paloalto NETWORKS | Google Cloud

The Rise of Zero Trust

People-first security in the era of remote work

Digital transformation, cloud adoption and remote work are eroding physical perimeters, creating an imperative for a scalable way to secure remote access for every user and remote location.

The abrupt shift to remote work in 2020 led to increased interest in Zero Trust initiatives from organisations seeking to address challenges as they adapt to an operating model in which working from home has become the **'new normal'**.

Palo Alto Networks believes that Zero Trust is a strategic approach to cyber-security that protects organisations by eliminating implicit trust while continuously validating every step of a digital interaction.

The concept of Zero Trust architecture isn't new. Zero Trust has been around for years.

For example, Google has been working on Zero Trust for more than a decade. BeyondCorp is Google's implementation of the Zero Trust model, embracing Zero Trust principles and the idea that implicit trust in any single component of a complex, interconnected system can create significant security risks.

However, for the majority of organisations, Zero Trust has been a theoretical ideal rather than a practical strategy to be implemented there and then.

That all changed in 2020.

Prior to the COVID-19 pandemic, organisations were already faced with the security challenges of migrating to the cloud. So when lockdowns came into effect around the world, organisations of all types and sizes had to transform operations virtually overnight.

The immediate priority was business continuity – which meant finding ways for teams to work remotely with as little impact on productivity as possible whilst dealing with the newly introduced security challenges.

Every remote worker represented a new workspace to be secured, with every home network and every personal device introducing additional risk.

In larger organisations, the potential attack surface didn't just increase; it multiplied. And cybercriminals were quick to take advantage.

73.5%

of IT leaders are extremely concerned about the security of their cloud-based systems, data and infrastructure[1]

3X

increase in endpoints by 2023 [Gartner], creating more targets for cyberattacks

32%

increase in successful cyber-attacks in 2020[2]

[1] The State of Cloud Security in 2021; IFP

[2] State of Cybersecurity Resilience 2021; Accenture

With no time to develop complex new security strategies, and no option *but* to allow remote work, the simplest option for many businesses was to make their systems as impenetrable as possible.

As a result, employees no longer had the same easy and unfettered access to assets and resources as they enjoyed in the office.

The trust dilemma

Every time an employee is met by the words Access Denied, there is an obvious productivity cost as attention switches from the core task to administrative issues; requesting and waiting for access or coming up with a workaround.

A less obvious cost is to employee morale, not only from the frustration of not being able to work effectively, but also because every denial of access seems to suggest the organisation doesn't completely trust them.

However, it isn't the employee the business distrusts; it's the device.

In the wake of COVID-19, the challenge for organisations is to reestablish a productive and trusted relationship with employees – without implicitly trusting their devices.

Today's organisations are looking for a model of security where secured networks aren't enough. A modern approach is required to truly protect an organisation's most secure assets and allow for your employees to be productive under the right circumstances.

Let's explore what a Zero Trust model really is – busting some myths and repairing the trust.

What is zero trust really?
(And what it isn't)

A Zero Trust model allows for greater security posturing and policy for both applications and devices, while providing end users with a better user experience no matter where they access from or what type of device they use to do so. It embraces the idea that implicit trust can create significant security risks.

Implicit trust is the automatic assumption that once a certain device and a digital asset have proven their right to access and talk to each other, they can continue to do so indiscriminately. Trust is implicitly assumed, meaning further checks and controls are often overlooked for the sake of simplicity and perceived agility.

However, should an attacker find a way to exploit an implicitly trusted connection to a trusted device, they can immediately use it to access and compromise the entire interconnected system.

"Zero Trust is the only cyber-security strategy that aligns with business outcomes and does not focus specifically on preventing compromise or catching threat actors, but on keeping organisations running despite the overwhelming amount of daily cyber-attacks."

Riccardo Galbiati
Cyber Advisor - Office of the CSO,
Palo Alto Networks

Zero trust is a strategy, not a product

As with any technology trend, there will always be some providers who choose to define Zero Trust security within the context of their product or service.

However, no product or service can deliver Zero Trust out of the box. There are no silver bullets, no set-and-forget solutions, no shortcuts.

Security isn't embodied in a tool, but in how that tool is implemented, used and maintained. The best lock in the world is worthless if it isn't installed or used correctly or the key is lost or stolen.

And that means the security of your business in the cloud has as much to do with the people in your business – their behaviours, workflows (and workarounds) and practices – as it does the software, hardware and configurations that comprise the cloud.

In short, security is a relationship between process, technology and the people who use it. The first step in adopting a Zero Trust model is to know your people and know your devices.

61%

of data breaches involve the use of stolen credentials

2021 Data Breach Investigations Report; Verizon

When the network no longer provides the trust required to access critical company information, we instead turn to the information we have about individual employees and their devices. Without a reliable, up-to-date set of data about the people and their machines, we can't make good decisions about access.

For example, Palo Alto Networks begins developing a Zero Trust strategy for a client by exploring and investigating how the organisation operates. In doing so, Palo Alto Networks has identified three common scenarios where an organisation will most likely need to apply Zero Trust:

1. **Remote users accessing critical data and applications.**
2. **Applications built and maintained in the cloud.**
3. **An ever-growing infrastructure comprising old and new assets, such as servers, networking devices, IoT and OT.**

In all three use cases, it is necessary to focus on removing implicit trust, by continuously validating the interactions between digital assets.

Only once this discovery and use-case analysis is done can we custom-fit a Zero Trust model to your business that will support and empower your employees, not restrict and frustrate them – while keeping your digital crown jewels safe and secure.

Zero Trust is about more than identity

It's not uncommon for Zero Trust to be viewed as merely a question of identity confirmation – reliant on solutions such as multi-factor authentication (MFA).

However, this is still a very binary approach to security – each user is either in or out. Usually, out. And if they are in, should the fact they successfully authenticated their device once mean the same device is allowed to indiscriminately access and interact with critical assets?

Meanwhile, credentials such as user IDs and passwords remain the number one target for hackers. Why try to break through all that security when you can target a vulnerable user and steal their (implicitly trusted) front door key?

Instead of an over-reliance on confirming the identities of authorised users, a Zero Trust strategy considers multiple criteria to assess each device and connection in context, while continually monitoring for unauthorised or suspicious activity.

The Kipling Method

A Zero Trust model treats identity as only one factor in determining whether a user should have access or not.

Rudyard Kipling defined the six one-word questions journalists need to ask to get the full story. An effective Zero Trust model can use the same six questions to build a more nuanced and complete picture of every connection.

WHO The User-ID. The identity of the person accessing the resource.

WHAT The App-ID. The application the person is using to access the resource.

HOW The Content-ID. How traffic from the app/user should be handled.

WHEN Any time-delineated rules, such as if the access is within expected working hours or not.

WHERE The location of the asset or resource being accessed.

WHY Any other rules and definitions created to filter out threats while continuing to allow authorised or non-suspicious activity.

Read more about **how to apply the Kipling Method** using the Palo Alto Networks Next-Generation Firewall.

Zero Trust is about IoT, not just remote working

The Internet of Things (IOT) is another area where the ubiquitousness of cloud connectivity butts up against the need to maintain cloud security. Each of those endpoints represent a potential attack vector if it isn't kept as secure as every other part of the network.

That's why a solid Zero Trust architecture isn't solely concerned with user devices. It's also concerned with the growing number and variety of smart tools that we keep adding to our networks.

These always-on IoT devices rely on uninterrupted connectivity to the internet. As such, they can only be secured properly by continuously controlling what they attempt to access, while monitoring the nature of the internet traffic for anomalies.

Palo Alto Networks currently has a list of more than 3,600 applications and App-IDs that can be used to build your rules around user and application traffic. These include the full suite of Google Cloud apps, which enabled so many organisations to quickly transition to remote work.

On top of that, Palo Alto Networks has a number of dedicated IoT modules which are capable of identifying in real time the myriad protocols and non-user devices that constantly communicate over our networks.

Because a compromised device can easily go undetected, all IoT devices should be treated with maximum distrust – or rather, Zero Trust.

Zero Trust is about removing implicit trust from technology, not people

One of the biggest misconceptions about Zero Trust is that it removes trust from people. In reality, the weak link is technology – presenting attackers and bad actors with their best opportunity to exploit trust.

When someone in your business has their credentials stolen or their laptop is compromised, the problem isn't that employees can't be trusted. Instead, it is the device that can no longer be trusted. The technology has betrayed the user by performing unsanctioned background operations or ceding access or control to unauthorised others.

No one expects to be able to access everything. Trust doesn't mean an open house policy.

At the same time, striking the right balance between controls and agility is hard. The number of capabilities and tools required to implement a Zero Trust model can be daunting.

But if you adopt a strategic mindset that relies on a platform approach – for example, with a single vendor that has aligned its entire portfolio of services to support a Zero Trust model – many of the frictions and inefficiencies tend to disappear.

For this reason, Palo Alto Networks has aligned its entire portfolio to the Zero Trust model, allowing us to offer more than 90% of the required capabilities.

A platform approach minimises the need for ad-hoc solutions and point products, which would otherwise require expensive integration with the rest of the ecosystem.

It also means employees encounter fewer (if any) restrictions because the strategy is shaped to how they work – the very work you trust them to do well.

With the right approach in place, a Zero Trust strategy can actually build greater trust, empowering employees to produce their best work unhindered.

In short, Zero Trust isn't about distrusting your employees, requiring them to continually justify themselves to access what they need.

Zero Trust is about ensuring trust isn't even an issue.

Cybersecurity that doesn't just react to threats, it stays ahead of them.

In 2021, Google assembled a group of partners that share its Zero Trust vision, with a commitment to helping their joint customers make that vision a reality: the BeyondCorp Alliance.

These partners are key to Google's effort to further promote and democratise this technology. They allow customers to leverage existing controls to make adoption easier, while adding key functionality and intelligence that enable customers to make better access decisions.

Palo Alto Network's long partnership with Google Cloud has resulted in a joint security plan, built on secure connectivity between our respective services within a Zero Trust model.

An example of this partnership is Palo Alto Networks Prisma Access service, offering remote users complete Zero Trust network access. Prisma Access is fully hosted across Google Cloud Compute's 100+ locations, providing customers with maximum coverage.

The Google Premium Network also ensures Prisma Access customers experience market-leading low-latency – whether they're accessing Google services or other cloud providers.

All of Palo Alto Network's Zero Trust capabilities available to remote users are possible only thanks to its proven partnership with Google Cloud.

Integrated
with the latest capabilities as needed to achieve the best possible visibility, control and efficiency.

Automated
to respond quickly and eliminate threats at scale while reducing the complexity and number of security tasks.

Simplified
so your team(s) are free to operate and innovate faster with less risk – making a secure cloud transition a lot easier.

Palo Alto Networks, Google Cloud + You = Better, Together

Ready to put Zero Trust theory into action?

Download our white paper on

Architecting the Zero Trust Enterprise

paloalto NETWORKS

Level 28, 100 Mount Street
North Sydney, NSW, 2060
Sales: 1 800 870 869
Support: 1 800 002 378
www.paloaltonetworks.com.au