ZERO TRUST –
A SECURITY MINDSET FOR MODERN BUSINESSES

advance

ZERO TRUST – A SECURITY MINDSET FOR MODERN BUSINESSES

Long before the covid-inspired work-from-home revolution, the traditional enterprise security perimeter was already disappearing. With remote work poised to be a mainstay of future business operations, and more and more businesses adopting software as a service (SaaS) subscriptions, the idea of securing a network inside four walls is no longer relevant.

While many solutions exist that attempt to draw a secure "perimeter" around outside assets, modern best-in-class cybersecurity is based on a zero-trust approach.

"Zero-trust" is one of the hottest buzzwords in cybersecurity today[1]. The term describes a systematic approach to minimising, or even eliminating, implicit trust and instead continuously confirming every digital transaction. While traditional methods aim to protect networks and assume everything within them can be trusted, zero-trust focuses on safeguarding resources.

In a recent study of IT professionals[2], Australian respondents were substantially more likely (88%) than their counterparts in Malaysia (75%), Singapore (65%), India (62%), or Japan (43%) to be investigating a zero trust approach. In fact, following a sharp rise in cybersecurity incidents, more than a quarter of Australian respondents had begun implementing zero-trust in 2021 alone.

This article will cover everything businesses need to know about zero-trust and why it should form a key part of their cybersecurity strategy.

[1] https://csrc.nist.gov/publications/detail/sp/800-207/final
[2] https://www.technologydecisions.com.au/content/security/news/australia-leads-apac-in-adoption-of-zero-trust-25447591

HOW DOES ZERO-TRUST WORK?

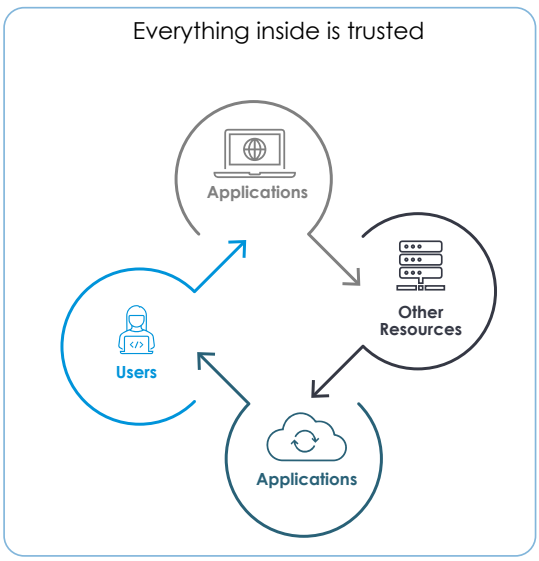
Zero-trust is the movement away from always trusting whole networks, to validating trust every time, for every device, connection, and resource.

Traditionally, trust was given to any device connected to the corporate network. This provided connectivity to other devices and resources, such as network shares and applications. This can be exploited by attackers, who breach the corporate network, or a device trusted by the corporate network and gain access to everything inside the network.

In a zero-trust architecture, there's no such thing as a traditional secure network perimeter. Instead, security policies are continuously applied to new connections based on multiple contextual factors and aim to provide the least access required without hindering work, rather than presuming trust.

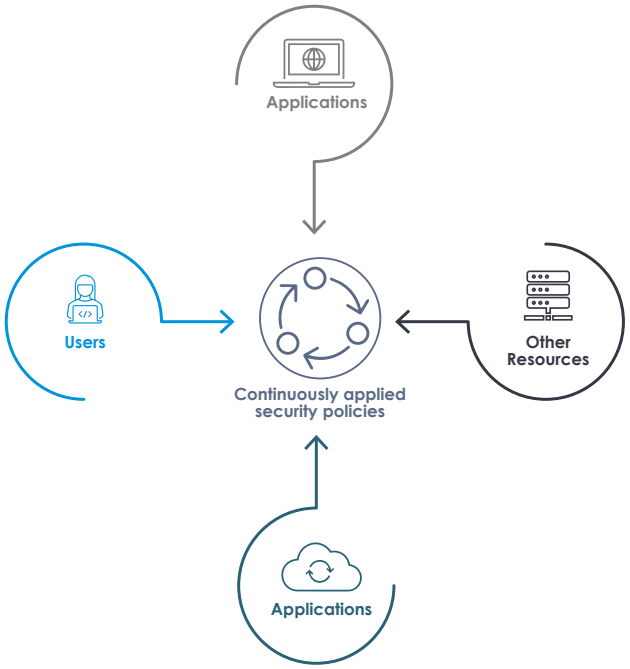
Done well, zero-trust improves user experience and cyber defences while facilitating remote work, bring-your-own-device (BYOD) and cloud-based services. With people and resources dispersed worldwide, zero-trust is a fundamental change in security mindset. It is not a single solution but an approach to implementing security across all business systems.

Traditional Perimeter Security



Zero-Trust Architecture

Trust is established for every connection



FUNDAMENTAL TENETS OF THE ZERO-TRUST MODEL

1. CYBERSECURITY THREATS ARE INEVITABLE

Traditionally, network security assumed that everything within the network was 'safe' unless a threat had been detected. This leaves resources vulnerable when a breach does occur, and the compromised device can leverage the implicit trust it has to access and compromise further network resources. Zero-trust acknowledges that in today's world, threats are inevitable and ensures the network is prepared to contain and isolate them to reduce their impact.

2. UTILIZE GRANULAR, CONTEXT-BASED POLICIES TO PROTECT DATA

Traditional perimeter security focused on building a secure border around all resources and keeping untrusted people outside. Meanwhile, any device within the perimeter was implicitly trusted and allowed access to resources. For example, an employee could immediately access their company's shared drive simply by connecting to the office Wi-Fi. Working from home was enabled by a VPN (virtual private network), which extended the "perimeter" to include the connected device. Unfortunately, this model meant that if attackers could gain access to the corporate network or even the VPN, they could move laterally and access devastating amounts of corporate resources.

In a zero trust model, connecting from the corporate LAN may be only one factor in determining trust or may not be used at all. Various other contextual factors—including country of origin, type of device, user role, what application they're requesting and how—are factored into the trust equation. More advanced factors such as pattern analysis and user heuristics may also be included. This enables frequent authentication without impacting the user experience and facilitates dynamic permissions being assigned based on the calculated level of trust for every connection.

3. AUTHENTICATE EVERYTHING, EVERY TIME

In the old perimeter security model, authentication happened once, allowing a device onto the corporate network. Because there is no trusted network in a zero-trust architecture, authentication occurs for every new connection.
This approach ensures that even if a device and its connection are legitimate and trusted today, they will be revalidated before their next session, removing the risk of trusted devices becoming compromised and causing a breach.

4. MITIGATE RISK BY REMOVING THE ATTACK SURFACE

Users in a zero trust architecture always connect directly to the programs and resources they require, never to a network containing those programs and resources. This means there's no "perimeter" for an attacker to breach, forcing them to focus on individual resources or devices. But even if they manage to breach a resource or device, their access is confined to that resource; there's nowhere for them to move laterally and 'discover' other resources to compromise.

ADVANTAGES OF A ZERO-TRUST ARCHITECTURE

Zero-trust is essential to ensuring future security as cybersecurity threats grow and business becomes more dispersed. It enables businesses to secure more data by implementing multiple layers of protection and better contain any potential data breaches.

Here are some of the most notable advantages of implementing zero-trust:

ACCESSIBLE FOR SMES

Moving to a zero trust approach doesn't need to be a time-consuming or costly endeavour. While a full-scale overhaul from traditional perimeter security to a complete zero-trust architecture would be a large project (and have equally large benefits), businesses can transition to zero-trust over time with minimal impact on the budget.

Many SMEs already have elements of zero-trust in their toolkits without realising it. Modern SaaS solutions, such as Microsoft 365 and Google Workspace, already incorporate zero-trust and have features and functionalities to extend the practice across the ecosystem. As SMEs move away from traditional server-client infrastructure, zero trust principles are often inherited through the cloud-based SaaS platforms that replace them.

Even taking the approach beyond SaaS can be done for a reasonable cost. However, each business's spending on zero trust practices will vary according to the value of the data it has to protect. Like any cybersecurity investment, spending on zero-trust should be considered risk mitigation and tailored to the potential business damage caused by a successful cyber attack.

REMOTE MANAGEMENT

A key benefit of a zero trust network architecture is the ability to fine-tune each user's access to resources—even when working remotely. (Conventional VPNs, on the other hand, typically give users much broader network access than they need but can only connect them to a single location.)

A zero-trust network can be dynamic and flexible without compromising security. Access controls can be created based on identities and characteristics rather than merely IP addresses to instantly change access and privileges and to isolate crucial systems with granular micro-segmentation.

As work from home becomes a standard approach and business-critical apps are hosted by cloud vendors, zero trust solutions offer remote access that is significantly more scalable, efficient, and resilient than that provided by typical VPNs.

SIMPLE TO INTEGRATE

Over time, businesses should strive to cover all of their resources under zero trust security strategies, including anything 'on-prem' such as servers and laptops and internet-based resources.

A robust zero trust solution will integrate with a business's existing identity management system. As a result, users will enjoy a streamlined authentication and access experience across all the devices, corporate systems and resources they use. Zero-trust-based access controls automatically follow users across their devices, offering uniform security for all resources.

IMPLEMENTING ZERO-TRUST SECURITY

Implementing best practices for zero trust security will look different for each business. Several organisational factors will impact implementation, including:

- Size of the business
- IT budget
- Resources available to staff
- Number of assets to secure
- Sensitivity of the data to safeguard

Remember, zero-trust is an approach to security rather than a single solution and can be adjusted to fit the unique needs of each business. When implementing zero-trust, there are several areas to consider.

UNDERSTANDING THE DATA TO BE SECURED

The first step to implementing zero trust security is understanding the data the business holds and needs to protect. Questions to ask here include:

- What types of data does the business manage?
- How sensitive is each type?
- Where is each type of data located?

Based on the answers to these questions, the business can decide who should have access to various resources—and, more importantly, who does not need access to perform their role.

The business can then create policies and processes to ensure that access is controlled and managed by each type of data's usage requirements and security implications.

ENSURING RETURN ON INVESTMENT

As with most cybersecurity investments, there are many options and extents to which zero-trust can be implemented. Businesses should use a risk-based approach to determine the right investment level and the technologies used to implement zero-trust.

If expertise does not exist in-house, then temporary expertise or partners can be leveraged to ensure the right technology mix is selected and ongoing operations can be managed.

Without expert guidance, it's too easy to waste a cybersecurity budget on solutions that cover one area of security to a depth not required by the business—leaving other areas of cybersecurity under-invested in and open to exploitation. As mentioned, many businesses are already using software solutions that contain zero trust features. However, vendors attempting to sell a discrete security solution may ignore these options to justify their own costs.

When seeking external assistance in building a zero trust strategy and selecting technologies or initiatives to implement, businesses should look for partners interested in their long-term security rather than vendors who want to sell an individual product or service.

CONCLUSION

With businesses evolving to a distributed model that leverages more external SaaS subscriptions, and cyber threats evolving to take advantage of this setup, cybersecurity must also evolve.

A key part of this transformation is a security approach known as zero-trust. Zero-trust enables increased security and improved user experience while supporting remote working, BYOD initiatives and business-critical SaaS solutions.

Zero-trust is an approach to cybersecurity, rather than a solution in and of itself, and should be considered when securing all technology and data assets.

CONTACT INFO

+61 8 8238 6500

www.advance.net.au

sales@advance.net.au