where to start and what to prioritize. In the real world, however, this abundance of direction is often confusing and overly complicated. The reality is: Zero trust is an underlying framework. But more than that, it's a journey. Because threat actors constantly evolve their techniques, you're never there, and you're never done. It's critical that you do all you can to stay ahead of the threats.

Getting started

Your organization's priorities, risk appetite, compliance and business requirements, and environment health are unique. One of the more effective approaches to getting started is to list your priorities and assess your IT roadmap. Consider key parameters and question your organization's requirements as part of your zero trust strategy.

Priority	Considerations
Identity and access management: Touted as the new perimeter, identity is regarded as a top priority	Has your organization: • Implemented multi-factor authentication and single sign-on? • Leveraged conditional access? • Enabled just-in-time access functionality? • Formulated processes regarding joiners, movers and leavers? • Defined robust access policies? • Implemented privileged access or an identity governance and administration solution?
Network security: The network perimeter has derailed to look more like a spider web than the traditional linear concept you could control with relative ease	Has your organization: • Designed and implemented your architecture according to best practices? The National Institute of Standard and Technology recommends strategies, deployment models and practical guidance for a zero trust architecture.6 • Adopted microsegmentation? • Implemented network protection solutions and controls, such as network security groups, NACLs, WAFs and a secure access service edge? • Developed and deployed software-defined perimeters? • Enabled distributed denial-of-service protection?
Workload cybersecurity across applications, infrastructure, IaaS and PaaS: Your applications and associated resources are dispersed across your on-premises, private, public, hybrid and multi-cloud data center(s) as well as software-as-a-service (SaaS) apps; you need to implement controls to adequately protect them	Is your organization: • Classifying data and encrypting it while in transit and at rest? Additionally, are you doing this with automation? • Using a cloud access security broker to govern access to your SaaS apps and discover shadow IT? • Utilizing server-side encryption? • Adequately protecting every endpoint? • Identifying, controlling and managing assets? • Taking advantage of fit-for-purpose cloud-native controls (provided by cloud service providers, often at no additional cost) or using a best-of-breed cybersecurity solution strategy? • Including cybersecurity testing and best practices directly in your DevOps pipeline and shifting left to fully embrace a DevSecOps model?
Governance and control: While the cloud provides unprecedented agility, scalability and growth opportunities, it fosters an unwieldy environment that requires a zero trust lens to control the sprawl	Has your organization: • Implemented a cloud management system to easily protect, control and enable your development staff to effectively manage resource provisioning? • Adopted infrastructure as code, with cybersecurity controls infused directly into your deployment templates? • Deployed real-time policy enforcement? • Enabled UEBA to detect internal threats or abnormal behaviors? • Embraced automation to reduce manual intervention? (Automation has led to average savings of $3.58 million in the event of a breach, which is compounded when you consider a reduction in support hours.[5]) • Tracked your environment's health by monitoring all logs and implemented automated remediation? • Implemented continual compliance assessments in your environment and adapted your controls to identify gaps and systemic issues? • Been consistently working to optimize costs, controls and policies to protect your overall cloud security health?

Conclusion

Digital transformation creates a realm of new possibilities and potential. While it eliminates challenges we've historically faced with IT, it also creates an environment of unrealized risks and threat potential. Leveraging a zero trust mindset helps bridge the gap, protect your financial interests and enable a safer, more cohesive future.

Digital transformation requires a risk transformation. The cybersecurity strategies of yesteryear will not protect your business in the rapidly evolving threat landscape. Zero trust, if applied consistently and comprehensively, can protect your organization today while giving you the flexibility to grow into the future.

Let's get started

An assessment or workshop will put all this into action, and the right service provider can help start your organization on a zero trust journey.

Partner with NTT DATA to benefit from agnostic and unbiased recommendations. We help you explore key considerations that need to be addressed and itemize initiatives based on criticality. Our holistic view of what others are facing across industries and against countless use cases helps ensure your plans are future-ready.

Start your zero trust journey with NTT DATA's cybersecurity experts.

- Deep industry expertise and market-leading technologies
- Tailored capabilities with your objectives in mind
- Partnerships to help you build and realize your vision

Contact our experts, or us.nttdata.com/en/services/cybersecurity-services to learn more.

Sources

1. Chase Cunningham. “A Look Back At Zero Trust: Never Trust, Always Verify.” Forrester. August 24, 2020. https://go.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/

2. Stephen Paul Marsh. “Formalising trust as a computational concept.” University of Sterling. 1994. http://hdl.handle.net/1893/2010

3. Microsoft. “Embrace proactive security with Zero Trust.” https://www.microsoft.com/en-us/security/business/zero-trust

4. Adam Cerini, Ben Potter, Bill Shinn, Brigid Johnson, et al. “Secure Pillar — AWS Well-Architected Framework.” Amazon. May 21, 2021. https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/wellarchitected-security-pillar.pdf

5. IBM Security. “Cost of a Data Breach Report 2020.” Conducted by the Ponemon Institute. https://www.ibm.com/security/digital-assets/cost-data-breach-report/

6. Scott Rose, Oliver Borchert, Stu Mitchell and Sean Connelly. “NIST Zero Trust Architecture.” National Institute of Standards and Technology Special Publication 800-207. August 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Visit **nttdataservices.com** to learn more.

NTT DATA Services is a recognized leader in IT and business services headquartered in Texas. A global division of NTT DATA — a part of NTT Group — we use consulting and deep industry expertise to help clients accelerate and sustain value throughout their digital journeys.

NTT DATA
Trusted Global Innovator

September 2022 | 975048-Zer-Trust-Element- White-paper-V2.indd | Rev. 1.0