ZERO TRUST
Executive Roundtable
Issues Paper
Sydney | Melbourne
2019
Sydney

HOST

RICHARD BIRD
Chief Customer Information Officer
Ping Identity

MARK PERRY
APAC Chief Technology Officer & Principal Architect
Ping Identity

THOR ESSMAN
CEO & Founder
Versent

EDDIE SMITH
CISO & Cofounder
Versent

VENUE HOST

JAMES NORTH
Head of Technology, Media & Telecommunications
Corrs Chambers Westgarth

MODERATOR

TIM SHEEDY
Principal Advisor
Ecosystm

ATTENDEES

JASON LAVERTY
Senior Manager, Major Business Programs - Security
Westpac Group

JOHN MIHALIS
Enterprise Security Architect
TransGrid

PURU NAYAK
Senior Program Manager - Governance & Transformation (IT)
Coca Cola Amatil

KATHERINE SHARAH
Policy Officer, Policy & Legislation
NSW Department of Finance, Services and Innovation

TODD WILLIAMS
Director
NSW Cyber Security Network

CHRISTIAN HAIDER
Manager Cyber Security Policy, Architecture & Compliance
Transport NSW
Melbourne

HOST

RICHARD BIRD
Chief Customer Information Officer
Ping Identity

MARK PERRY
APAC Chief Technology Officer & Principal Architect
Ping Identity

THOR ESSMAN
CEO & Founder
Versent

EDDIE SMITH
CISO & Cofounder
Versent

VENUE HOST

ARVIND DIXIT
Partner
Corrs Chambers Westgarth

MODERATOR

TIM SHEEDY
Principal Advisor
Ecosystm

ATTENDEES

TONY WILSON
Chief Information Security Officer
Latitude Financial

PETER TEIERMANIS
Principal Architect & Member of WoVG IdAM Working Group
Department of Health & Human Services Victoria (DHHS)

JOANNE LU
Head of Cyber Security Transformation Program
Jetstar

JOHN O’DRISCOLL
Chief Information Security Officer (whole of government)
Department of the Premier & Cabinet Victoria

JAMIE ROSSATO
Chief Cyber Security Officer
Orica

ANDY SINGH
IT Services Manager
GE Holdings

CHRIS BETTS
Identity Consultant
Department of Education & Training Victoria
Introduction

Zero Trust Security is an architecture that many believe is the future of cybersecurity – but in order to understand the concept of Zero Trust Security, it is important to understand where we have come from for technology security – and where many organisations are today.

Traditional security models had physical business locations at their core, with a network perimeter on the outside – built like a walled town. This perimeter was built to stop outsiders from getting in. Inside of the perimeter – on the corporate network, access to information is typically restricted at an application level – with users maintaining many usernames and passwords for the systems they need to access in order to get their jobs done. The job of security professionals was to keep the perimeter, comprised of firewall, virus, and other content filters operational and effective.

But over the past ten years this model has broken. The concept of “inside and outside the perimeter” has all but disappeared, as businesses have punched holes all through their firewalls in order to allow remote employees, customers and partners deeper and deeper access to systems that typically resided within a corporate datacentre.

The Zero Trust security model shifts security from the perimeter to individual devices, users, workloads, transactions and data, augmenting network segmentation to protect sensitive resources. This allows all resources to be deployed as if they were exposed to the public Internet, accessible through a user and device-centric authentication and authorization workflow.

This makes Zero Trust architecture significantly easier to adopt. It takes away the need to map data movement across networks and applications and to micro-segment those networks in order to limit exposure – it puts the user of data (human or device) at the centre of the model – and assumes end-to-end encryption so data can never be accessed by users who do not have the encryption key.

As Australian businesses and government departments begin to embrace Zero Trust for a number of uses – for example, to enable BYOD and remote work strategies for employees, to deploy applications, APIs and data in multiple clouds, to support the rollout of digital licensing, to secure mine sites and oil rigs and as an approach to bring Operational Technology and Information Technology together, they have come up against recurring challenges about what secure identity actually is.

Zero Trust Executive Roundtables with Versent and Ping Identity

Two executive roundtables were held recently in Sydney and Melbourne, hosted in partnership with Ping Identity, a leading US-based provider of trust and identity solutions and Versent, an Australian services, product and platform provider. The aim was to stimulate wide discussion on the Zero Trust Model - what it is and why it starts with Identity.

These roundtables included Chief Information Security Officers, Chief Information Officers, Enterprise Security Architects, Chief Technology Officers, along with Heads of Cyber Security Delivery and Transformation Programs, from a range of sectors including banking, aviation, education, manufacturing, transport and energy, who provided unique insights on their challenges and opportunities associated with modernising their cyber security strategy and adopting Zero Trust.

Delegates discussed how identity is not just about people in the organization - it’s about the identities of the applications, APIs, transactions, data and other resources which need to interact with each other with increasing frequency. Some highlighted the challenges of identity management for organisations with a large, diverse populations who need access to distributed resources from anywhere. Others were keen to discuss best practices in delivering a better government experience, while avoiding reputational issues arising.

Ping Identity and Versent would like to thank all those who participated in the discussions for their time and valued opinions which have provided important context to this paper.
The old ways of establishing trust in a corporate environment concerned the perimeter: everything inside the firewall was automatically trusted, and everything outside was regarded with suspicion. With the advent of Zero Trust, along with the rise of cloud services and the impact of bring your own device (BYOD), the old trust models don’t cut it. The perimeter has long since ceased to have any real meaning, with users and resources inside and outside the perimeter, a threat appearing as a legitimate interaction could come from anywhere, both notionally inside the organisation, or from outside.

Beyond perimeter based security, a significant challenge is that many organisations are counting exclusively on usernames and passwords for access control, hoping that this will prevent large scale breaches of data... It won’t.

Key insights gleaned from the wide-ranging discussion

• The current ways of establishing trust don’t cut it – and could negatively impact the security and productivity of your business

• Zero Trust doesn’t mean distrusting everyone

• Confusion reigns about what Zero Trust actually is

• Boards need to care about trust and identity – but often don’t

• For governments, Zero Trust is complicated

The current ways of establishing trust don’t cut it – and could negatively impact the security and productivity of your business
There is an immense amount of confusion about what Zero Trust actually is, and how to organize security around it.

For many companies, Zero Trust is a marketing slogan, one they can wheel out when questions arise about their security posture. Another issue is that identity groups reside within infrastructure organizations, instead of where they should be, as part of the security operation.

Many organisations are struggling when it comes to aligning their operations with Zero Trust principles, as several round table participants pointed out. The question arising is how a security-focused organisation moves forward in an environment that makes it very difficult...
for change to occur. This comes back to the idea that arose in the course of discussions at the round table – that is, Zero Trust is widely misunderstood, and is for many organisations nothing more than a marketing pitch. Moving the needle on Zero Trust means harnessing the board, the security operation and the staff to all move towards high security principles and towards a revitalisation of what identity management and verification means for a modern company.

The board needs to care about trust and identity – but often doesn’t

One of the challenges faced by security staff and organisations is that they haven’t, historically, been good at marketing themselves to management and the board. As a result, boards are often less than concerned about identity management, and are happy to rely on existing practices such as usernames and passwords.

As one participant pointed out, “board members want to receive their board papers on their personal iPads, but this comes with a host of security concerns. So, does security simply roll over and allow highly sensitive documents to be accessed via an unsecure pathway, or do they put in place robust security principles that will require the board member to jump through 2FA hoops? This, and related concepts, are questions that many security leaders have to grapple with daily.

Boards need to understand that risk does not go away, and for security practitioners, it’s an interesting time to be alive as they struggle to frame the case for security as a business cases in a way that hasn’t necessarily been the normal way of them doing things.

“We’re always trying to find a way to make security easier, make it feel better, make it frictionless. Yet, the reality is, is that for each of us that sit in an executive level position for a security function, ultimately the decision on buying something, implementing something has to swing on a primary team that says, it reduces residual and inherit risk for either one or both. If you don’t reduce risk and you bought it, you wasted your money.”

Richard Bird,
Chief Customer Information Officer
Ping Identity

For governments, Zero Trust is complicated

One of the challenges for governments wanting to adopt Zero Trust principles with their constituents is that from a provider and solutions perspective there’s a lack of understanding about real world use cases.

One question that arose in the round tables was how to invoke Zero Trust for an individual that is not able to manage their own healthcare and has to rely on others to negotiate the complexities of the healthcare system on their behalf.

“Common sense has to apply at some point and then has to support investment. Yes it’s hard to do and it can be expensive, but it’s a lot less expensive than losing your business.”

Thor Essman
Chief Executive Officer and Founder
Versent
“How do you invoke Zero Trust for an individual who may not be managing their own healthcare outcomes because they are, worst case scenario, they’re in a coma or their family is managing your health care or in situations where you have students [and], parents need access to direct information that’s associated with the student? I mean, this is what concerns me about Zero Trust is it does not take these complexities into mind.”

Education industry executive

Participants in the round table noted that any delegation model that accompanies a Zero Trust scenario requires extra consideration. As one participant said, we need to be very careful if someone is acting on behalf of someone else. There needs to be additional checks and balances in the identity verification model to take these variations in situation and circumstance into account.

Compounding this problem for governments is the idea that the bad guys are already one step ahead. Today, bad actors aren’t stealing financial details, they’re stealing complete identities and therefore stealing complete people and then using that data as proxies to go out and do bad things.

“I think the risk to government is reputational damage. You see that this lack of trust in delivery of services, even though they might not be digital services. So, I think the challenge for government is not that we want to deliver better government experience, but it’s often around avoiding reputational issues arising.”

Government security executive
Conclusion

Intelligent authentication and authorisation is the backbone of a Zero Trust security architecture. This means the user needs multiple “factors” to prove their identity, with the three factors being something the user knows (like a password), has (like a phone) and is (like a fingerprint), and that access is granted to sensitive resources exclusively in the appropriate contexts. Different user activities might require different levels of authentication and authorisation.

The only way to implement Zero Trust in a simple manner is by actually taking the concept back to its core. Encrypt and secure everything and hand out trust as it is proven and earned. This should involve a simple but effective two or three factor authentication process and an identity management capability that not only manages the gateway but also continually gathers data and monitors usage in order to continually verify the user and manage access levels as dictated by access rules.

The growth in connected devices – in the home, workplace, factory, car and every other conceivable location - will drive the need for new security architectures and paradigms. With IoT devices finding their way into operational technology environments, security leaders should start a conversation about the partnerships and technologies they need to secure their most important assets leveraging digital identity.
Key Terms

Micro-segmentation
This is the process of placing security perimeters into small, isolated areas (or zones) to maintain separate access for different parts of the network. With micro-segmentation, files in a network can be placed in separate, secure zones. A user or program with access to one of those zones won't be able to access any of the other zones without separate authorization. This ties security to individual workloads and prevents lateral movement by bad actors who have breached the network perimeter.

Application Behaviour and Visibility
One of the benefits of micro-segmentation is the enablement of application security that includes built-in policies that define allowed behaviour and protection for each individual build. For example, ideation through development occurs in an environment isolated from the rest of the network so that any breach of an application will be contained and prevent spreading into the rest of the network. Visibility into application behaviour on devices that access applications also needs to be taken into account so that anomalous activity can be detected and action can be taken more quickly.

Multi-factor authentication (MFA)
The use of multi-factor authentication is now widely used and accepted by consumers and stakeholders. Other forms of authentication such as biometrics, for example, are emerging to bolster identity verification.

Least Privilege
This is a principle of information security that grants only as much access as an end user - a device, a worker, a bot - needs for a particular purpose or role for a certain period of time. It's a key part of Zero Trust, identity and access management, and a way to unify end user and data center security. It reduces risk to a segmented level - to applications and data - and is a way of containing or shrinking the perimeter of each individual user and device.
Ping Identity envisions a digital world powered by intelligent identity. We help enterprises achieve Zero Trust identity-defined security and more personalized, streamlined user experiences.

The Ping Intelligent Identity™ platform provides customers, employees and partners with access to cloud, mobile, SaaS and on-premises applications and APIs, while also managing identity and profile data at scale.

Over half of the Fortune 100 choose us for our identity expertise, open standards leadership, and partnership with companies including Microsoft, Amazon and Google.

We provide flexible options to extend hybrid IT environments and accelerate digital business initiatives with multi-factor authentication, single sign-on, access management, intelligent API security, directory and data governance capabilities.

Versent is a services, product and platform company headquartered in Australia. An exclusive AWS premier partner, with Managed Services, Migration, DevOps, Solution Provider and Security competencies. We were founded in 2014 and specialise in automating how change is delivered in the enterprise.

We partner exclusively with Amazon Web Services (AWS) and Ping Identity to offer the industry’s best solutions in data & IOT, cloud migration, AppDev & API, managed services, security and identity.

Versent was ranked #7 in LinkedIn’s Top Startups 2018, placed second in Australian Financial Review’s “Fast Starters” List in 2017 & 2018, won AWS Consulting Partner of the year in 2017, 2018 & 2019 for AUS/NZ and AWS APAC Partner of the year for 2018. We were named Ping Identity’s Partner of the Year for 2018 and “Better Together” Winner in 2018.