



# ZERO-TRUST MINDSET

THE BUSY EXECUTIVE'S GUIDE  
TO ZERO TRUST

”

“Zero trust is not a single architecture, but a set of guiding principles for workflow, system design, and operations that can be used to improve the security posture of any classification or sensitivity level.”

SP 800 - 207, NIST



# TABLE OF CONTENTS

<b>INTRODUCTION</b>	04
<hr/>	
<b>CHAPTER ONE</b>	07
<hr/>	
Zero Trust Implementation Plan	07
Primary Principles	08
Five Step Model	11
Potential Challenges to Zero Trust Path	18
Change is Hard but Implementation is Harder	19
<b>CHAPTER TWO</b>	20
<hr/>	
Priorities to Secure the Workforce	20
The Zero Trust Approach to Workforce	21
<b>CHAPTER THREE</b>	27
<hr/>	
Zero Trust Maturity Model	27
Zero Trust Networking	30
The Pandemic of Cybercrime	31
The Zero Trust Architecture Network	32
Strong Identity and Access Management	33
The Best Defense Against Breaches	34
Continuous Innovation	35
<b>CHAPTER FOUR</b>	36
<hr/>	
Identity and Access are the Core	36
Scaling and Securing Remote Access	37
The Zero Trust Network Access Model	38

# INTRODUCTION


---

Cyber security professionals have the monumental responsibility of defending increasingly dispersed and intricate enterprise networks from sophisticated cyber threats. Adapting zero trust principles is essential to securing sensitive data, systems, and services. The zero trust security model is a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. It eliminates absolute trust in any one element, node, or service. Instead, it requires continuous verification of the operational picture via real-time information provided by multiple sources to determine access and other system responses.

However, it is losing its appeal. A recent large-scale IBRS survey<sup>1</sup> of security professionals reveals over a third of organisations are turning their back on zero trust. This is attributed to the overemphasis on technology solutions since organisations are inundated with various products claiming to provide ultimate security through zero trust technology. There is also a lack of clear implementation guidance that has left many grappling with a patchwork of tools and approaches along with unrealistic expectations of complete protection. The significant shift in organisational culture and practices that zero trust often requires has also led to resistance, resulting in less receptive adoption and disillusionment with the concept.

IBRS has observed that these enterprises share a common emphasis on adopting the latest security products at the expense of grasping the core principles of zero trust. This results in simplistic implementations that fall short of expectations.

1. ['The State of Identity in Australia & New Zealand'](https://ibrs.com.au/wp-content/uploads/2023/04/Organisations-Plans-for-Zero-Trust-for-2023.png), IBRS. (2023). From <https://ibrs.com.au/wp-content/uploads/2023/04/Organisations-Plans-for-Zero-Trust-for-2023.png>



# INTRODUCTION

---

Many organisations also overlook the human factor, failing to recognise that zero trust requires a shift in mindset and behaviour across all levels. Some have poor integration with existing systems and processes that eventually create security gaps, inefficiencies, and complexity. Finally, many continue to struggle to define and measure the success of their zero trust initiatives, lacking clear metrics to assess effectiveness and make necessary adjustments.

Zero trust is an *assumed breach* security model. It operates under the theory that a breach is inevitable or has likely already occurred, so it constantly looks for anomalous or malicious activity and restricts access to only the essentials. The components of zero trust, such as comprehensive security monitoring, granular risk-based access controls, and system security automation are embedded in all aspects of the infrastructure in order to protect critical assets (data) in real-time. By allowing or denying access to critical assets, the zero trust security model encourages the *least-privileged access* approach to be enforced on every access decision.

Implementing zero trust solutions takes time and cannot be done overnight. Therefore, transitioning to a fully mature zero trust architecture all at once is not possible, nor is it even necessary. Incremental implementation can be integrated into the existing environment, allowing defenders to keep pace with external or internal threats.

To ensure that the organisation is better positioned against existing threats, organisations who choose to migrate to a zero trust solution must fully embrace zero trust principles and commit to the mindset necessary for planning, resourcing, and operating under this security model.



# INTRODUCTION

---

To enhance an organisation's cyber security strategy, IBRS recommends keeping critical zero trust elements such as least privilege access, continuous verification, network segmentation, data-centric security focus, and continued emphasis on visibility and analytics. These allow the enterprise to detect and prevent potential breaches, develop more robust defence against threats, and gain valuable insights into potential vulnerabilities.

This process requires thorough deliberation that involves the buy-in of key stakeholders. The new, perimeter-less workplace makes it increasingly hard to defend against threats from all access points. That problem could easily be compounded by the lack of full support throughout the organisation, particularly from leadership. If leadership is hesitant to spend the required resources to build and sustain it, the benefits of zero trust will not be realised. Management must understand that today's IT landscape is highly susceptible to malicious activities, whether through cloud connectivity, user diversity, wealth of devices, or the sheer volume of globally distributed applications and services.



# CHAPTER 1

---

## **ZERO TRUST IMPLEMENTATION PLAN**

---

### EVERYTHING YOU NEED TO KNOW

Zero trust (ZT) barely warranted a mention years ago, but today, organisations are looking into its in-depth implementation to cope up with the demand for secured operations. Businesses want to combat security threats vigorously, and they consider ZT as the ultimate solution. However, ZT is not just a single product, and the implementation is not just one big-bang sprint project. It needs practical and strategic execution, which may take up to a two-year timeframe, or it will simply fail.

As the network-oriented, perimeter-based security model diminishes in usefulness, security experts and tech leaders have turned to the ZT model. It is to keep up with the demand for a hybrid working environment and prioritise Cloud-oriented environment security. The best way to implement ZT is to work with existing security capabilities. Then, gradually migrate to the ZT model.



# CHAPTER 1

---

## PRIMARY PRINCIPLES

---



ZT is a philosophy that is converted into frameworks and roadmaps following its primary principles:

### 1 ● **Never Trust**

Always verify because the robust firewalls that were a well-trusted technology are now obsolete. Change the mindset. You don't trust anything inside and outside your network anymore. The current environment already dictates that you can't control every IP address and every device. Hence, you can no longer assume trust within and all the more beyond the network perimeter.

---

### 2 ● **Granting Access is No Longer Binary**

The difference between outside and inside access is already long gone. Today, it is based solely on the identity and device of the user accessing the application. The main requirement now is that the network knows that the user requesting access to a resource is who they say they are and is verified to access that particular resource.

---

### 3 ● **Authenticate. Check**

In a ZT environment, consistent authentication and authorisation checks are essential in securing the network. Therefore, access controls should be dynamic and must be continuously verified.



# CHAPTER 1

---

With the rising popularity of ZT, organisations opt to buy ZT products and implement them right away. However, no single vendor or provider can deliver all the capabilities and components of ZT. It still depends on your organisation's requirements; hence, partnering with multiple providers will likely occur. Also, ZT implementation needs a practical and pragmatic roadmap to identify the needs and evaluate the vendors' capabilities.

The transition from traditional security setup to ZT may be easy to say, but it requires a massive shifting of investment. Furthermore, it will create an avalanche of technical and procedural change across the organisation.

Hence, you must narrow down the critical key players for your ZT strategy alongside stakeholders' cooperation. Consider these individuals in helping you formulate your roadmap and strategies:

1. The board members who make ultimate decisions.
2. The business and IT executives who will support and approve the budget.
3. The enterprise architects and application owners who ensure that ZT supports the broader IT strategies.
4. The network security and IT ops team that will manage the infrastructure that you are building.



# CHAPTER 1

---


Establish a balanced understanding among each stakeholder and address them strategically. Make them understand the essence of a ZT effort and its roadmap. There would be a deep discussion among decision-makers such as project dependencies, existing security, IT, and business projects.

In ZT implementation, ensure to correctly map and communicate your implementation plan. A carefully laid out plan may help eliminate micro-segmentation that is too granular and disrupts existing network functions. It will also aid the organisation in identifying interdependencies among different sectors that may hamper the overall operation. And, if curated carefully, an in-depth ZT implementation plan will become a solid catalyst for ZT's transformation.

The rise of ZTs popularity led organisations to acknowledge ZT as a way to prevent cyber attacks. However, just like any innovation, there's looming hesitancy on the horizon.

One question that often comes up in most conversations is whether you need a total tech stack overhaul? Not at all. It only requires teaching the core principle of changing how people understand ZT and network security.

Fortunately, building ZT architecture is less complicated than it may appear. The primary reason is that ZT is an augmentation of the organisation's existing architecture. Hence, you can take advantage of the different technologies that you have while deploying ZT strategies gradually. The important thing is that the organisation should be privy, and tech leaders should explain to stakeholders where they are in the implementation process and where to go next.



# CHAPTER 1

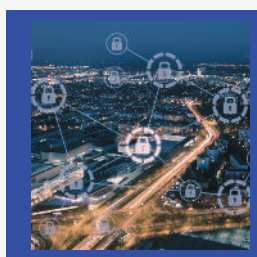
---

## FIVE STEP MODEL

---



Consider this five-step model as a guide for ZT implementation plan:



### 1. Define Your Protected Landscape

Protecting your entire organisation's network is already given, but it is impractical to look at it that way with ZT now.

Moreover, focusing on reducing attacks, threats, and breaches is not viable in today's evolving IT environment. Your network is constantly expanding and changing, making it difficult to define. For instance, one organisation may be fully operating in the Cloud. Another organisation may have a Cloud deployment and on-prem processes for sensitive resources and information. Hence, the idea of guarding the entire organisation network is not applicable anymore under the ZT architecture.

With ZT, tech leaders should identify the specific areas that are high risk. Don't engage on the macro-level of the attack surface anymore. Explore areas susceptible to attacks, such as critical data, applications, assets, and services. Generally, these are the most valuable assets that your organisation needs to protect.

# CHAPTER 1

---

You can start mapping all departments and processes that house critical information such as sensitive personal data, intellectual property elements, sensitive health information, and more. Next, create an inventory of all the critical applications, assets, and services, whether in-house, custom, or vendor-supplied applications that may cause operational disruption if jeopardised.

It is the process of inventorying, risk-ranking, and prioritising inside your protected landscape. Do it precisely so that your organisation will have a good start and leverage the next step, which is to map the transaction flows.



# CHAPTER 1

---



## 2. Map the Transaction Flows

Once you have identified your protected landscape, the next step is to map out its transaction flows. Considering the value of data and information stored in these areas, expect that there should be a volume of traffic converging to it. Thus, it is imperative to gain contextual insight into these vital resources.

Overseeing the traffic flow offers insights on how to protect your valuable resources. Also, documenting specific interdependencies among resources and how they interact creates avenues for stringent protection without hindering your business process.

Mapping transaction flows is doable because ZT networks are entirely customised. It is not derived from a single, universal design. You build your own ZT architecture using your protected landscape and its transaction flows as the foundation. And once you have mapped out your protected landscape, start creating precise and understandable policies among stakeholders. For sure, you have policies in place before; however, your new policies should now embody the ZT philosophy.

# CHAPTER 1

---



## 3. Create Zero Trust Policies

ZT policies are needed to establish the culture, and reconcile the complex environment and mobile workforce. Policies are essential to kickstart your ZT implementation because you can't enforce something if you can't check on it. Policies emphasise the ZT's usability as it protects the network, workforce, devices, and all the vital resources.

Here are some examples of ZT policies:

### A. Implement the Least Privilege

You already identified your protected landscape and mapped out its transaction flows. Now, it's time to restrict employees' access to the specific data or resources they need to do their job. A content marketing manager having access to the organisation's employee database might create a conflict of interest and be used by hackers to access this valuable resource. The manager who only accesses the database for newsletter purposes once a month unknowingly becomes the carrier of malware to steal that information.

# CHAPTER 1

---

## **B. Peer-to-Peer Security Audit**


Hierarchical security auditing is no longer viable due to the veracity of threats created every second. Develop and incentivise peer-to-peer audits, especially for processes and responsibilities that are split between two people. A peer-to-peer audit means employees audit each others' work, which detects incorrect or unauthorised procedures that may create a loophole and facilitate breaches.

## **C. Separate Duties/Processes with Conflict of Interest**

Each user should have specific privileges as not to misuse the system. For example, the person doing the final assembly should not be doing the quality checking and releasing of the product. Doing so allows employees to have a broad accessibility that may trigger breach security policy and may obscure the product's quality at the same time.

## **D. Backup Employee**

An employee with access to critical processes and information is always essential. But, what will happen during their absence? Policies related to critical processes should be in place when vital employees take leave – for instance, an organisation with one technical writer in charge of releasing release notes. Not appointing a secondary person is risky as to who will access pertinent data and information. Mitigate this security risk with concrete strategies such as assigning backup employees up to the third point person.

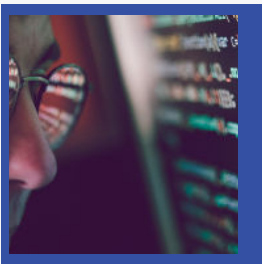


# CHAPTER 1

---

## **E. Random Inspection**

Part of the policies under ZT is random inspection. An organisation needs to audit an employee's device/s to discover fraudulent behaviours. With the mobile workforce where Bring Your Own Device (BYOD) is common, embezzlement also becomes prevalent. Random inspection is ideal, especially when supervision across a hybrid environment becomes complex.



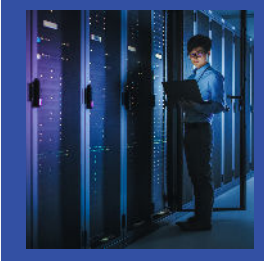
## **4. All About Logs**

Logs are essential to validate the success of any ZT implementation. Historical logs play a vital role in determining the success and loopholes of the implementation. All forms of logs, internal and external, are recorded, from the lowest layer of the Open System Interconnect (OSI) model up to the application layer. Logs such as configuration changes, resource accesses, and network traffic will provide valuable insights into improving the implementation in the long run.



# CHAPTER 1

---



## 5. Adopt a Zero Trust Mindset

A ZT mindset is not only applicable at the start of the journey. It's the classic example of the rinse, repeat, rinse again mantra. Adopting a ZT mindset is a vital key to successfully implementing this philosophy. It should start with the top executives to address dynamic security threats with coordinated and aggressive system monitoring. ZT mindset is always assuming that something wrong will happen. Leniency is no longer part of the equation. People from top management down to the rank and file must assume that all requests for critical resources and network traffic may be malicious. Also, all devices and infrastructure are assumed to be compromised and may incur risks to the entire organisation.

# CHAPTER 1

---


## POTENTIAL CHALLENGES TO ZERO TRUST PATH

---

Just like any disruptive technology or philosophy, implementing ZT in enterprise networks is bundled with challenges. These challenges may reduce or even hinder your operation. The first potential challenge is culture. You can't simply change the mindset of the people and turn them into ZT advocates overnight. Changing the culture needs full support throughout the enterprise, from leadership, to administrators, and finally users.

Changing the mindset is difficult if leaders are unwilling to spend the necessary resources to build and sustain it. That is why the ZT advocacy should come from the top management. Changing the mindset must start with administrators and network defenders avoiding buy-in, circumventing the policies, and trusting the process.

Another challenge is consistency. Fatigue within the organisation and among the workforce will eventually weaken the implementation. Yes, there is adherence to the mindset and application of the ZT security model, but doing it in repetition can be fatal. However, the approach here is a constant reminder and continuous improvement. It instills the idea that repetition is key, and just a one-time act of leniency in the ZT approach will eliminate and degrade its overall cyber security benefits.



# CHAPTER 1

---

Dealing with legacy applications and network infrastructure is also a challenge. However, ZT vendors are now building products compatible with legacy systems and can work with real-time network monitoring solutions. The caveat is that in dealing with legacy systems, the environment is still vastly reactionary. Hence, it is advisable that implementing ZT architecture also considers the compatibility of systems and security technology.

## **CHANGE IS HARD BUT IMPLEMENTATION IS HARDER**

---

The ZT architecture is a game-changer. The model itself is a challenge as there is no defined and universal design that you can recreate or follow. Most of all, the design that you adopted may not be entirely adaptable for every entity in your organisation. It is even difficult for organisations that don't practice security measures at all, like startups.

Adding to the challenge is the rise of the remote work environment, which needs clear strategies for tackling mobile device management. The best way to deal with this challenge is to implement best practices and workflows that empower information security practitioners and the rest of the workforce. Everybody should start thinking of a big-picture strategy to defend against evolving threats, the implementation plan, and perform continuous improvement to implement the ZT philosophy successfully.



# CHAPTER 2

---

## PRIORITIES TO SECURE THE WORKFORCE

---

The biggest question in deploying ZT is how do we get there? In Chapter 1, a sample implementation plan was laid out and several challenges were presented. In this chapter, let's narrow down the details of the most challenging areas by introducing the three pillars of ZT.

The three pillars are *workforce*, *workload*, and *workplace*. Among these three pillars, the workforce is the most susceptible to inherent trust exploitation. The workforce consists of employees, contractors, partners, and vendors that have access to work applications using their personal or corporate-managed devices. On the other hand, workload refers to the application processes while the workplace is the perimeter or jurisdiction with secure access to the enterprise networks.



# CHAPTER 2

---

## THE ZERO TRUST APPROACH TO WORKFORCE


---

Security threats, in general, are initiated by humans. On the other hand, the ZT workforce principle states that the right users and secure devices can access the network and the applications at all times. Hence, here are four things to prioritise concerning the ZT workforce:

### ESTABLISH USER TRUST

Transform your organisation's security credentials practices. For example, start changing the employees' mindset regarding password creation. Using the same password across the organisation is fatal. For organisations that began with relaxed security measures begin by changing the culture of implementing exclusivity. The device used for work is exclusive for work only and will not be used otherwise.

Implement suitable mechanisms and processes to ensure only authorised users can access the resources. There are ways to achieve this process, like multi-factor authentication (MFA) and a single strong authentication factor. To establish user trust, it is imperative to declare that ownership is not a control. Both users and the IT department should validate and extend trust to devices, applications, and networks that they don't own or manage. It applies to the concept of Bring Your Own Device (BYOD), Internet of Things (IoT) devices, and remote working.



# CHAPTER 2

---

Control is established within the perimeter, which is responsible for access control decision-making. The control decision process is carried out by choosing layers and process points (TCP/IP or OSI layers). Also, access decisions should be dynamic and allow the re-establishing of trust, allowing the system to learn. Containment is another way to establish user trust. In chapter 1, the idea of the protected landscape was introduced, which also introduced the segmentation process. Establish user trust among employees to be mindful of the transaction flow and carry out response capabilities to monitor for threat activities, thus limiting its spread by default.

## DEVICE AND ACTIVITY VISIBILITY

ZT is not feasible with device and activity visibility only. Deploy a ZT architecture that provides business intelligence and insights to the people administering the technology. These insights are then converted into informed policies. Trust here is no longer binary nor permanent. Continuous assessment about users' posture, devices, and applications will let the organisation adjust the trust level accordingly. Device and activity visibility is also the main ingredient to create adaptive policies (will be tackled later) to respond to events that raise the risk level. Hence, ZT is continuously improving, finding newly discovered threats and vulnerabilities, and creating policies to combat these risks.



# CHAPTER 2

---

## DEVICE TRUST

How do we establish device trust? Device trust no longer plays around the idea between insiders and outsiders. Whether it's corporate-owned or not, and managed or unmanaged, an organisation can now identify trusted devices it has registered.

The policies surrounding device trust in a ZT implementation are tricky. It would be best if you enforced endpoint controls for risky devices or corporate-owned devices. For instance, real-time notification for users with out-of-date software or unencrypted disks is an excellent way to start.



# HERE ARE A FEW THINGS TO WORK ON WITH DEVICE TRUST:

---



## **Enforce Endpoint Controls**

Leveraging the visibility of devices across your network, especially those endpoints situated in your protected landscape. Create access policies to prevent any risky or untrusted devices from accessing your applications.



## **Identify Corporate vs Personal Devices**

As mentioned, inventory is vital in a ZT implementation. Create a checklist of corporate-managed and personal devices accessing your applications, and enforce policies based on device type. From there, go back to your policies and ensure that your network is designed to issue device certificates that are checked at login. This application-layer approach provides greater insight into and control over your BYOD and mobile environment. Furthermore, it also limits access by any personal devices that don't meet your security requirements.



# HERE ARE A FEW THINGS TO WORK ON WITH DEVICE TRUST:

---



## **Get Detailed Device Logs and Reports**

Part of the implementation plan mentioned in Chapter 1 is the importance of logs. Your organisation must enforce compliance by offering device visibility and detailed reports on user behavior and compromised devices. For example, for mobile device management (MDM), there should be compliance regulations and regular audits requiring user activity and device security logs and reports. A simple logs report where a user on mobile accesses your network from different locations is already a way to enhance your security information and event management implementation.



## **Streamline Authentication and Keep Remembered Devices**

Fatigue and the inability to adapt to change are challenges embedded in your ZT journey. Users are easily annoyed and want to login into their systems quickly. With streamlined authentication, specific devices and platforms are logged and identified as trusted and let users log in without going through the two-factor process each time.

# CHAPTER 2

---

## ADAPTIVE POLICIES

Conforming with your protected landscape, implement requirements for access based on the sensitivity of the resources. Also, the known security state should have desired policies to manage risk levels appropriately. These policies can cover authorised devices requiring the latest OS versions, disk encryption, or step-up authentication based on user access behavior.

ZT for the workforce requires people to use known and approved endpoints to access the most critical data, and applications; hence straightforward and concise policies should be in place. For instance, privileged users dealing with critical resources and processes must use a corporate-owned device, and it is non-negotiable. Policies should be adaptive if valuable insights are gathered based on how users behave according to their access to proxies that enforce access to corporate resources. Enforcement strategies include assessing risk tolerance, threat, user community, regulatory requirements, and right-sizing those policies to achieve ZT for the workforce.

Policies should not be static and must be aligned with the baseline level of trust for all users. It should be formulated with the increased awareness on risk management level to access the most sensitive tiers. Therefore, ZT access policies must be flexible to allow access, allow access but need immediate remediation to improve trust, or establish modus operandi and identities for those deemed untrustworthy.



# CHAPTER 3

---

## ZERO-TRUST MATURITY MODEL

---

The IBRS ZT Maturity Model guides organisations in their transition towards a ZT architecture by offering a snapshot of what level of effective security strategies and implementation plans they currently hold. Enterprises must assess their existing systems, resources, processes, and infrastructure to help better identify current strengths and areas that require improvement.

The IBRS ZT Maturity Model is based on the following valuable principles that can enhance an organisation's cyber security strategy:

1. **Least Privilege Access:** limiting user access to the minimum necessary for their job functions reduces the risk of unauthorised access and lateral movement within the network.
  2. **Continuous Verification:** regularly verifying the identities and permissions of users, devices, and applications helps to detect and prevent potential breaches.
  3. **Network Segmentation:** dividing the network into smaller, more manageable segments makes it easier to control access and monitor activity, reducing the risk of a widespread breach.
  4. **Data-Centric Security:** focusing on protecting the data, rather than just the perimeter, ensures a more robust defence against threats.
  5. **Emphasis on Visibility and Analytics:** continuous monitoring and analysis of network activity provide valuable insights into potential vulnerabilities and ongoing threats, enabling proactive response and remediation.
- 

# CHAPTER 3

The IBRS ZT Maturity Model is composed of four levels, each with distinct characteristics based on the above principles.



# CHAPTER 3

1

2

3

4

**PROJECT  
INITIATION**

**LEVEL 1:  
PRE-ZERO  
TRUST**

**LEVEL 2:  
FOUNDATION  
FOR ZERO  
TRUST**

**LEVEL 3:  
STANDARDISED  
ZERO TRUST**

**LEVEL 4:  
FULL ZERO  
TRUST  
MATURITY**

**NETWORK  
SEGMENTATION**

Network segments are broad, with limited isolation between different parts of the network. Access control is not well-defined, and monitoring is limited.

Network segmentation efforts are underway, but there are still some uncontrolled or overly permissive connections.

Network segments are well-defined and controlled. Access is based on a ZT model, and policies are consistently enforced.

Network segmentation is complete, with strict isolation between segments, and access is tightly controlled using automated policies.

**DATA-  
CENTRIC  
SECURITY**

Data protection primarily relies on perimeter defences, with limited focus on data-level security. Data classification and encryption are rare.

There is growing awareness of the importance of data protection, with initial steps taken to secure sensitive data.

There is a strong focus on data protection, including data classification, encryption, and access controls.

Data is fully protected, with comprehensive encryption, data loss prevention, and robust access controls in place.

**EMPHASIS ON  
VISIBILITY  
AND  
ANALYTICS**

Visibility into network activity is limited, with little analysis of potential vulnerabilities or threats. Incident response is reactive and often manual.

Visibility into network activity is improving, with more regular monitoring and basic threat detection. Incident response is becoming more proactive.

Continuous monitoring and advanced analytics provide real-time insights into network activity and potential threats. Incident response is proactive, with automated threat detection and response.

The organisation has achieved full visibility into its network, and advanced analytics and AI-driven threat detection and response are the norm. Incidents are swiftly identified and mitigated, often before they can cause harm.

# CHAPTER 3

---

## ZERO TRUST NETWORKING

---

### ALL YOUR BORDERS ARE BELONG TO US

The rise of remote working due to the pandemic is inevitable, and as we're facing the new normal, so is the adaptation of ZT architecture. In the previous chapters, we've presented implementation plans and the priorities for securing the workforce. In this chapter, let's dive in on how ZT can protect the organisation's network.

Virtual Private Networks (VPNs) and firewalls are the go-to technologies for organisations with critical processes. It helps the workforce to access resources and assure network protection safely. But what happens if the VPN gets hacked?

According to *THE 2021 DATA BREACH NOTIFICATIONS IN AUSTRALIA*, in July 2021, LimeVPN suffered a significant data breach with over 69k users at risk. The incident compromised critical information such as customer payment details, private keys, and more.



# CHAPTER 3

---

## THE PANDEMIC OF CYBER CRIME

---

The kind of incident mentioned above triggers CISO and other tech leaders to address cyber attacks differently. As a result, organisations take a tremendous interest in the *assume breach* mindset brought on by the ZT philosophy. But a more catastrophic threat has been looming around in the IT world for decades now, the ransomware attack.

In the tight-lipped world of cyber security, ransomware is an open secret. Organisations across the globe tried to battle it eye-to-eye, but when it finally hit them, monetary solutions are always the answer. According to several studies, most Australian organisations have been quietly paying millions in ransoms to hackers who have stolen or encrypted their valuable data and information.

With that, Australia and the rest of the world are facing a *pandemic of cyber crime*. Studies show that there has been an up to 60 per cent increase in ransomware attacks against Australian organisations in the past years. And it is foreseen to increase in the future.



# CHAPTER 3

---


## THE ZERO TRUST ARCHITECTURE NETWORK

---

Ransomware is not just a one-time attack, but a strategically deployed maneuver in the art of threat propagation. There are stages of breaching the network, wherein an attacker may lurk into your network for months before it fully attacks the entire system. Thus, organisations have shifted strategies and priorities to adopt ZT and combat ransomware utilising ZT network access (ZTNA).

ZTNA is a set of technologies that works under the ZT philosophy. It's an adaptive model wherein trust is never absolute. It works around granting users access on a least-privileged basis defined by segmented policies. Some security experts called it a software-defined perimeter (SDP) that provides users seamless and secure connectivity to private applications without ever placing them on the network or exposing apps to the Internet.

Furthermore, ZTNA completely isolates application access from network access which focuses on a user-to-application approach rather than a network-centric approach to security. In dealing with threat propagation leading to ransomware, it isolates infected devices and only grants application access to authorised users, thereby reducing risks to the network.





# CHAPTER 3

---


## **STRONG IDENTITY AND ACCESS MANAGEMENT**

---

To complement ZTNA, an organisation should implement a strong identity and access management practice. Identity holds the core control of your ZT implementation. The organisation can control the devices, network, and application (software and hardware); however, identity and access management fall outside. So, how do you police the workforce identities to work in unity with your network security goals?

A successful ZT network strategy requires identifying threats and how threat propagation works. It should start with identity management and stringent access compliance. Start with a strong identity management as weak credentials can compromise the entire network. Implement best practices of creating strong identity credentials and strengthening them with MFA. Hackers will hunt the weakest link and always wait for the right time to infect the first victim. Most practices include phishing, targeted campaigns, and others.

Attackers will mass infect devices and propagate laterally to gain access to critical information. Reduce your infected areas by eliminating older and less secure protocols. Secure access to entry points, and implement significant control of administrative access to resources. Then, automate threat response by using audits and logs of security-related events and related alerts. It detects patterns that may indicate internal attacks or attempted or successful external penetration of your network.



# CHAPTER 3

---

## THE BEST DEFENSE AGAINST BREACHES

---

As per the statistics above, the question now is not when you will have a network breach, but how often will you experience it? Every organisation has mission-critical and business-specific applications. It is autonomously tied directly to the success and efficiency of employees. As the attacks become sophisticated, the rise of ZT-based solutions will increase dramatically. Some vendors now have features that help your organisation establish the best defense against threats and breaches, particularly the infamous ransomware.

For example, how do you address phishing? Look for solutions under the ZT model that can perform device profiling and autonomous grouping. Logs mentioned in Chapter 2 are an excellent asset to indicate that a particular device is not behaving the way it should be.

Containment is also vital in network security as threats and infections propagate laterally. Find solutions that provide in-depth visibility and control of the threat movement. It should prevent the lateral movement of malware, provide attack isolation, and ensure the protection of critical and sensitive resources.



# CHAPTER 3

---

## CONTINUOUS INNOVATION

---

ZT requires all network requests to flow through the access control system, and all evaluations to be based on the device and user identity trust model. Organisations must leverage device and user trust claims to protect access to organisational resources. The remote working conditions faced by most organisations globally can be supported with conditional access management that provides comprehensive yet flexible policies to secure corporate data. All the security measures are in place while ensuring user productivity. Deploying ZT is a continuous battle; organisations must continue to innovate to protect the modern workplace where users can work productively beyond the perimeters of the corporate network.



# CHAPTER 4

---

## **IDENTITY AND ACCESS ARE THE CORE**

---

Today, ZT is central to almost all IT security. In chapter 3, ZT Network Architecture (ZTNA) was introduced. It discussed how ZTNA could complement strong identity and access management to protect the organisation's network securely. The identity of who can be trusted lies in how effective the organisation's security strategy is, how stringent the policies are?

Identity and access management (IAM) go hand-in-hand and comprises multiple components. It would depend on the nature of your industry, but commonly it consists of the following: policy engines, policy administrator, policy enforcement, and more. These are essential things to realising your IAM ZT goals.



# CHAPTER 4

---

## SCALING AND SECURING REMOTE ACCESS

---

Remote working presented organisations and businesses with new security challenges. Organisations must ensure their employees have secure access without experiencing additional friction in their daily workflows. On the other hand, these organisations must protect critical information and minimise risk.

With the myriad of devices and unsecured networks, attackers can compromise a single device within an organisation. Most threats and security breaches are executed using the *hopping* method. Attackers can move laterally across the network using stolen credentials. So, how do companies secure remote work, and what makes a solid and secure remote access strategy? The answer is a solution based on the ZT network.



# CHAPTER 4

---

## THE ZERO TRUST NETWORK ACCESS MODEL

---

With ZTNA, it is possible to establish a model built on strong identity and access management solutions. It balances the security needs of the enterprise with a seamless user experience. To leverage ZTNA, here are some steps to consider:

### 01 IDENTITY PROOFING

Identity proofing is a method to identify a user to a trusted source of truth initially. An external source of truth can be a credit bureau or a government entity that can verify or validate identity information, driver's license, or Social Security number. The external source of truth is accessed through an application programming interface (API).

# CHAPTER 4

---

02

## THE IDENTITY LIFECYCLE

After identity proofing, the next phase is the identity lifecycle stage. It is a method of defining the creation, maintenance, and retirement of a digital identity. For example, when an employee resigns, the admin must deactivate their digital identity immediately to prevent abuse of the credentials. It is often the fatal mistake of most organisations, leaving themselves open to the risk of a breach.

Another aspect of ZTNA implementation is the automation of IT processes related to the identity lifecycle. It reduces the risk of mistakes from manual input, and frees up labour from repetitive tasks. Additionally, it ensures consistency in operations while enforcing standardisation. Furthermore, automation reduces complexity and maintenance costs and increases the scale of administration, policy enforcement, and regulatory compliance.

# CHAPTER 4

---

03


## STRONG AUTHENTICATION

Generally, modern standards of authentication are accepted as a secure mechanism for initial access. However, there are other security gaps to look into. For instance, some of those gaps include IP header security and API security. Organisations should not solely focus on what's coming in. It is best to also deal with what's coming out. An unnoticed breach may be inevitable, but outgoing traffic also needs enforcement. It is where data encryption in transit and at rest and managing authentication within a session works best. For example, data from your protected landscape is not allowed to get out of the network. It must be thoroughly investigated and must be stopped to protect your critical resources and Intellectual Property artifacts.

04

## MULTIFACTOR AUTHENTICATION

Password and personal identification numbers (PINs) are identical to VPNs and firewalls, trusted but obsolete. The new landscape makes these tools inherently insecure. Hence, Multifactor Authentication (MFA) is the new era of securing your credentials. Most known applications now require a second means of authentication, such as tokens or codes sent by phone or text message, or biometric input such as fingerprints. Leverage MFA for every privileged account and must be utilised in unity with the organisation's access policies.





# CHAPTER 4

---

05

## ADAPTIVE AUTHENTICATION AND AUTHORISATION

The landscape is constantly changing, and MFA falls short with users repeatedly prompted for additional authentication factors. It hinders the goal of seamless access leading to a loss of productivity.

The step-up authentication is an adaptive authentication that leverages the organisation's pre-determined but customisable policies. It uses multiple risk conditions and assigns a score to each condition of the access request. Then, it dynamically adds the scores together and compares them to a baseline standard. The process then makes one of three decisions – allows access, denies access, or prompts the user for an additional proof factor (MFA) of authentication.

It balances the need between security and user experience, is transparent to the user but provides the necessary security assurance.

# CHAPTER 4

---

06

## CONDUCT PROPER AUDITING AND DISCOVERY

Hackers and cyber attackers are getting sophisticated as well. Threat propagations are carefully planned. For instance, a successful network breach goes unnoticed for a number of months or even a year. They tried to study the behaviour of the organisation and its employees and use the concept of social engineering to find the weakest link. Hence, IAM solutions need complementary security tools that operate in real-time to conduct proper auditing and discover among users and entity behaviours. Many organisations use a security incident and event management (SIEM) system and/or a user and entity behaviour analytics (UEBA) solution to collect, view, and analyse activities and processes. This combination is a perfect system to look for unusual behaviour of transaction flows and anomalies.

# CHAPTER 4

---

07

## SUPPORT ONGOING EXPERTISE

A ZT implementation is a continuous process. Security begins with culture, mindset, and with strong IAM. Today, it is too easy to spoof mobile phone numbers, capture identities, and gain illicit access to critical resources. A robust IAM procedure provides assurance that only legitimate users have access, and it continuously evolves to counter the ever-changing threat landscape. Continuous improvement is a key factor, and organisations should assign key personnel with the knowledge and skills to deploy and maintain all the ZT technologies and processes. Most specifically with the IAM to achieve and sustain a ZT security posture.



# ABOUT US

IBRS is an Australian ICT Advisory Company. We help our clients mitigate risk and validate their strategic decisions by providing independent and pragmatic advice while taking the time to understand their specific business issues.

## SCHEDULE A CALL WITH US

