
Never trust.
Always verify.

Content

Introduction

Introduction

The more digitally connected you are, the greater your risk of cyberattacks. The question isn't if your organization will be breached, but most likely, when.

The problem is that many organizations still have a siloed approach to cybersecurity, which is inadequate against modern-day cyber threats. And as more businesses become interconnected, a breach can have a dramatic ripple effect on others. A zero trust model establishes trust in users and devices through authentication and continuous monitoring of each access attempt, with custom security policies that protect every application.

Read on to learn more about zero trust and why it is a comprehensive approach to securing your networks, applications, and environment.

Why top performing organizations put security front and center

> 96% of CXOs state that achieving security resilience is critical to their business. Yet nearly two-thirds of respondents reported suffering major security incidents that jeopardized business operations.[1]

Why top performing organizations put security front and center

In the past, security followed the castle-and-moat model, where nothing outside the network could access data on the inside. If you were working in the office, access was trusted, and virtual private networks facilitated remote working.

But as more people have started working from remote locations, organizations require a new way to connect them securely to the systems and data they need.

Now, simply being connected to the network no longer matters.

96% of CXOs state that achieving security resilience is critical to their business. Yet nearly two-thirds of respondents reported suffering major security incidents that jeopardized business operations.

Today's security defenders not only have to consider increasing threats and an expanding attack surface, but also bigger picture risks, such as warfare or financial instability.

Fewer than half of CIOs/CTOs agree strongly that their current cybersecurity controls are effective in protecting and enabling their employees, wherever they work.[2] It's no wonder that enhanced cybersecurity is therefore their top criterion when assessing customer or employee experience technology solution partners.

Security can impact the bottom line. Top-performing organizations are twice as likely to have fully aligned their security strategy with their business strategy.[3]

1 Cisco Security Outcomes Report Volume #3

2 NTT's 2022–23 Network Research Report

3 NTT's 2023 Global Customer Experience Report

What is zero trust?

What is zero trust?

Many organizations still have a siloed approach to cybersecurity. Usually, this comes down to organizational structures. Different security tools may have different custodians: the firewall falls under the infrastructure team, application security under the cybersecurity team, and data-loss prevention under the risk department, for example.

Many recognize the gaps inherent in this approach, including limited visibility, delayed manual problem-detection, and a reactive response, but aren't sure how to use their existing security tools to address these gaps and operate as a single platform. How do they deliver the right layers of security for their unique operating environment?

> "Zero trust is a way to modernize the cybersecurity infrastructure to align to how you know business is being done.
>
> Scott Coner, Vice President, Solutions Presales: Systems Integration at NTT

> Effectively, we've shifted the security barrier to a different area – but you still need to have technical controls in place.
>
> Gary Dawkin, Principal Go-to-Market Practice: Cybersecurity at NTT

What is zero trust?

The default assumption within a zero trust security framework is that all users, devices, endpoints and network traffic – both inside and outside an organization's network – are compromised and therefore cannot be trusted.

Zero trust is a flexible, scalable and, most importantly, proactive approach to security that enables organizations to protect sensitive data and systems by reducing the attack surface and limiting access to only those who need it. Access to resources is based on a user's identity, device posture and other contextual factors. Every access request is authenticated and authorized before access is granted, with custom security policies that protect every application. Continuous monitoring and analysis of user behavior is used to detect and respond to anomalies.

The overall zero trust layer is made up of policies and procedures, for example, making sure not only that users have access to applications but also what those applications are allowed to interact with. An attacker who gets into your network might get one application to speak to another if you have not implemented a full zero trust security model.

According to Gartner, zero trust network access is growing rapidly, and by 2025, at least 70% of new remote access deployments will rely on zero trust rather than VPN services.[4]

Put simply, just being connected to the network no longer matters. Instead, every time you connect to anything, the security system will check who you are, what application or data you're connecting to, whether it's on-premises or in the cloud, when you're connecting, where the data resides, why the data is being accessed (the context), and how the data is being accessed.

A mature zero trust environment, which protects access as well as assets, can boost your security resilience by 30% compared to organizations lacking zero trust.[5]

4 Gartner: Zero trust Will Replace Your VPN by 2025 (datacenterknowledge.com)

5 Cisco Security Outcomes Report Volume #3

Five reasons why you should move to zero trust

1.
Manage increasingly complex IT environments

Cloud computing, IoT, mobile devices, and the decentralized workforce have resulted in IT environments becoming more complex and difficult to secure.

Zero trust enables you to be more responsive to changing business requirements. At the same time, strong access controls and ongoing monitoring of user behavior help you to protect data, measure compliance and regulatory requirements, and avoid costly fines and reputational damage caused by cyber threats.

A software-defined approach to security also allows you to quickly adapt to new threats and implement new security policies without disrupting business operations. You can reduce the attack surface by authenticating and authorizing all traffic before access is granted.

2.
Optimize your investments

The cost of doing nothing can be far greater than the investment in a robust security strategy.

Security strategies require ongoing evaluation and adjustments to ensure they are effective and relevant. Investments in security systems need to be optimized and integrated with new technology.

Zero trust is a journey, and partners such as NTT offer consulting, advice, design, implementation and management, giving your business access to expert guidance.

3.

Respond to ever more sophisticated cyberthreats

Cyberthreats have become more sophisticated and more difficult to detect. They're also changing all the time.

Zero trust continuously monitors and analyzes user activity for signs of malicious behavior, and to detect and respond to anomalies. It provides better visibility and control over user and device access to critical resources. With traditional security models, security is not extended to the new perimeter. Zero trust extends trust to support a modern enterprise with BYOD, cloud apps, hybrid environments, and more.

By implementing granular access controls, you can ensure users access only the resources they need to perform their job functions, and monitor user activity in real time, allowing you to enforce security policies more effectively.

> Zero trust provides a similar experience despite me accessing different programs or different platforms hosted by different companies. And the experience is similar whether I’m in the office or in a coffee shop.

Shawn Gibson, Senior Solutions Architect: Systems Integration at NTT

4.

Reduce complexity in implementation, user experience, and improved employee culture

Traditional security models can be overly restrictive and create friction for users, leading to workarounds and reduced productivity.

Zero trust simplifies security by consolidating controls into a single framework. Centralized security policies reduce the complexity of security architectures, making them easier to manage and maintain.

Zero trust also improves the user experience by reducing the need for complex passwords and other security measures, while ensuring the flexibility of remote work adopted by many employees in today’s modern workforce is possible without the interruption of cyber threats.

5.
Lack of skills and talent for implementation and management

The lack of skills and expertise in implementing and managing improved security measures can be a major barrier to moving from traditional security models to a more comprehensive approach.

Zero trust removes complexity, enabling you to leverage the capabilities of zero trust without needing to invest in continuous upskilling of your IT organization to keep up with changes in technology.

There may also be challenges in implementing zero trust for your teams if they go it alone. Modifying enterprise networks will take time and may require troubleshooting and retooling of technology teams.

NTT and Cisco’s zero trust solution

NTT and Cisco’s zero trust solution

Together, NTT and Cisco enable organizations to embed zero trust across the fabric of their multi-environment IT stack by securing access in a way that frustrates attackers, not users.

Zero trust capabilities offer four functional requirements:

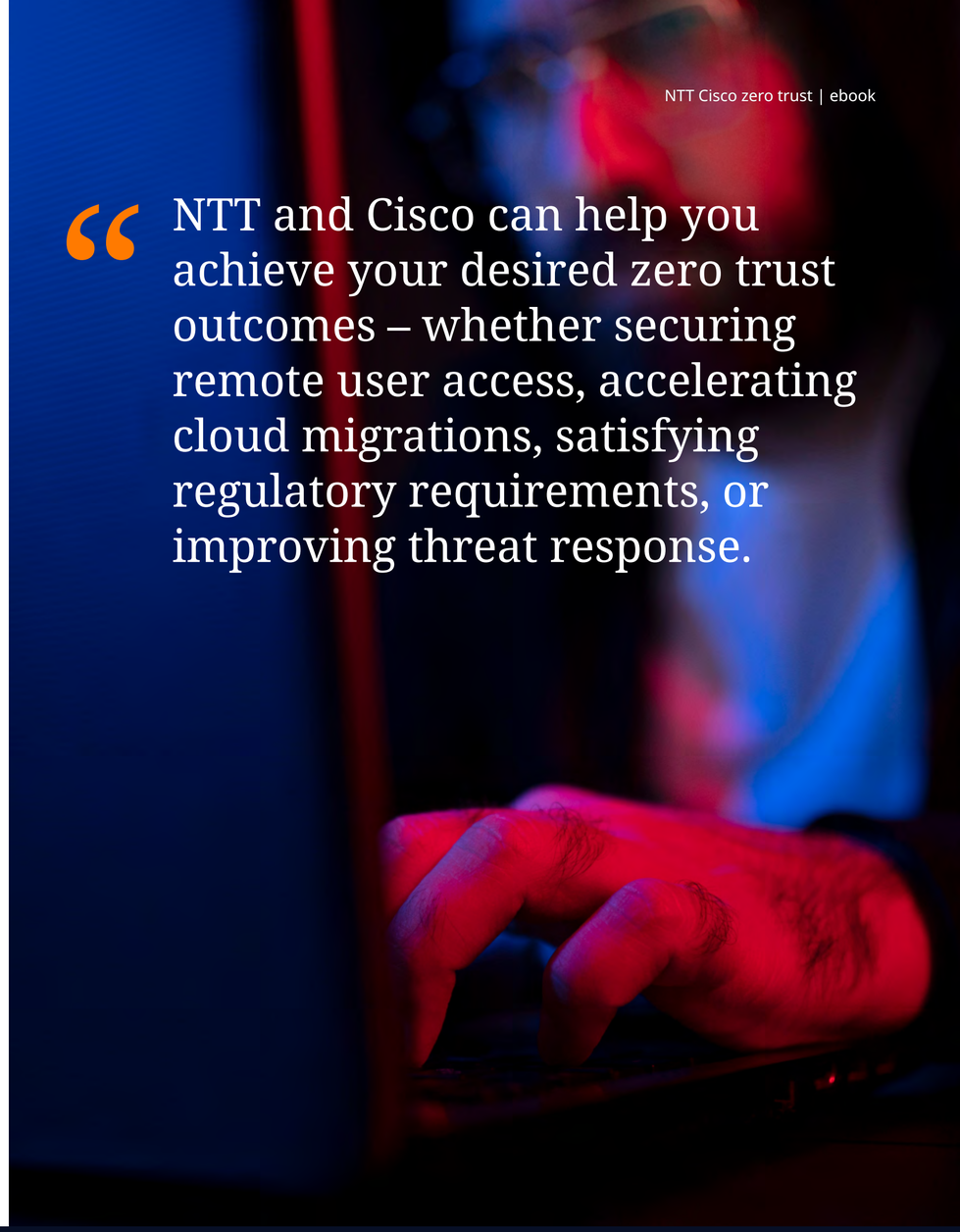
Establish trust
Whether for a user accessing an app, a device requesting access to a network or an app accessing another app.

Enforce trust-based access
So that access is granted explicitly, based on the principle of least privilege.

Continuously verify trust
Even after initial access is granted as change is inevitable, especially when it comes to risk.

Respond to change in trust
By either denying access, prompting the user to remediate, or by granting additional access once trust has been rebuilt.

The strength of NTT and Cisco’s solution lies in the ability to connect shared signals across all control points of user, device, network, cloud, applications, and data – so when zero trust access control policies are applied, they’re informed by real world contextual risk.



> “NTT and Cisco can help you achieve your desired zero trust outcomes – whether securing remote user access, accelerating cloud migrations, satisfying regulatory requirements, or improving threat response.

> Zero trust is cloud scale for a cloud-first world.

Scott Coner, Vice President, Solutions Presales: Systems Integration at NTT

NTT and Cisco’s zero trust solution

There are many complexities in moving to a zero trust model. You may have bought your technology from multiple vendors, using different budgets linked to teams in your business that still work in silos. The cloud team won’t necessarily inform the security team about changes in the cloud, and the security team’s efforts may then not extend to the virtual cloud network too.

Your security infrastructure may also need investment. Does it still do the job? Does it need replacing?

This is why organizations choose to work with an experienced third party to complete a cloud and cybersecurity assessment to establish how secure they are now, where the pain points are and what level of security they need – and, of course, how that aligns with their technology and cloud strategy.

NTT and Cisco’s zero trust solution

Our comprehensive approach to securing all access across your networks, applications, and environment, covers:

Workforce

To prevent breaches caused by stolen passwords, verify users’ identities using multi-factor authentication (MFA). This adds another layer of security to ensure your users are who they say they are before they’re granted access. Gain visibility and insight into the security hygiene of users’ devices, for example to ensure they’re running up-to-date software and they’re encrypted or passcode-protected. Identify whether or not the device is trusted and corporate-managed. And finally, respond to potential breaches of trust, by enforcing access policies for every application that limits access to trusted users and devices – and blocks any access attempt that doesn’t meet your security standards.

Workloads

Securing all connections within your applications, across multi-cloud environments. Contain breaches and minimize lateral movement with fine-grained application segmentation based on application behavior. Gain visibility into your applications, containers, and data across your multi-cloud environment, as well as workload relationships, components, communications, and dependencies. Enforce workload policies in an automated and scalable way. Respond to potential threats, block communication if any policies are violated by detecting both software vulnerabilities and any indicators of compromise – such as activity that is similar to how malware behaves (e.g., privilege escalation or shell-code execution).

Workplace

Securing all user and device connections across your network, including IoT. Protect access to your network by granting the right level of access to users and devices with network authentication. Gain visibility into what’s on your network – including users and devices (IoT and others) – and segment your network to protect access to critical business assets. Respond to risks by detecting and containing infected endpoints and revoking network access whenever suspicious activity, malware, or malicious behavior is seen on your network.

Case study

Universal Robina Corporation

Universal Robina Corporation (URC) Vietnam is a leader in the food and beverage industry in Vietnam with a key focus on using the cloud to adapt quickly to their changing business needs. Working with us, they created a zero trust environment to ensure that all users had secure access to all their applications, wherever they were located. With their devices and applications now secured, they can focus on driving innovation in their market and ensure they remain a leader in the food and beverage segment.

Read our case study

Why NTT and Cisco

Why NTT and Cisco

NTT and Cisco have built a close technology partnership, with more than 30 years' experience of addressing customers' complex challenges together. It has led to the co-creation of proven, full-stack solutions and services from infrastructure to applications, serving 75% of Fortune 100 companies.

Our deep understanding of each other's technologies has enabled us to co-innovate where networks, cloud, and applications converge – including in cybersecurity – and offer customers the benefit of our reach and experience. We'll enable your hybrid workforce to work productively and securely from anywhere.

Global presence, local support

As more businesses become interconnected, a breach can have a ripple effect. NTT has a global presence and can provide consistent zero trust security services to clients in different regions of the world.

Best of breed partnership

NTT's partnership with Cisco enables organizations to embed zero trust across the fabric of their multi-environment IT stack by securing access in a way that frustrates attackers, not users. For business and security leaders struggling to reduce risk at scale, we help to achieve zero trust progress without compromising on user experience and productivity.

Holistic approach

NTT's zero trust security framework is based on a holistic approach that takes into account the entire security ecosystem of an organization, including its people, processes, and technology.

Find out more about our zero trust solution

About us

About us

About NTT Ltd.

As part of NTT DATA, a USD 30 billion IT services provider, NTT Ltd. is a leading IT infrastructure and services company serving 65% of the Fortune Global 500 and more than 75% of the Fortune Global 100. We lay the foundation for organizations' edge-to-cloud networking ecosystems, simplify the complexity of their workloads across multi-cloud environments, and innovate at the edge of their IT environments where networks, cloud, and applications converge. We offer tailored infrastructure and ensure consistent best practices in design and operations across all our secure, scalable, and customizable data centers. On the journey toward a software-defined future, we support organizations with our platform-delivered infrastructure services. We enable a connected future. Visit us at services.global.ntt

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future.


NTT DATA
CISCO