THE JOURNEY TO ZERO-TRUST

An Industry White Paper published by

CIO ACADEMYASIA

In partnership with the following tech partners

adnovum

Attivo NETWORKS

MENLO SECURITY

INTRODUCTION

Against a background of disruption, companies are struggling to combat a deluge of cyberattacks and build resilience. Recent ransomware attacks which exploited supply chain vulnerabilities, have exposed gaps in cybersecurity posture — even for companies that have made the largest cybersecurity investments. Social engineering, predominantly phishing attacks, continues to act as a gateway for threat actors. Collusion between insiders and external threat actors is proving almost impossible to defend against, and increased cloud usage combined with endpoint proliferation is expanding attack surfaces and making traditional perimeters redundant. Companies are waking up to the fact that, if they have not already been breached by a cyberattack, they will be breached. This is leading to the adoption of a zero-trust approach to cybersecurity, which assumes breaches will occur and seeks to limit the damage caused by attackers.

This white paper uses CIO Academy Asia research, including insights form ASEAN-based technology leaders, to shed light on zero-trust maturity in the region, and propose ways in which gaps in cybersecurity posture can be narrowed or closed, using a zero-trust approach.

LEAD AUTHORS

Andrew Milroy
Principal Advisor
CIO Academy Asia

TECH PRACTITIONER CONTRIBUTORS

Abhijit Dasgupta
Global Head - Technology Risk, Control & Governance, ManpowerGroup

Chim Chin Kiat
Chief Information Security Officer, Dyson

Huang Shao Fei
President, Cybersecurity Chapter, Singapore Computing Society (SCS)

Murari Kalyanaramani
Chief Information Security Officer (CISO) Singapore, United Overseas Bank (UOB)

Perry Young
Executive Director, Perimeter & Network Security, Standard Chartered Bank

TECH EXPERT CONTRIBUTORS

David Chan
Managing Director, Adnovum

Leh Tee Teo
Technical Director
Attivo Networks

Nick Edwards
Vice President of Product Management
Menlo Security

PRODUCED BY

P. Ramakrishna
Chief Executive Officer
CIO Academy Asia

EXECUTIVE SUMMARY

Companies need to take a new approach to cybersecurity. They need to assume that breaches will occur and implement controls which minimize the damage that adversaries can cause once they gain access to systems and networks. In other words, a zero-trust approach is required.

According to the National Institute of Standards and Technology (NIST), zero-trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

A zero-trust approach requires a change of focus to an 'assume breach' posture. It requires an evaluation of current and desired cybersecurity posture. This evaluation determines which additional controls need to be implemented to adopt a zero-trust approach, commensurate with a company's risk appetite. A zero-trust framework can enable companies to evaluate their current cybersecurity posture and identify the controls that need to be implemented.

Zero-trust typically focuses on five pillars. These pillars are people (identity and access management), workloads, networks, data and devices as shown in Figure 1.

Using insights from technology leaders in the ASEAN region, this paper highlights important aspects of a zero-trust approach including:

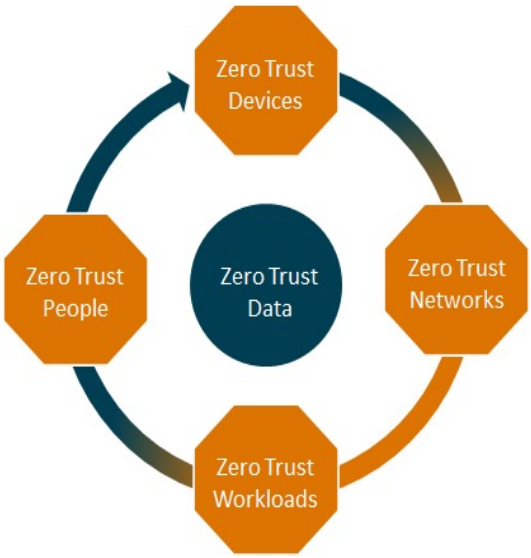


Figure 1 – The Five Pillars of Zero-Trust

- Zero-Trust maturity and implementation
- People: Enhancing IAM and the need for secure and usable identities
- Devices: isolate content before it reaches endpoints
- Workloads: Re-evaluating the perimeter and Secure Access Service Edge (SASE)
- Networks: Segmentation and deception ways of constraining lateral movement
- Data: The increased need for full visibility and control of all data within company systems, networks and devices.
- Limitations of a zero-trust approach.

ZERO-TRUST MATURITY & IMPLEMENTATION

All companies start from a different point on their zero-trust journeys — there is no 'one size fits all'. **As Leh Tee Teo, Technical Director at Attivo Networks in Singapore commented, "Every company needs to know where to start with zero-trust".** Companies have already made investments in security controls which they are keen to use. Taking a zero-trust approach is iterative. It requires organisations to revise their cybersecurity strategies and policies while gradually building on existing investments. There is no big bang approach to zero-trust. **President of the Cybersecurity Chapter of Singapore Computing Society (SCS), Huang Shao Fei, explained that "CIOs need to understand what can be done to re-purpose and re-use existing controls before seeking any additional investment. Chim Chin Kiat, CISO of Dyson added "There is a need to understand the business benefits of this approach. For example, can it drive efficiencies or cost savings?"** Describing zero-trust benefits in business terms is clearly necessary to gain wider corporate buy-in.

Where Should Organisations Start and What Should They Prioritise?

Figure 2 below illustrates zero-trust maturity with reference to the five pillars of zero-trust namely; data, devices, workloads, networks and people. It also proposes some controls that can be considered by companies if they wish to enhance their zero-trust maturity.

CIO Academy Asia research indicates that most organisations in ASEAN have evaluated their current cybersecurity posture and are seeking to clearly identify and limit the attack surface that must be protected. If a company hasn't evaluated its posture, this should be its starting point. Advancing further on a zero-trust journey requires existing security controls to be augmented

with zero-trust controls. Organisations with a comparatively low risk tolerance are more likely to be implementing these kinds of controls. An ideal zero-trust state is one in which organisations can continually monitor all their data traversing all systems, networks and endpoints while continuously adapting cybersecurity posture to address changing threats, technology mix and risk tolerance. In this ideal state, the damage caused by breaches is limited and incident response is automated. Importantly additional controls do not impact experience — they are invisible to users.

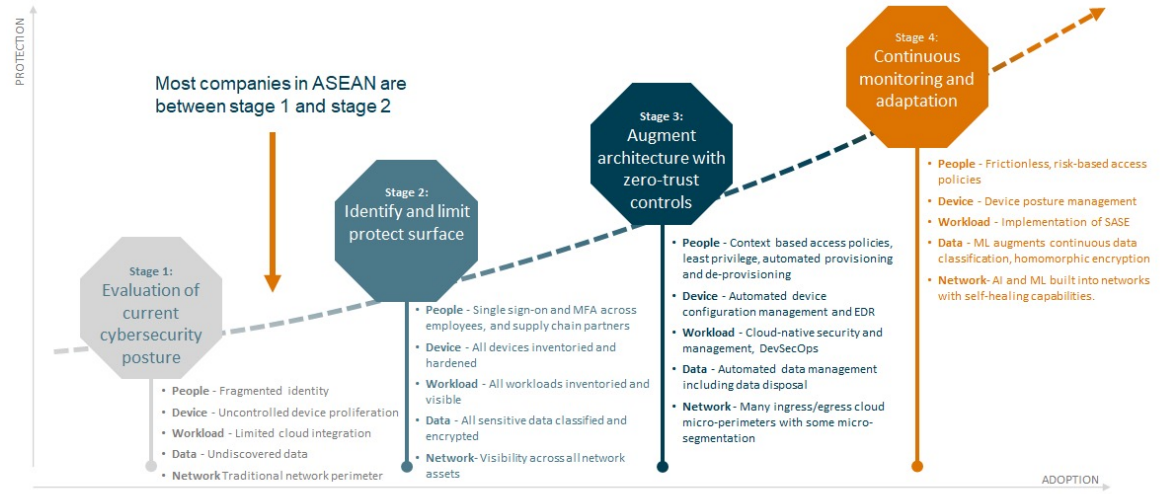


Figure 2 – Zero-Trust Maturity

As organisations progress on their zero-trust journey, the five pillars described above, provide a useful framework for looking at zero-trust approaches in more detail. Although there is a lot of overlap between the pillars, zero-trust maturity can be evaluated for each one. This in turn, gives organisations a baseline from which to start, as they decide which zero-trust controls are necessary to satisfy policies and match the organisation's risk appetite.

Overcoming Cultural Inertia

There is also a cultural element to progressing with zero-trust initiatives. Senior management must clearly understand the risks that a zero-trust approach is

"Senior management needs to understand the business risk so as board members understand why any change is being made. Their buy-in is critical to the success of a zero-trust approach".
- Abhijit Dasgupta, Manpower Group.

designed to manage. Together with CISOs and CIOs they must decide what level of risk is acceptable to an organisation. This decision will determine the controls that need to be implemented. According to SCS's Shao Fei, "CIOs need to look at cybersecurity from a strategic business perspective. It is not just about technology". Abhijit Dasgupta, Global Head of Technology Risk and Governance at Manpower Group added that, "Senior management needs to understand the business risk so as board members understand why any change is being made. Their buy-in is critical to the success of a zero-trust approach".

CIO Academy Asia research also indicates that the operational structure of an organisation can make it difficult to take a zero-trust approach. For example, the infrastructure team might make decisions in certain areas such as cloud usage, without involving the cybersecurity team. Policies around cloud usage are a critical part of a zero-trust approach. So, organisations must find ways of breaking down siloes and involving all relevant stakeholders in developing a zero-trust approach. This level of collaboration is often very difficult to achieve.

Manpower's Dasgupta added "There is not usually a clear mandate on who operates what tool. There is a need for a framework for the segregation of duties in companies before a zero-trust approach can work".

The Importance of Policy Enforcement

Core to policy enforcement are zero-trust policy engines and zero-policy administrators. Together, the policy engine and policy administrator make the decision on what level of access to grant. The policy then needs to be enforced. As David Chan, Managing Director of Adnovum Singapore stated that "Zero Trust Policies requires organizations' IAM solutions to constantly monitor, secure their users' identities and access points. These need to be enforced consistently across different locations, users and devices."

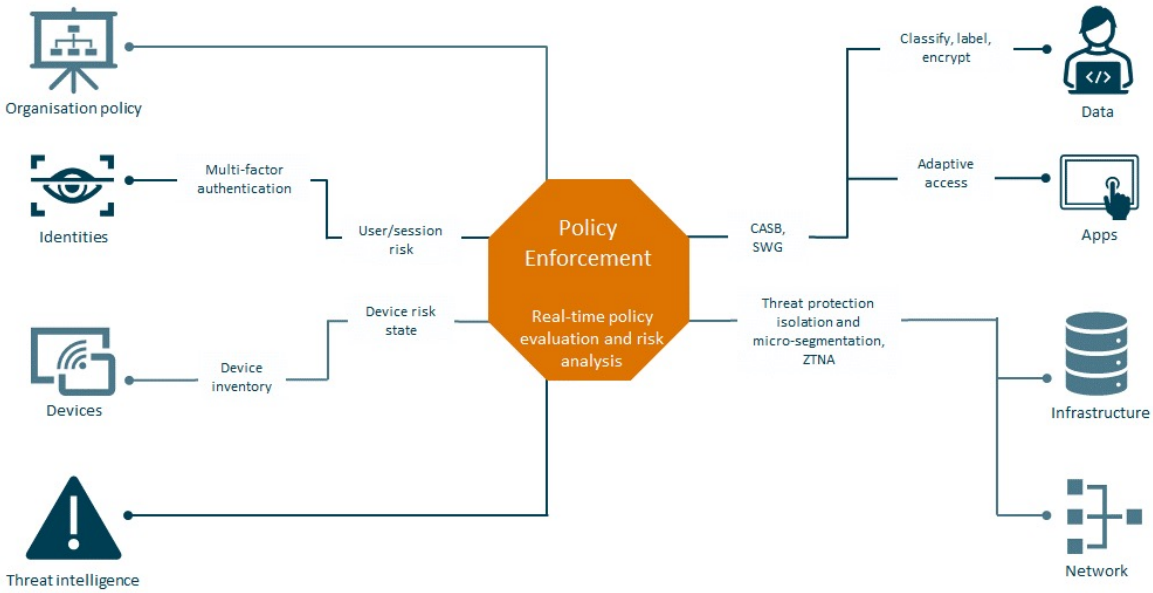


Figure 3 – High-Level Schematic View of Zero-Trust Architecture

Policy enforcement is also challenged by the tendency for different zero-trust capabilities to sit in siloes. Dyson's Chim made the point that, "Zero-trust capabilities tend to sit in siloes. There is a need to pull them together and understand where to start. Zero-trust is still very siloed by solution".

PEOPLE: ENHANCING IDENTITY & ACCESS MANAGEMENT (IAM) AND THE NEED FOR SECURE & USABLE DIGITAL IDENTITIES.

The people pillar of zero-trust focuses on IAM and enforcing the principle of least privilege. Most breaches involve the compromise of IT and business user credentials such as IDs and passwords. Possession of these credentials allows attackers to gain access to the systems and networks of their victims and, often, to move laterally. IAM is an essential way of mitigating the risk of illegal access.

Increased cloud integration and the proliferation of digital identities is placing increased focus on securing identities and making customer experience seamless. As public cloud infrastructure is more widely used, particular focus needs to be placed on user identity management issues related to over-assignment of entitlements and a lack of visibility into those existing permissions. Another major concern is the explosion in 'non-human' identities, such as applications, virtual machines, containers, serverless functions, and other objects — gaining visibility across all these identities can be a major challenge.

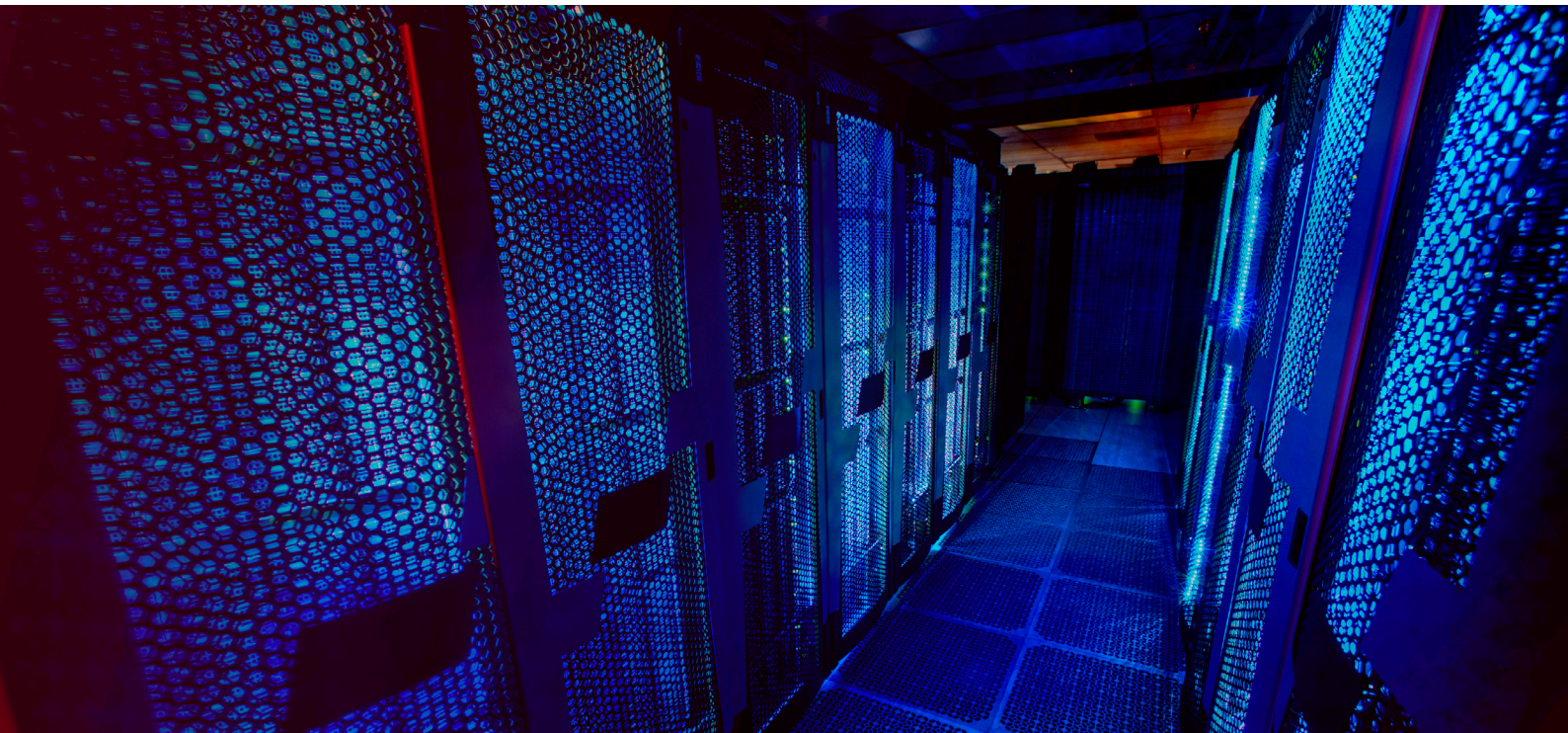
Cloud infrastructure entitlements management can address these challenges by providing visibility to identity entitlements across multi-cloud environments including users, groups, and applications by risk level. This can allow organizations to be equipped with detection capabilities for identity privilege escalation across multi-cloud environments. As Adnovum's Chan stated, "Securing hybrid and multi-cloud environments requires a different IAM and security strategy that encompasses zero-trust. As companies move to the cloud, securing infrastructure, data, and access becomes increasingly

difficult across the cloud and on-premises datacenters. Organizations thus leverage on a "zero trust" approach to cloud security due to this highly dynamic environment. The Zero Trust framework includes the enablement of advanced technologies such as continuous authentication, risk based multi-factor authentication, identity protection, and robust cloud technology to verify a user's or system's identity, access and security at any point in time."

Active Directory is a Major Vulnerability

While consistent IAM policy is critical across multiple resources in on-premises and cloud environments, it is equally important to improve the security of Active Directory (AD) used on-premises. AD is proving difficult to replace because it serves many traditional applications and infrastructure that are hosted on-premises and may be too sensitive to move to the cloud.

AD provides resources and information, such as privileged credentials or critical system information, for all computers joined to a particular domain. Using a zero-trust approach, the principle of least privilege can be made more granular by masking sensitive information on privileged credentials or critical systems. This approach limits resources to those that need them. AD can be



further protected with continuous automated assessments — ensuring it is updated, configured correctly, and doesn't contain open attack paths.

Zero trust assumes any user, or device that accesses networks, services, applications, data, or systems must never be trusted and its access must always be verified. New devices and users must identify and verify themselves based on multiple security controls. They should encounter progressively more controls as the sensitivity of resources increases. After verification of identity is established, users and devices can be classified according to the access required for an activity. **According to Perry Young Executive Director of Perimeter and Network Security at Standard Chartered Bank, "Zero-trust offers pervasive access wherever users are, but you need to treat every user scenario as untrusted. Even the requests from the corporate office need to be treated as untrusted. This approach creates a common experience for all users, regardless of their location".**

Third Party Access Management Needs Greater Focus

These classifications of trust and risk must be dynamic and core to IAM. Policies need to be created and enforced across the enterprise for identities, services, applications, data, and systems. As Perry Young also stated, "Third party requests can sometimes be treated with less rigour than employees. This doesn't make sense". Nick Edwards, Vice President of Product Management at Menlo Security added that "We want a stack that enforces the same rigour regardless of whether resources are being accessed by employees or third parties". Different user requests can vary if policies are changed in line with risk and trust classifications. For example, third party identities might always be verified and monitored, and employee classifications could be adaptive based on the sensitivity of the data being accessed. Always verify policies typically require credentials and multifactor authentication, while always monitor policies usually audit, analyse and record all activity.

Prioritise Access Controls Around the Crown Jewels

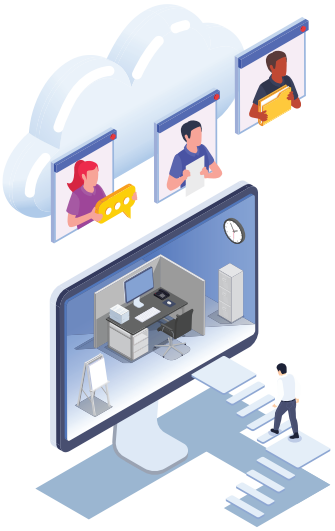
Murari Kalyanaramani, Chief Information Security Officer at UOB Singapore, noted that "security leaders should take stock of their access control points with a greater focus on their organisation's crown jewels, by looking into the organisation with a cyber attackers' mindset and gaining an understanding of the potential adverse business impact from a regulation and compliance standpoint or impact on customers should a breech occur."

Key Considerations for the People Pillar of Zero-Trust

- Evaluate existing IAM controls and augment them with additional controls to meet policy requirements.
- By default, treat all users as untrusted. But, ensure that IAM controls are aligned with both risk profiles and policy. For example, a supplier should be treated very differently from a customer based on their risk profile and corporate policy.
- Apply the principle of least privilege. This enables the enforcement of a risk-based zero-trust approach. When a user is verified, their access is limited to only what is necessary to undertake a specific activity.
- Eliminate passwords. The very existence of passwords is a major security vulnerability. Risk can be substantially reduced by offering less time-consuming forms of authentication that are both more secure and more user friendly.
- Balance access controls with the need for usability. It is important to ensure that access controls are not so arduous that user experience becomes compromised.

DEVICES: ISOLATE CONTENT BEFORE IT REACHES ENDPOINTS

The device pillar focuses on limiting the expanded attack surface caused by the proliferation of endpoints and reducing the likelihood of device compromise.



Remote working has enabled business operations to continue in a time of extreme disruption, but it does expose businesses to many more threats. The increased number of endpoints inevitably expands attack surfaces and exposes companies to new vulnerabilities. Often companies are not aware of the status of devices accessing their resources. Companies need visibility across all corporate devices and need to apply strict risk-based access controls to non-managed devices. They need to continually manage threats coming from devices and automate the elimination of threats and recovery from them.

Policies must be triggered in real time, based on access authentication and other customisable attributes. For example, a new IoT device with outbound internet access must be identified and automatically assigned to a restricted network segment. Changes in security state need to be identified, such as changes in antivirus agents or encryption. Devices must be continually assessed while they are on the network, and each time they start and finish a session. These assessments must analyse device health and context in real time and initiate necessary actions such as re-scanning devices for vulnerabilities and indicators of compromise. Ideally, network traffic is isolated in the cloud where content is visible but never downloaded to endpoints.

Browser exploits are a major source of vulnerability, creating an increased need for regular patches on devices — this is a major challenge when workers are widely dispersed. Any remote device could potentially have a devastating impact on enterprise networks.

Remote Browser Isolation Gives Greater Visibility and Control Over Devices

Remote Browser Isolation (RBI) plays an increasingly important role in zero-trust approaches. It moves the execution of all browsing activity from the user's device to a remote server. This remote server can be hosted in the cloud or located on-premises. It stops malware from reaching end user devices regardless of what documents are downloaded or which links have been clicked. Menlo Security's Edwards commented that **"RBI should be built into a zero-trust approach. It can ensure that users never directly touch applications".**

Isolating all online traffic before it reaches endpoints is an important part of a zero-trust strategy. This approach usually isolates content in the cloud where it is visible but is never downloaded onto an endpoint. An isolation layer is created between networks and the Internet where content is cleaned and securely delivered from the cloud browser to the user's browser. This isolates users from potential threats with minimal friction. No content is executed within the user's browsers which massively reduces risk.

Placing content in this isolation layer provides greater visibility and control over security and makes it much easier to apply policies consistently across networks.

Isolating the browsing process creates an air gap between the Internet and enterprise networks. Content is securely rendered from the remote browser to

the browser on the end user's device, giving the user a frictionless experience — identical to the desktop experience. All attacks are completely isolated from the endpoint and from the user.

Email security technologies often fail to detect threats because they don't seem to be malicious. The threat from phishing attacks can be mitigated by email isolation. Emails and attachments pass through the isolation layer, protecting endpoints. All email content is isolated from the user device and typically executed in a cloud isolation platform. This means that malicious links delivered within email are scanned and isolated, so that secure and compliant content is delivered to users.

Along with remote browser isolation, email isolation plays a key role in any zero-trust strategy and protects devices from the threats.

Key Considerations for the Devices Pillar of Zero-Trust

Key steps for the devices pillar of zero trust include:

- Inventory and audit all corporate devices access systems and networks.
- Harden all devices including IoT devices and consistently enforce policy across devices.
- Treat all devices as untrusted. Apply risk classifications to all devices, both corporate and those belonging to suppliers and customers. Apply RBI.
- Continuously monitor and manage devices including ongoing health checks.
- Apply more controls to any unmanaged devices, including customer and supplier devices.

WORKLOADS: RE-EVALUATING THE PERIMETER AND SASE

The workload pillar refers to applications being used for operational purposes and securing them in a consistent manner that is in line with policies.

Frequently, security controls are not designed for the dynamic, distributed, and virtual nature of cloud environments, and widely dispersed remote working. Companies tend to react to cloud security challenges by adopting multiple point solutions to plug gaps and address varying needs, including Cloud Access Security Broker (CASB) technology to secure SaaS traffic, and Secure Web Gateway (SWG) technology to secure web traffic. Each solution needs to be configured and managed — this creates complexity and risk. Failing to apply any setting correctly can prove to be disastrous.

Indeed, cloud security solutions are often unable to scale across an expanding number of people and devices, located outside the conventional enterprise perimeter.

A zero-trust approach requires full visibility across their cloud resources and a single set of policies which can be managed and configured on a single dashboard. They also need an integrated set of tools. This is a very challenging undertaking. Companies typically have complex heterogeneous IT environments with many technologies and functions operating in silos. This makes visibility and control very difficult, especially when legacy OT environments are also involved.

Companies require the ability to deliver an integrated set of network and security services in a consistent way — enabling digital transformation, cloud migration, edge computing and remote working.

These requirements can be addressed by SASE technology. A SASE solution can enable rapid cloud adoption and remote access, by offering security services from a common cloud-delivered architecture, using the same policies and a single dashboard.

More specifically, SASE solutions integrate security and networking into one cloud-native solution. Instead of having multiple discrete services, it typically offers the following as a unified solution:

- Zero-trust network access
- Virtual private networks
- Software defined WANs
- Firewall as a service
- Secure web gateway
- Data loss prevention
- Cloud access security broker.

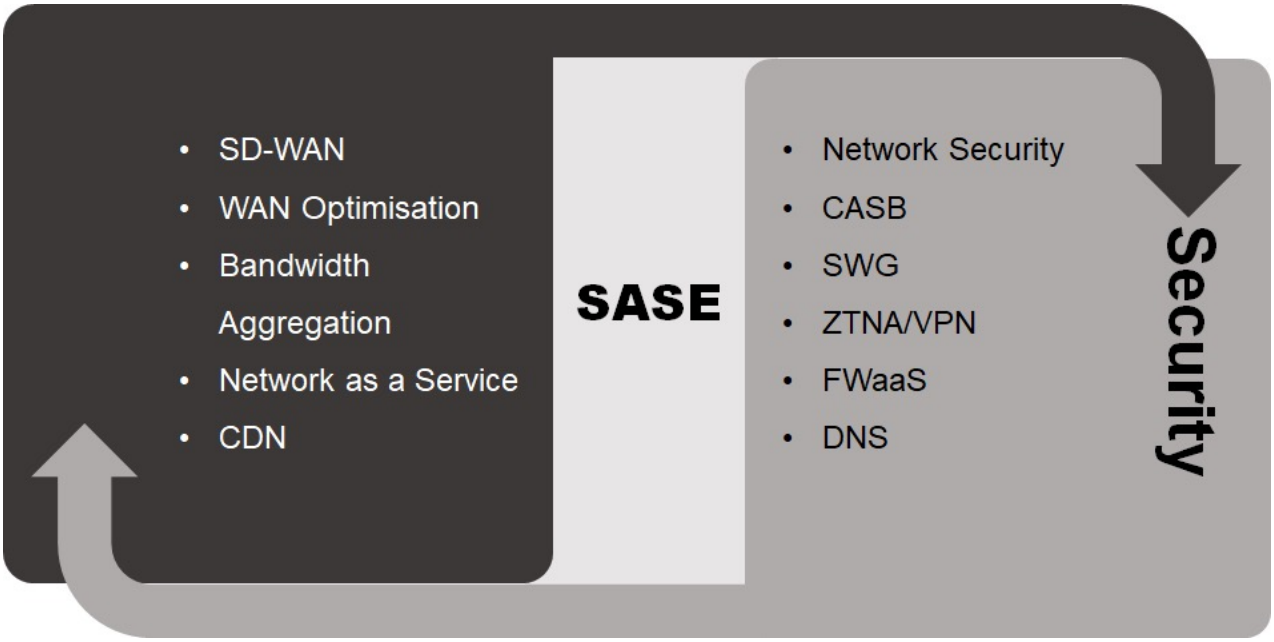


Figure 3 – SASE Model

The elimination of a complex and fragmented set of physical and virtual solutions by providing one integrated cloud-native solution, removes the cost of appliances and reduces network complexity. SASE can offer much lower latency, greater visibility across assets and centralized control.

Importantly, some SASE offerings isolate email and remote browsers. Browsing activity can be isolated away from end user devices and onto remote cloud servers. This prevents active code from reaching local browsers and stops web-based infections from spreading. Email isolation can eliminate phishing attacks breaking the attack chains of many threat actors.

It Takes Two to Tango - Shift Left, Yes. But Also Shift Right.

The shift-left approach in embedding cybersecurity controls as early as possible in the design of new digital systems, must be complemented with robust threat detection capabilities. UOB's Murari highlighted "security teams also need to depend on reliable SIEM logs and telemetry data to identify anomaxlous activities and fine-tune their zero-trust policies."

Key Considerations for the Workload Pillar of Zero-Trust

- Inventory and audit all workloads to limit sprawl.
- Apply cloud governance which focuses on cloud configurations and compliance.
- Focus on cloud native security and move away from 'lift and shift'.
- Bake security into coding and implement DevSecOps.
- Implement SASE in a way that limits vendor lock-in.

NETWORK: SEGMENTATION AND DECEPTION AS WAYS OF CONSTRAINING LATERAL MOVEMENT

The network zero-trust pillar focuses on the segmentation and isolation of resources so as the impact of a breach is limited.

Segmentation is designed to enhance security through the creation of smaller attack surfaces. There are multiple approaches to segmentation, each designed to limit the ability of malware to move laterally once systems or/and networks are breached. The most common type of segmentation is network segmentation.

Network segmentation is the act of dividing a computer network into smaller physical or logical components. It is one of the best mitigations against cybersecurity attacks.

It involves giving groups of devices including servers and PCs only the connectivity required for specific functions. This limits the ability of malware to move laterally.

Segmentation can also be based on device type. For example, IoT devices can be placed on their own network partition to increase security. In the healthcare sector, medical devices such as MRI machines might be separated from the rest of the network. Different approaches to segmentation can be blended, depending on requirements.

Dividing networks into VLANs and subnets is the conventional way of segmenting networks. But, it doesn't scale well as a solution and requires a

lot of manual effort. Network engineers have the complex task of determining which resources belong in which segments and implement policies to govern communication between segments. This can be a major challenge, can lead to mistakes being made, and can potentially disrupt business operations.

Even if you can make segmentation work well enough on the network, it must also account for public clouds, third party services, and APIs, making it more difficult to achieve.

Companies are adopting other approaches like micro=segmentation. This approach decouples the enforcement of segmentation policies from the physical network, allowing more granular control and simpler, more flexible administration. The end game is to protect each workload with its own micro=perimeter making lateral movement almost impossible.

Decoys and Deception Play a Major Role in Active Defence and Restricting Lateral Movement

A key aspect of zero-trust is active defence. **Attivo Networks Teo added that, "Active defence is an integral part of a zero-trust strategy".** Active

defence can include the use of decoys such as fake credentials, and irrelevant applications that create a deceptive fabric. This contains attacks and allows security teams to reduce the effort involved in hunting threat actors because they can be lured into the decoys. This allows defenders to detect attacks early and restrict lateral movement.

When a breach occurs and the threat actors are lured into the deceptive fabric of resources, counterintelligence can be provided to allow security teams to understand the tools, techniques and procedures executed by the attackers. This information can then be used to review and improve on the existing zero-trust architecture and policies.

Zero-trust involves much greater focus on segmentation and other techniques such as active defence, as a means of containing breaches after they occur.

Key Considerations for the Network Pillar of Zero-Trust

- Move away from the traditional 'castle and moat' network perimeter and treat all networks as untrusted.
- Implement software defined networks (SDNs) so as the network can be centrally controlled and greater visibility across network assets is provided.
- Focus on the protection of resources by segmenting around applications and services.
- Apply micro-perimeters allowing more granular control.
- Build AI and ML into networks and push controls to the edge.

DATA: THE INCREASED NEED FOR VISIBILITY AND CONTROL OF ALL DATA

This zero-trust pillar is centred on the classification and categorization of corporate data. A key principle of a zero-trust strategy is the discovery and classification of all data that is used. Different levels of protection are then applied to data based on its sensitivity and value. Once categorised, data can be isolated from everyone except those that need access. Typically, basic data security controls are already established due to compliance requirements. But, these controls are often insufficient.

From a data perspective, zero-trust also involves considerations around data storage, least privilege, and importantly, encryption mechanisms for data at rest, in transit and in use. Often, data in use is decrypted so that calculations to be made on that data. This is a major vulnerability especially when data is being used in cloud applications. New technologies such as homomorphic encryption which allows calculations to be performed on data while it is encrypted are emerging. Ultimately, a zero-trust approach will make any leaked or stolen data useless to an adversary. Data visibility is also essential so that anomalous patterns of data usage can be identified rapidly. Visibility of data in all business ecosystems makes it easier to quickly detect breaches and contain them. This involves building capabilities for visibility into the interaction between users, applications, and data across all devices policy enforcement across all of these devices.

With a zero-trust posture, devices, networks, data and systems must continually be evaluated against policies and enforcement must be ensured by a policy engine and a policy administrator.

Given the complexity of today's IT environments, the skills shortages and the vast numbers of false positives, remediation actions must be automated. These actions should include reinstalling vulnerability assessment software, endpoint protection, encryption and other security software through orchestration with third party products. Perhaps most importantly, patching needs to be frequent and orchestrated. Failure to patch vulnerabilities rapidly is one of the greatest security vulnerabilities, so requires particular focus.

Key Considerations for the Data Pillar of Zero-Trust

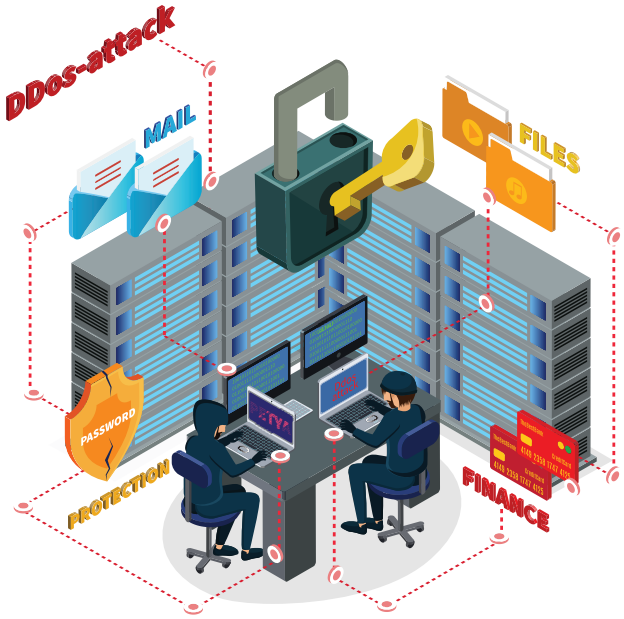
- Discover and classify all data
- Identify sensitive and valuable data and understand how, why and by whom it is used.
- Apply data obfuscation to data in use, at rest and in transit with a mix of encryption and tokenization technologies.
- Continually inspect data usage patterns and ensure compliance.
- Ongoing data classification aligned to risk.

ZERO-TRUST LIMITATIONS

Standard Chartered's Young explained that "As companies embark on their zero-trust journeys, there is a growing risk of dependence on a single vendor or a small number of vendors. Indeed, the SASE framework encourages a consolidation of solutions to deliver cloud driven capabilities".

Policy engines and policy administrators are core to zero-trust for enforcement. Communications between resources is typically approved and configured by the policy engine and policy administrator. The impact of any policy engine or policy administrator compromise can be huge. Focus must be placed on configuration and continuous monitoring of policy engines and policy administrators and all changes must be logged.

Policy engines can also become targets for DDoS attacks. This threat can be mitigated by locating policy enforcement in a properly secured cloud environment or by replicating it in several immutable locations.



Privileged credentials will continue to be stolen and used to move undetected within systems and networks. Contextual trust algorithms and network segmentation mitigate but do not eliminate this risk.

Segmenting networks in a way that is aligned to changing policies limits its ability to prevent lateral movement. Segmentation approaches that are logical

decoupled from the physical network offer much more promise although scarce skills will be required.

Encrypted network traffic can contain malware. Deep packet inspection of this traffic is impossible for most companies. Machine learning techniques which analyse encrypted traffic are emerging.

For companies that embark on a zero-trust journey, focus must always be placed on the risks that are amplified by this approach.

CONCLUSION

The increasing impact and frequency of cyberattacks combined with expanding attack surfaces is driving a need for a complete re-evaluation of cybersecurity postures.

The conventional approach to cybersecurity typically involved protecting assets and devices that were approved and resided, often physically, within corporate premises. Over time, companies have incrementally enhanced their controls to secure workloads as they migrate to the cloud, to secure remote working and to address OT vulnerabilities. But this approach has often been piecemeal in nature, leaving significant gaps. Companies need to change their approach to cybersecurity. They need to place much greater emphasis on the principle of least privilege across an expanding estate of assets and devices and segment networks to inhibit lateral movement. This approach must be balanced with usability as customer expectations grow. They also need to isolate content with technologies like RBI and email isolation and place greater focus on securing the edge.

A zero-trust approach requires visibility and control across company ecosystems. Although this may seem obvious, it is a very difficult task to accomplish, especially with a mix of legacy and cloud technology. Companies need to know what assets and data they have and continually classify them depending on vulnerability and on risk. It is this continuous monitoring and adaptation that is a shift from earlier approaches to cybersecurity.

As conventional perimeters cease to exist and companies need to secure devices and assets at the edge, it is more important than ever deliver an integrated set of network and security services in a consistent way. This involves integrating multiple security technologies onto one platform — adopting a SASE model.

Companies must remain alert to the risks that a zero-trust approach amplifies. Attackers will increasingly focus on the policy engine and the policy administrator — ensuring their integrity will be more critical than ever before.

Companies increasingly understand the need for a zero-trust approach as they face rapidly growing digital risk. However, the implementation of the processes, policies and technologies that are required for this approach remains immature for most companies. More aggressive zero-trust approaches are needed now.

For Enquiries, Please Contact:

David Chin
Deputy CEO
CIO Academy Asia
david@cioacademyasia.org