

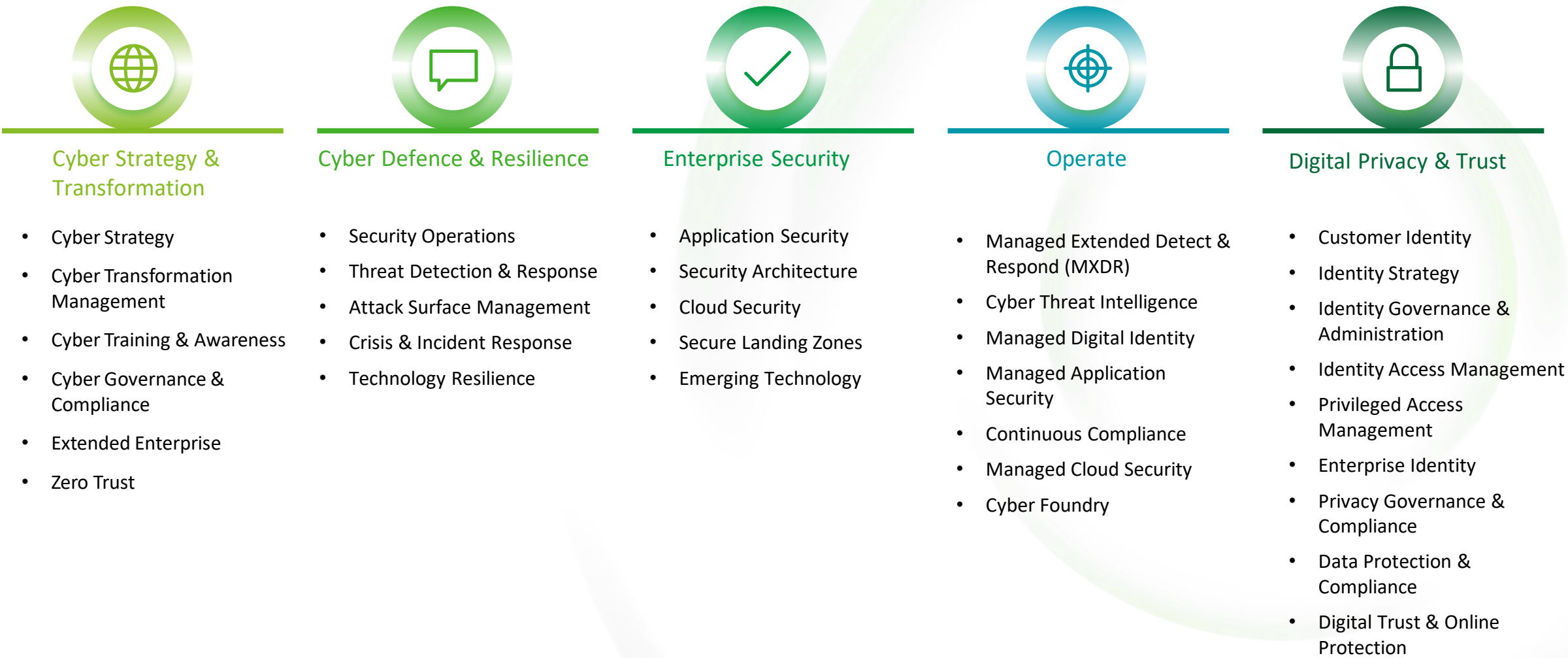


# Zero Trust Services

September 2024




# The Deloitte difference

With human insight, technological innovation, and enterprise wide cyber solutions, Deloitte Cyber works alongside clients to help find those answers and solve for the complexity of each challenge, from the boardroom to the factory floor. The ubiquity of cyber drives the scope of our services. Deloitte Cyber advises , implements , and manages solutions across the following areas:



# Deloitte Zero Trust Service Offerings

Deloitte’s solutions and services extend across the advice-implement-operate spectrum—from strategy development to technology integration and deployment to ongoing managed services for solutions in a modern security architecture.

	 ADVICE	 IMPLEMENT	 OPERATE
	<ol style="list-style-type: none"><li>1. Build the business case and create a detailed <b>roadmap for Zero Trust adoption</b></li><li>2. Develop your <b>strategic vision</b> for a modern security architecture that enables the business</li><li>3. Explore <b>use cases, technologies</b>, and possibilities through interactive labs and workshops, including our Zero Trust Experience Center</li></ol>	<ol style="list-style-type: none"><li>1. Design and execute <b>proof of value (PoV)</b> exercises within a client’s environment</li><li>2. <b>Deploy and integrate leading solutions</b> to modernize capabilities in each of the Zero Trust core domains: Identities, Workloads, Data, Networks, and Devices</li><li>3. Integrate cyber solutions with other enterprise apps and third-party solutions</li></ol>	<ol style="list-style-type: none"><li>1. Provide <b>outcomes-based managed services</b> that streamline and operate capabilities needed to support a modern Zero Trust architecture, including Cyber Operate services</li><li>2. Provide <b>24x7 security operations center (SOC)</b> services through Deloitte’s Global Cyber Intelligence Centers</li></ol>
Deliverables	<ul style="list-style-type: none"><li>• Zero Trust Strategy and Roadmap</li><li>• Zero Trust Readiness</li></ul>	<ul style="list-style-type: none"><li>• Zero Trust Security Reference Architectures</li><li>• Zero Trust Solution Implementation</li></ul>	<ul style="list-style-type: none"><li>• Managed Detect and Respond Service</li><li>• Managed SASE</li></ul>

Alliances



Google Cloud

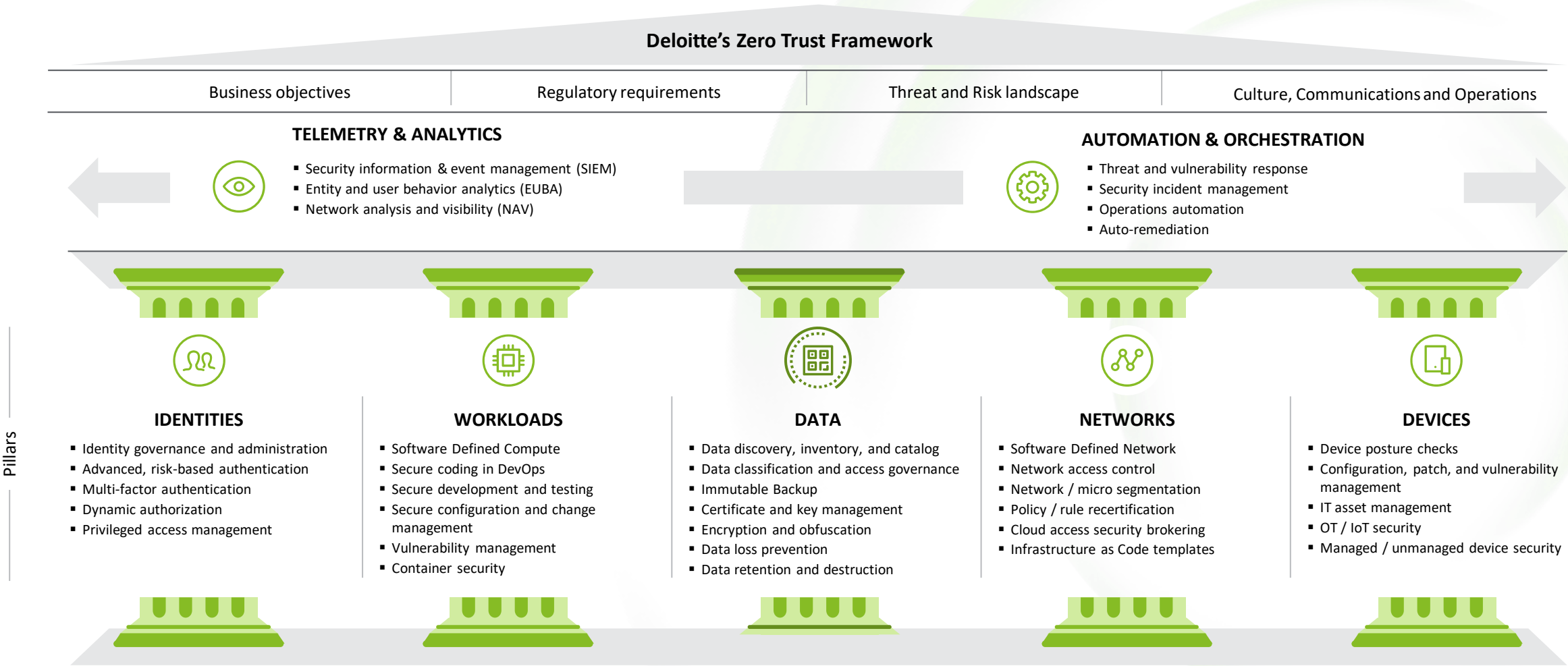


paloalto  
NETWORKS

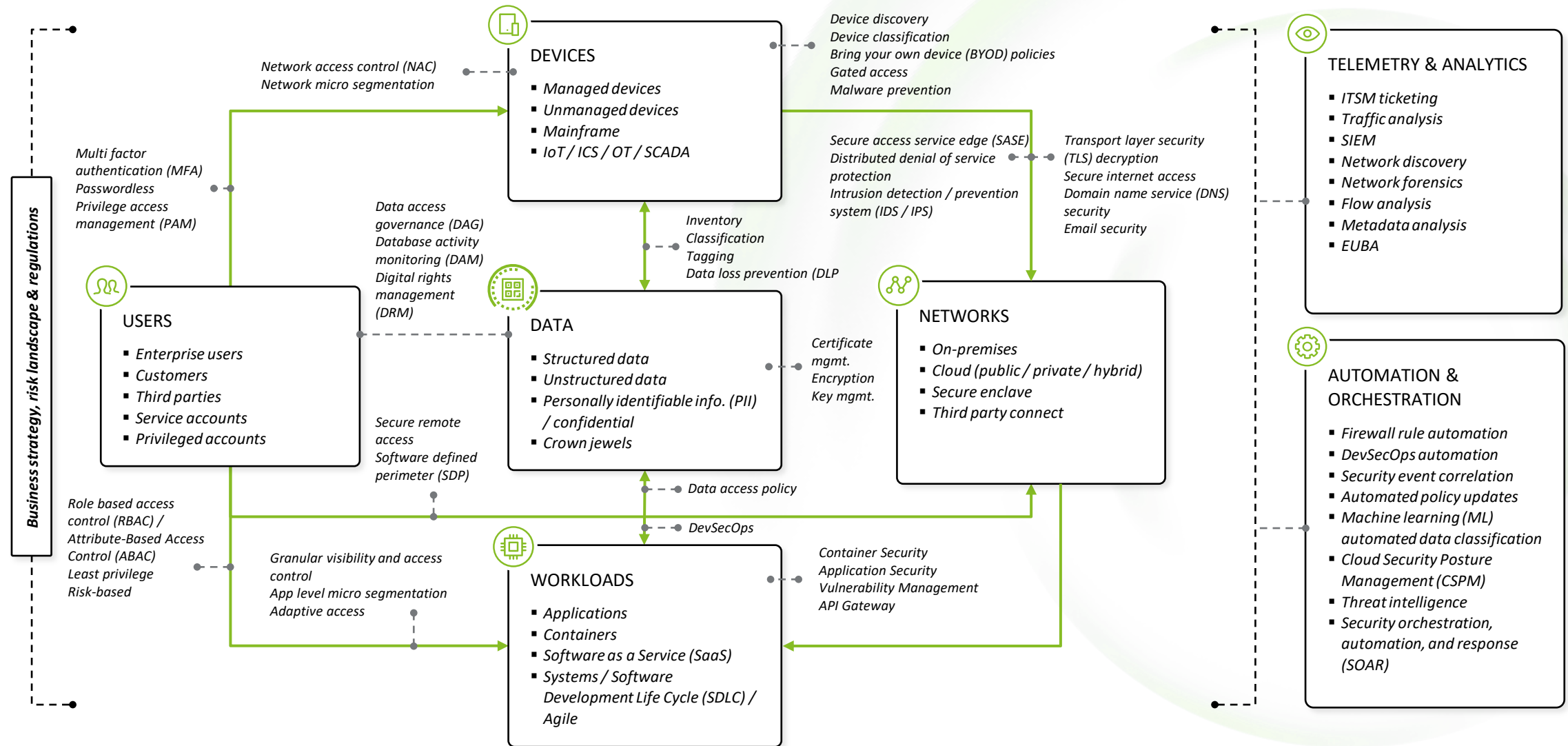


netskope

# Deloitte Zero Trust Service Framework



# Illustrative Zero Trust reference architecture



# Case Study 1

## Financial Services

### Solution

- Established Zero Trust as a holistic approach to manage cyber risk and implemented Zero Trust capabilities across 2 pilot locations (Singapore & New Zealand) using CISA Zero Trust maturity model
- Built Architecture Blueprints for AWS and Azure that can be reused across all their entities
- Implemented Zero Trust Controls across pillars (Identities, Device, Networks, Data, Applications and Telemetries) using Terraform

### Impact

- Addressed client priorities: Infrastructure hardening, IT protection, Zero Trust, secure cloud environments







### Ecosystem & Tools



## Enhanced security posture through Zero Trust

### Infrastructure and data protection based on zero trust principles

#### Key Challenges

- |   |   |
|---|---|
|  <b>Cybersecurity incidents impacting business</b> operations                            |  <b>Unclear cyber baselines</b> across the hybrid technology environment |
|  <b>Lack of access control</b> across various stakeholders (staff, contractors, vendors) |  <b>Performance issues</b> in accessing business applications            |
|  <b>Compliance Issues</b> and inconsistent security policies                             |  Lack of <b>holistic approach</b> to manage cyber risk                   |

#### Outcomes achieved with ZT

- Enhanced Security Posture:** Significant improvement in the overall security posture, reducing the risk of data breaches and cyber threats.
- Scalable Security Infrastructure:** A scalable and flexible security infrastructure that supports future growth and technological advancements.
- Improved Access Management:** Implementation of strong, multi-factor authentication (MFA) mechanisms, enhancing user security across various stakeholders.
- Operational Efficiency:** Streamlined security processes and operations, reducing the complexity and cost of managing IT security.
- Compliance achieved:** Full compliance with industry regulations and internal control requirements.



# Appendix

# Deloitte Zero Trust – Use cases

Zero Trust by Deloitte offers a broad range of services to help organizations align to the ‘never trust, always verify’ cyber approach while securing the ubiquitous nature of their modern enterprises.



## Secure Remote Access

Replace legacy remote access solutions such as virtual private network (VPN) or virtual desktop infrastructure (VDI) with a cloud-native service that is inherently scalable, resilient, and secure.



## Third Party Access

Provision least privilege access and data protection for third-party access to enterprise resources. Control access to applications that require heightened security (e.g., copy/paste or download prevention) and apply granular access controls based on the sensitivity and regulatory requirements of the underlying data.



## Cloud Adoption

Adopting Zero Trust for cloud environments ensures consistent security across multi-cloud and hybrid setups by enforcing identity-based access and real-time threat detection. This approach enhances security, streamlines access to cloud resources, enabling secure and agile cloud adoption.



## Securing Digital Transformation

Zero Trust secures digital transformation by continuously adapting to new risks, protecting critical assets with granular controls, and ensuring seamless, secure access across evolving IT landscapes. This approach enables organizations to confidently embrace innovation while maintaining robust security.

## Benefits



## Enhanced Security, Less Complexity

- Limit lateral movement, data exposure and provides heightened threat detection, thereby enhancing the overall security posture and resilience against evolving threats.
- Eliminate the need for complex, layered security perimeters, making the network architecture more straightforward and easier to manage.



## Enhanced User Productivity

Enable secure, seamless access from any device or location, minimizing disruptions and ensuring smooth workflows. This allows employees to work efficiently while maintaining robust security.



## Cost Reduction, Ease of Operations

Zero Trust reduces costs by streamlining security infrastructure and automating access management, lowering maintenance expenses and operational burdens. This approach simplifies operations, enabling IT teams to focus on strategic priorities.



## Business Agility

Supports rapid adaptation to new technologies and changing business needs, allowing organizations to innovate and scale efficiently while maintaining robust security. This enables faster response to market opportunities and evolving threats.



# Illustrative Zero Trust adoption journey

We believe that organisations should not use a big bang approach to implement Zero Trust. By using an evolution approach rather than a revolution approach, Zero Trust can be implemented in stages, with nominal business interruptions in the production environment.

01

## ESTABLISH A BASELINE

1. **Identify** user base, critical apps / services / data, third-party integrations, business processes
2. **Map** application relationships and known / approved traffic flows
3. **Assess** threat landscape
4. **Review** existing security policies and regulatory drivers
5. **Align** ZT principles with overall cybersecurity framework
6. **Identify** technology requirements and capability gaps

02

## SET THE STRATEGY

1. **Define** strategy / roadmap for phased adoption
2. **Prioritize** initial use case(s) in low-risk environment to minimize disruption
3. **Gain** consensus from relevant stakeholders
4. **Collaborate** with potential vendors to align business needs and socialize requirements
5. **Design** “living” governance / support model to test in pilot phase

03

## PILOT AND TEST

1. **Define** scope
2. **Identify** PoC candidates / timeline
3. **Emulate** use cases against business requirements
4. **Collaborate** with vendors on implementation
5. **Update** and refine governance / support model
6. **Design** support processes
7. **Integrate** technology solutions to support telemetry & analytics as well as automation & orchestration
8. **Monitor** progress, risks, and document lessons learned

04

## IMPLEMENT INCREMENTALLY

1. **Implement** one discipline/use case at a time, taking an iterative approach
2. **Finalize** governance / operational structure
3. **Refine** processes to run and maintain
4. **Provide** continues subject matter expertise
5. **Conduct** user awareness training, as necessary
6. **Update** operational processes, as necessary
7. **Capture** metrics / reporting on potential impact to organization

# Cyber Strategy & Transformation



Every business will have to think about cyber security at one point. Processes, people management... everything is becoming increasingly digital.

Besides the obvious advantages technology brings, it also comes with threats. To properly defend itself, each company should know what its 'crown jewels' are, where weaknesses lie and what possible solutions exist. But the cyber landscape is vast and it can be extremely difficult to keep an overview and decide where to invest money.

Deloitte's Cyber Strategy & Transformation service goes a step beyond through a relentless focus on providing comprehensive, issue-based solutions to help Deloitte's clients address the rapidly changing business environment and stay ahead of the competition.



Supporting your entire business to move forward with confidence.

- Cyber Strategy
- Cyber Transformation Management
- Zero Trust
- Cyber Training & Awareness
- Cyber Governance & Compliance
- Extended Enterprise



# Cyber Defence & Resilience

As cyberattacks grow in frequency and sophistication, you need to outsmart the cybercriminals.

With the proliferation of remote work and the steady advance of the IoT, potential vulnerabilities are multiplying. As it gets harder to monitor this growing attack surface, deploying AI-based and other sophisticated automated technology for routine surveillance is becoming essential.

We provide evidence-based knowledge about existing and emerging threats in a timely, accurate, relevant, and predictive manner. Intel drives security operations and informs and enhances decisions at every level.

- Security Operations
- Threat Detection & Response
- Attack Surface Management
- Crisis & Incident Response
- Technology Resilience



# Digital Privacy & Trust

is the foundational element of a successful digital transformation. The ability to operate a trusted, agile, digital identity system, with better protection and a seamless, secure user experience across the entire organization is paramount.

However, it is a challenge to find the skilled talent, implement and integrate the right technologies, and establish leading security processes for digital identity, while keeping up with the ever-changing demands and threats of a globally connected world.

## This is why we are here.

When Deloitte operates digital identity for you, your organization benefits from a **complete package of integrated market-leading technology, proven processes, and world-class talent**. With Digital Privacy & Trust by Deloitte, you can embed continuous advantage while confidently focusing on your business needs.

We handle every step of your digital integration, operating a unified, seamless transformation.





# Enterprise Security

The more applications you run, the more you need a holistic approach to security.

We heard you when you said you need to achieve secure business transformation faster. That's why we provide cyber accelerators to speed up implementations that result in secure and well-controlled applications, whether migrating to SAP S/4 HANA or undergoing a cloud transformation effort. We'll help you to standardize processes and improve customer experience by more effectively managing identities across the application ecosystem.

Not only will you be able to deal with emerging threats, you'll be capable of monitoring the overall solution for delivery excellence, compliance, quality, process improvements and other innovations activities. And we'll help you to reduce risk and costs without compromise by using advanced technology to transform business-critical risk processes and approaches that make implementations more effective and efficient.

- **Application Security**
- **Security Architecture**
- **Cloud Security**
- **Secure Landing Zones**
- **Emerging Technology**



# Cyber Operate

## Embedding 24/7 vigilance into your operations

When clients operate with Deloitte, they embed 24/7 vigilance into their operations, freeing them and their people to focus on running the business.

Deloitte's Cyber Operate services provide talent, market-leading technologies, and processes to operate your cyber capabilities including: the identity lifecycle, security operations, threat intelligence, application security, business transformation, and continuous compliance including third party risk management.

- **Managed Extended Detect & Respond (MXDR)**
- **Cyber Threat Intelligence**
- **Managed Digital Identity**
- **Continuous Compliance**
- **Managed Application Security**
- **Managed Cloud Security**
- **Cyber Foundry**





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

#### About Deloitte Singapore

In Singapore, risk advisory services are provided by Deloitte & Touche Enterprise Risk Services Pte. Ltd. and other services (where applicable) may be carried out by its subsidiaries and/or affiliates. Deloitte & Touche Enterprise Risk Services Pte. Ltd. (Unique entity number: 197800820D) is a company registered with the Accounting and Corporate Regulatory Authority of Singapore