Security

Zero trust security

Five-step roadmap to zero trust

Stephen Mills
SVP, Information Security Services, NTT Ltd.

In the past, employees used to go to the office each day to work. Enterprise security assumed that people in the building with the correct username and password could access systems. However, the moat-and-castle approach is problematic, even with added security features such as multifactor authentication (MFA)

Hybrid working means people connect to work systems from anywhere and from various devices, complicating the IT environment and making it more difficult to secure. The traditional model can cause extra work for people trying to do their work, making it more likely that they'll find workarounds.

Cyberthreats have become more sophisticated and more difficult to detect, which means security procedures have to evolve quickly. Organizations need to optimize security investments and integrate new technology with current systems. The default assumption of trust even with checks and balances has become medieval.

What is zero trust?

There are many definitions for zero trust; however, the core tenet is to change the paradigm from a more traditional security model that implicitly trusts to one that never trusts, and always verifies continuously. This framework enforces a model where every request for access is authenticated and authorized before access is granted, regardless of your location. User behavior is constantly monitored and analyzed, making it possible to detect and respond to anomalies in real time.

Why do you need advanced security?

Zero trust and its benefits are no longer limited to tech-savvy businesses with deep pockets; technologies that underpin zero trust's goals have become more accessible and affordable. Increasingly, advanced security features such as zero trust are now expected by business partners to give assurance that their information is being processed securely, and for insurance companies to confidently provide insurance coverage — ultimately, you need zero trust to earn their trust.

Organizations use zero trust to:

- Better protect their people, clients, data and themselves.
- Enhance flexibility since their people can securely access resources from anywhere through various devices.
- Improve their employee experience and boost adherence by simplifying security applications and tools.

5 pointers for zero trust planning

You're ready to adopt zero trust. Now what? Many articles and publications describe the concept of zero trust and offer insights into how to plan and implement zero trust in your organization.

I've set out five steps you should consider to get you started on planning how to make zero trust work for your organization. You don't need to follow them in order.

1

Understand your entire IT and business environment

Zero trust is an all-inclusive approach to ultimately protect your sensitive data and valuable assets. To do this, you must understand all your platforms and infrastructures including, but not limited to, identity, endpoints, clouds, applications and networks.

Your organization must conduct a current-state assessment to understand the scope and size of your environment. Use this all-encompassing, 20,000-foot view of the estate to map the span of the new zero trust architecture.

2

Use user scenarios and use cases to document your business requirements

A pragmatic approach to zero trust requires you to understand how users will access your systems and applications securely. CISA's roadmap and NIST's architecture framework provide examples of use cases to consider. It's essential to establish your requirements before approaching your technology partners to ensure their solutions meet your expectations for a successful implementation.

3

Understand the art of the possible with your technology partners

You'll have heard — many times — that zero trust is not something you can buy off the shelf. It is an architecture framework that includes many interconnected components such as MFA, microsegmentation, continuous monitoring and user behavior analytics.

The use cases and user scenarios aligned to your business requirements will help you find gaps in your zero trust deployment based on functional capabilities and available integrations. This requires working with partners who have a deep understanding of the capabilities of their platforms. They must be able to translate your requirements into solutions and offer options. The beauty of the zero trust paradigm is that there is no right or wrong way to design or implement it.

Few technology partners can achieve an end-to-end solution without bringing in additional partners. In most cases, end-to-end solutions require a complete level of adoption across CISA's five pillars: identity, endpoints, network, applications and data. If the architecture requires multiple technology partners, you need a strong understanding of the interdependencies, risks, considerations and any limitations known to ensure they align to your business objectives. Any gaps that off-the-shelf solutions do not close may require custom integrations. It is highly desirable to limit the number of custom integrations or limit development to as few as possible, as these require additional maintenance and ensuring compatibility between each of the technologies.

Essential reference points

- The Cybersecurity and Infrastructure Security Agency (CISA)'s Zero Trust Maturity Model roadmap shows how an organization can tackle zero trust using a maturity model approach.
- The National Institute of Standards and Technology (NIST)'s Zero Trust Special Publication 800-27 incorporates logical components and example use cases.

> The beauty of the **zero trust paradigm** is that there is **no right or wrong way to design or implement it.**

4

Build a roadmap aligned to the CISA maturity model and what's technically possible

The CISA maturity model provides a foundation for adopting zero trust in a phased approach. Every organization has a different level of maturity and therefore timelines to adoption will vary. Knowing where you stand is crucial to understanding where you are as part of that journey. Incorporating the output of the current-state analysis will assist with the assessment process. By the end of the exercise, you should have documented a detailed list of technology partners and solutions that map to each step in the maturity model.

CISA maturity model. Source: Cisa

As part of the roadmap, take the time to instill confidence in executive stakeholders that the program has the necessary metrics to track and report key dependencies, milestones and budgeted costs. You can split up the roadmap into multiple project horizons. For example, horizon 1 may focus on establishing the identity platform and the tactical uplift of existing security controls. Horizon 2 will focus on deploying the foundation zero trust platforms and enforcing policies to protect applications and data. Horizon 3 may focus on further bolstering the controls by expanding the capabilities required by advanced automation and correlating multiple zero trust signals.

5

Obtain executive buy-in to support the program holistically

Senior executive leadership is critical to ensure the zero trust program will be successful. Information security teams that pitch zero trust need to prepare a narrative that closely resembles their business, incorporating information such as known previous incidents that could have been avoided had zero trust been in place, in addition to managing insurance premiums and improving the user experience in accessing applications.

To successfully deploy a zero trust project requires the cooperation of many organizational functions including IT and HR departments. A huge dependency on the cooperation between Information Security and IT is essential to ensure key controls are enforced across infrastructure. Engagement with HR is also critical in identity centric zero trust architectures that rely on having a robust human resources information system (HRIS) that keeps track of all employees, partner and contractor identities so that appropriate employee entitlements to applications are defined and managed.

Take the next step

When you need a partner to help you capitalize on your planned investments, we can help you accelerate your journey to software-defined. We have the experience and global resources to support your transition to a new operational model designed to maximize the performance of your new and existing assets.

We can help you implement a roadmap to a software-defined network designed to deliver the full value of your investment. Technology transformation calls for operational change — you can now enhance your support model with services designed specifically to realize the benefits of your new technology. Our Software-defined Infrastructure (SDI) Lifecycle Services provide the visibility and control you need to ensure your software is as consistently managed as your legacy hardware.

Find out more


NTT DATA