twenty three.

Evolving the zero trust approach

Hewlett Packard Enterprise

Cybersecurity risks aren't going anywhere. In fact, they're growing daily.

Here in Australia, a cybercrime is reported every 6 minutes, with ransomware alone causing up to $3 billion in damages to our economy every year.[1]

Increased activity at the edge of networks means there are now far more targets, and more opportunities for criminals to exploit. We're living with the reality that the more reliant we become on technology, and the more our IT networks expand, the more prevalent cyber incidents will become.

For over a decade, cybersecurity experts have recommended a zero trust approach to security. This approach assumes any user or device accessing a network is a potential threat—intentionally or otherwise—and therefore requires continuous verification and authentication.

While zero trust remains an extremely important and critical approach to security, A23 takes it a step further. Partnering with HPE, we go beyond the implementation of technology to provide businesses and governments with agile, holistic, and fully customised zero trust solutions. We also take a 'now and next' approach, which sees cyber resilience as an evolving, dynamic, and opportunity-rich space in which we can design, build, deploy and positively enhance our clients' cybersecurity postures, both now and in the future.

In this whitepaper we examine the challenges of cybersecurity in greater detail, discuss key considerations for an effective approach to zero trust, and highlight how together, A23 and HPE can deliver the positive protection today's organisations need.

> "Cybersecurity is an urgent national problem, and we need to act now... over the past 18 months, millions of Australians have been affected by devastating cyber incidents."
>
> The Hon Clare O'Neil
> MP Minister for Home Affairs
> Minister for Cyber Security[2]

In this whitepaper

What is zero trust?

Traditionally, security was provided at the perimeter of a network, with firewalls preventing unauthorised access.

As networks have expanded in size and complexity, threats have increased in sophistication, and hybrid working has become commonplace, this perimeter-based approach to security is no longer sufficient.

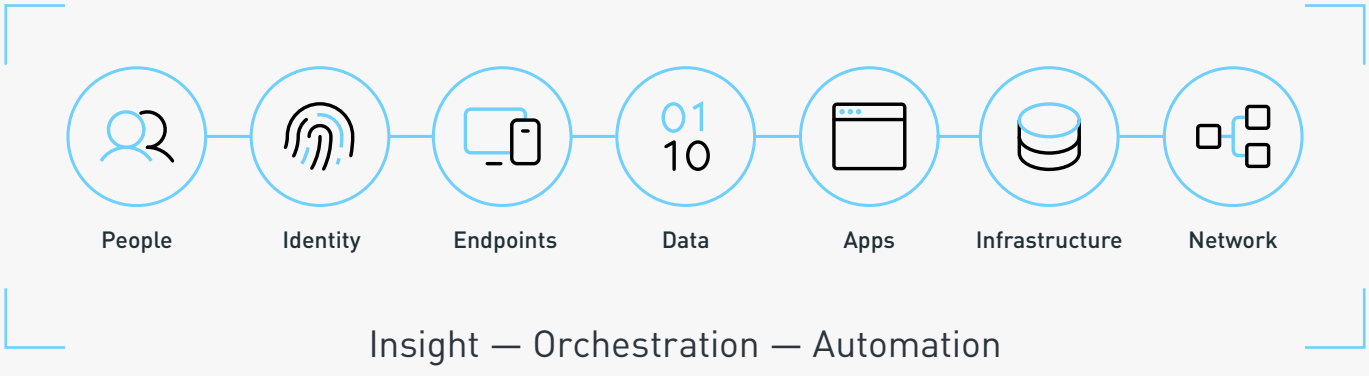
First gaining adoption around 2010, zero trust is a sophisticated approach to security which assumes every user and every device which accesses a corporate network is a potential threat. The threat could be intentional or simply accidental: 88% of all data breaches are caused by an employee mistake.[3]

The zero trust approach is based on the principle that no user, even if allowed to enter the network, should benefit from default trust, as that person could be compromised. Certification and authentication of identities and devices are required throughout the network.

Each component of the network must independently establish its reliability and be authenticated by any other component with which it interacts, including existing one-off security measures.

Ideally, a zero trust model should encompass every element that could pose a threat to an organisation's security, including identity, endpoints, data, apps, infrastructure, and the network as a whole. It should also be overlaid with automation to ensure the efficient and reliable detection of threats, as well as orchestration, and tools which offer clear visibility and insight for IT teams.

Zero Trust Security



What are the challenges of a zero trust approach?

While a zero trust approach is crucial for today's businesses and governments, its adoption can bring challenges. A recent survey found that while 57% of organisations are receptive to a zero trust approach, only 30% have partially or fully implemented it.[4]

1 — Piecemeal approach that creates gaps

Many technology providers market their solutions as designed with zero trust principles. This leads organisations to believe the technology will—entirely on its own—automatically deliver the level of security they require. In reality, 'all-in-one' zero trust solutions simply don't exist.

Switching 'off' legacy systems and implementing new technology can also create gaps that can be exploited by cybercriminals. Once a new zero trust solution is deployed, it's not uncommon for organisations to take a 'set and forget' approach, assuming ongoing and automatic protection.

2 — Negative impact on productivity

To support the new world of hybrid work, it's important that organisations give employees the tools and technologies to do their best work and drive the organisation forward—all while providing an environment that offers flexibility and collaboration. However, many proprietary zero trust security solutions will also impact productivity and efficiency.

Tightening processes and requiring continual authentication can affect day-to-day work, and quickly frustrate users. By contrast, a future-focused zero trust solution should enable employees to move freely with flexibility, secure in the knowledge that threats are being proactively neutralised without the need for cumbersome policies that drain productivity.

> "Most companies customise their zero trust strategies using a piecemeal approach, but gaps or cracks may develop that make zero trust less ironclad than advertised. At the same time, unwinding legacy hardware and software can create unexpected security lapses."
>
> Tech Target [5]

> "The challenge is that most of these apps do not go through an official purchasing process and are used outside of the governance of security... integrating into a zero-trust security framework would require weeks or months, which negates productivity and enterprise agility benefits."
>
> Forbes Technology Council [7]

3— Incompatibility with IT infrastructure

There are considerable risks from proprietary zero trust solutions not supporting open integration and automation. Incompatibility with the rest of the organisation's technology (which can limit efficiencies) results in data silos, and increased complexity for IT teams.

Merging zero trust technology with legacy systems simply isn't always possible, which can require custom-built solutions to fill the gaps, that can be costly and difficult to manage.

4 — Need for continued maintenance

Many organisations underestimate the effort involved in maintaining a zero trust model, especially as the organisation evolves over time. For zero trust to be effective, it's important that permissions are kept up to date and constantly monitored. Failure to do this can create gaps in security which can quickly become entry-points for cybercriminals.

05 — The rise of shadow IT

To deliver a positive impact, a zero trust approach requires a current and comprehensive registry of all devices and users which access a network. When users independently download solutions which are not part of the approved network, or utilise non-controlled devices, it can compromise the integrity of the entire solution. 77% of IT professionals are concerned about shadow IT becoming a significant security and maintenance issue.[6]

Realising the full potential of zero trust: key considerations

Take a ‘now and next’ approach

Many ‘off the shelf’ zero trust technology solutions have an immediate focus: protect the organisation and its infrastructure now, but do not give enough consideration given to how the approach will evolve or scale over time. This short-term thinking can impact the longevity of a solution and the level of protection it can provide.

It’s why A23 takes a ‘now and next’ approach, in which we continually review and enhance your security posture. We also recommend starting small and evolving your zero trust security over time, so you can scale at a pace that’s right for your organisation—without risking gaps along the way.

Implement intelligence and automation

As the volume and velocity of threats continue to increase, it’s becoming increasingly important that organisations leverage artificial intelligence (AI) and machine learning to keep pace.

Without automated monitoring in place, it’s extremely difficult for IT teams to effectively detect any vulnerabilities and respond to any potential beaches, while still maintaining the level of control required for a zero trust approach to be effective.

Focus on training and awareness

For a zero trust approach to succeed, developing and fostering a culture of security awareness across all levels of the business is essential. Education about the latest phishing schemes and social engineering tactics reduces the risk of successful attacks. Regular training and simulated cyber-attack exercises can also prepare your team to recognise and respond to threats more effectively.

Work with trusted partners

Collaboration with trusted partners with a proven track record in securing and recovering from cyber threats is invaluable. These partnerships can provide access to technologies and expertise that enhance your ability to anticipate, withstand, and recover from cyber incidents.

> “AI combines incredible speed, precision, and depth of data to give organisations a contextually-rich understanding of the threats that zero tarust practices aim to root out.”
>
> Cyber Risk Alliance[8]

A23 and HPE: a security-focused partnership

Hewlett Packard Enterprise

At A23, we approach cyber security as an agile philosophy, not an absolute, catch-all technology. We regard zero trust as a neutral, trusted space we configure for, and protect our clients within.

We leverage our long-standing partnership with HPE, and our deep understanding of HPE's technology, to deliver future-focused solutions with a zero trust approach at their core.

Together, we offer a security environment that adds value while also helping organisations reduce costs. Our zero trust approach creates a trusted space where governments and business can operate effectively and provide seamless services, while protecting critical data, assets, and infrastructure.

Our partnership is built on trust, excellence, mutual investment, and client commitment. A23 is an HPE Gold Partner, recipient of the HPE Rising Star Award in 2022, and Silver Partner of the Year 2023.

It starts with the silicon: HPE's edge-to-cloud zero trust security architecture

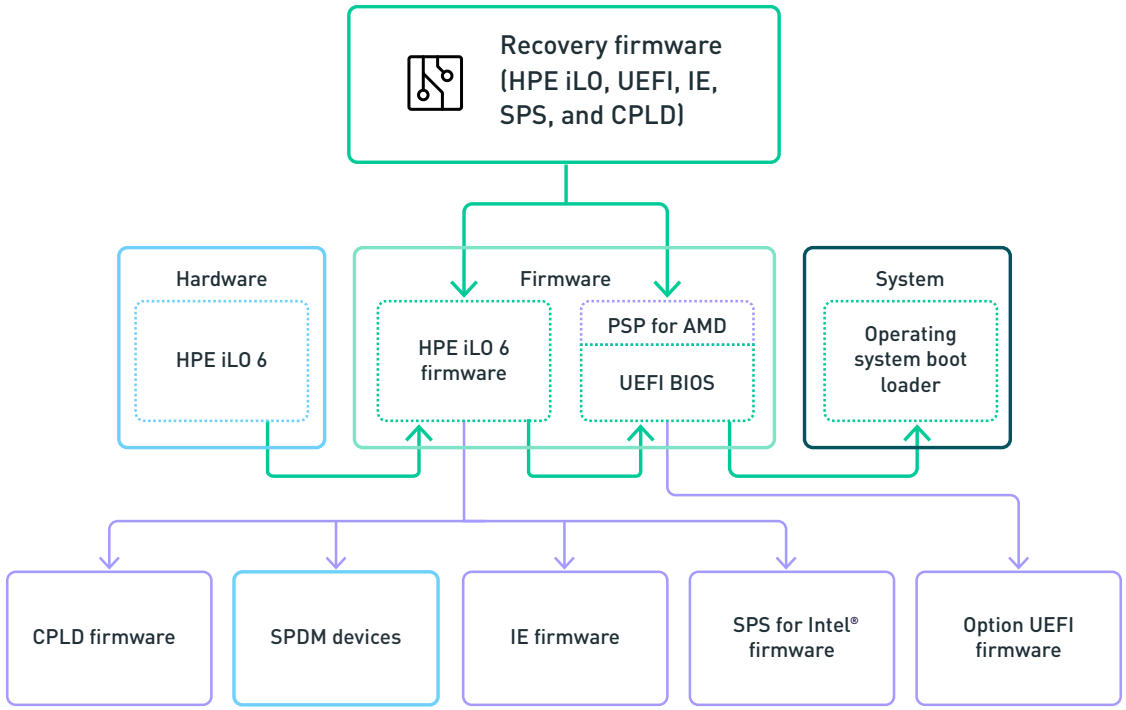
HPE offers an edge-to-cloud zero trust security architecture to help protect customers from some of today's most sophisticated cyberattacks.

It incorporates designed-in security technologies with automated verification and attestation to establish a defence-in-depth approach that begins at the lowest foundational layer—the silicon from which servers are made. HPE refers to this as the 'Silicon Root of Trust'.

By embedding security across a secure chain of trust, from the silicon to the workload, HPE enables organisations to have greater assurance in their distributed software systems, allowing for more agility and flexibility to bring cost-effective and differentiating solutions to market.

HPE ProLiant servers and as-a-service experiences use the industry's most secure standard servers with integrated 'Silicon Root of Trust', as well as complete firmware protection integrated into each phase of the IT lifecycle: from the supply chain to the end of life to automated firmware security.

HPE Silicon Root of Trust



Zero trust in practice

Are you ready to evolve your approach to zero trust?

When your business arrives at (and stays consistently) within a state of zero trust, you find yourself able to remove the barriers, concerns and blockers that can limit your business potential. As a business accelerant, there's no faster way to gain velocity than to keep yourself within a zero trust space, with A23.

Our capability, experience, and insights in delivering successful cyber security models for federal government agencies over many years means we can develop, deploy and manage a fit-for-client solution that satisfies your current need and determines the steps required to future-proof your cybersecurity posture.

Get started today

If you would like to explore the benefits of a zero trust approach to security for your organisation, get in touch with our team and book the A23 capability maturity assessment.

twenty three.

Hewlett Packard Enterprise

1, 2. Australian Government, 2023 – 2030 Australian Cyber Security Strategy, 2023 3. KnowBe4, 88% of data breaches are caused by human error, 2023 4, 8. SC Magazine, Can AI rescue zero trust?, 2024 5. Tech Target, Top risks of deploying a zero trust cybersecurity model, 2022 6. Security Intelligence, The growing risks of shadow IT and SaaS sprawl, 2023 7. Forbes, The top five challenges of zero trust security, 2023