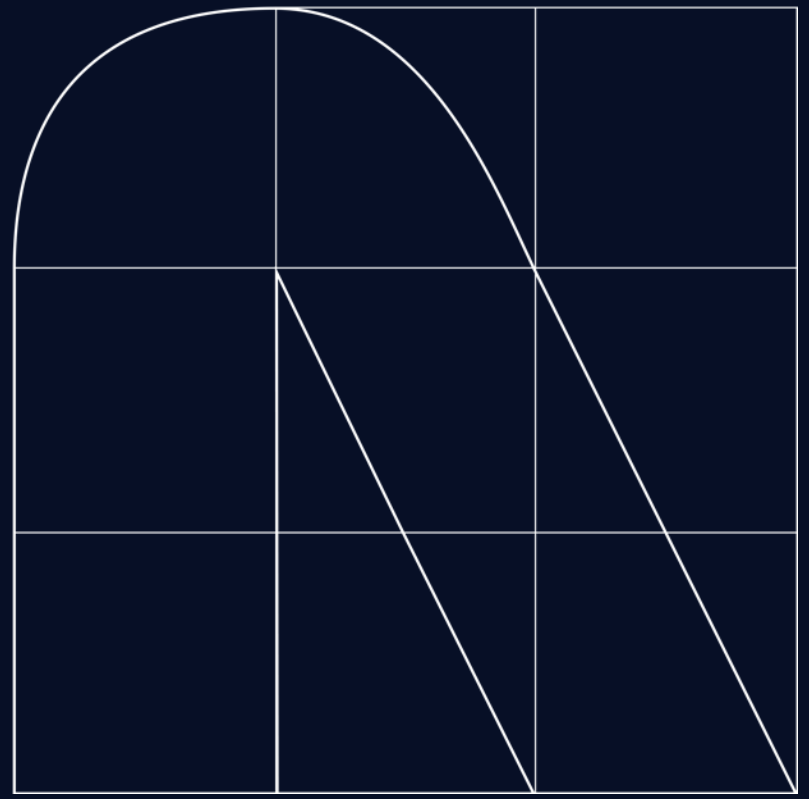
Beyond Firewalls: Embracing Zero Trust for Modern Cybersecurity

Stefaan Hinderyckx
Senior Vice President Cybersecurity

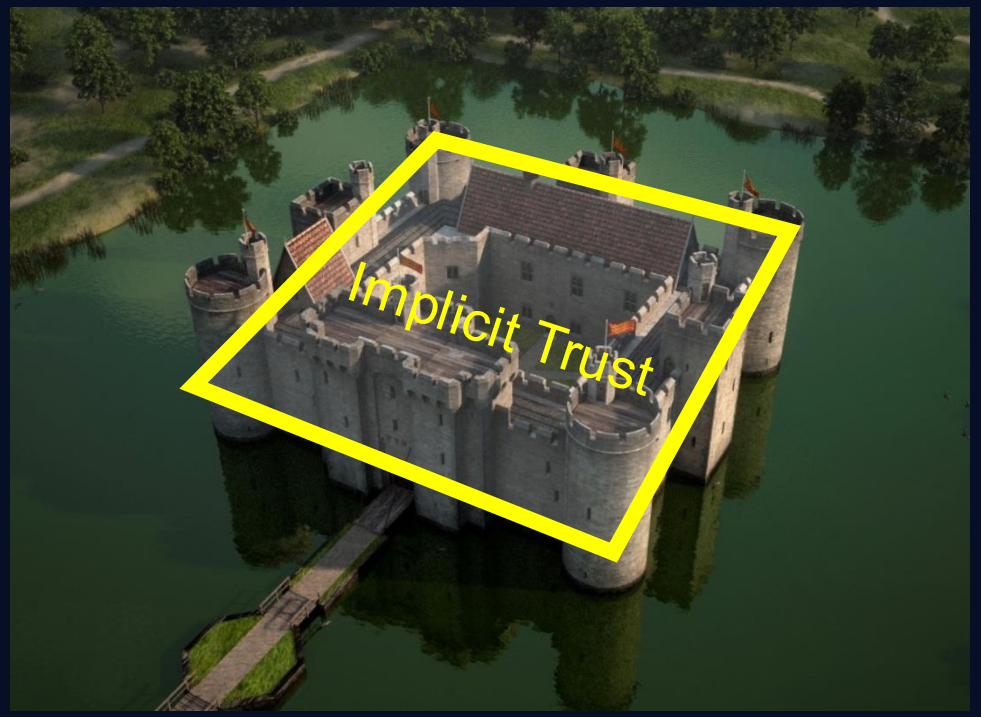


Zero Trust - The Philosophy

Never trust,
Always verify,
Assume breach

Why do we need Zero Trust?

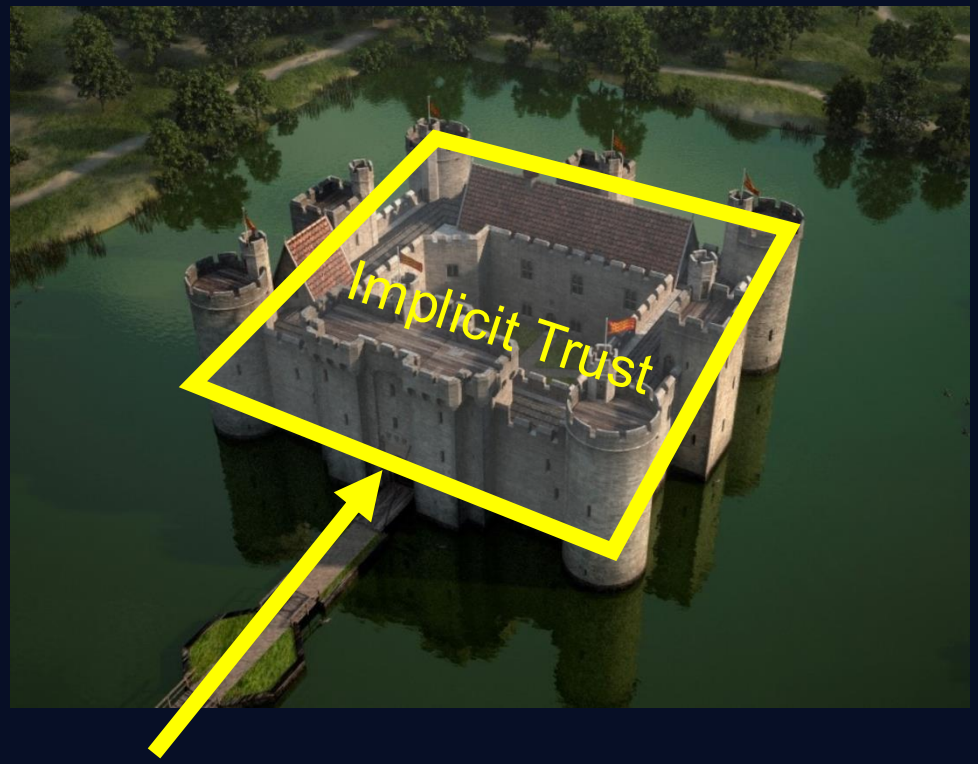
- Originally trust was based on you being ‘inside your place of work’ – whatever you did was trusted and whatever you sent came from a ‘trusted location’ - it meant ‘that everything inside an organization’s network should be implicitly trusted’



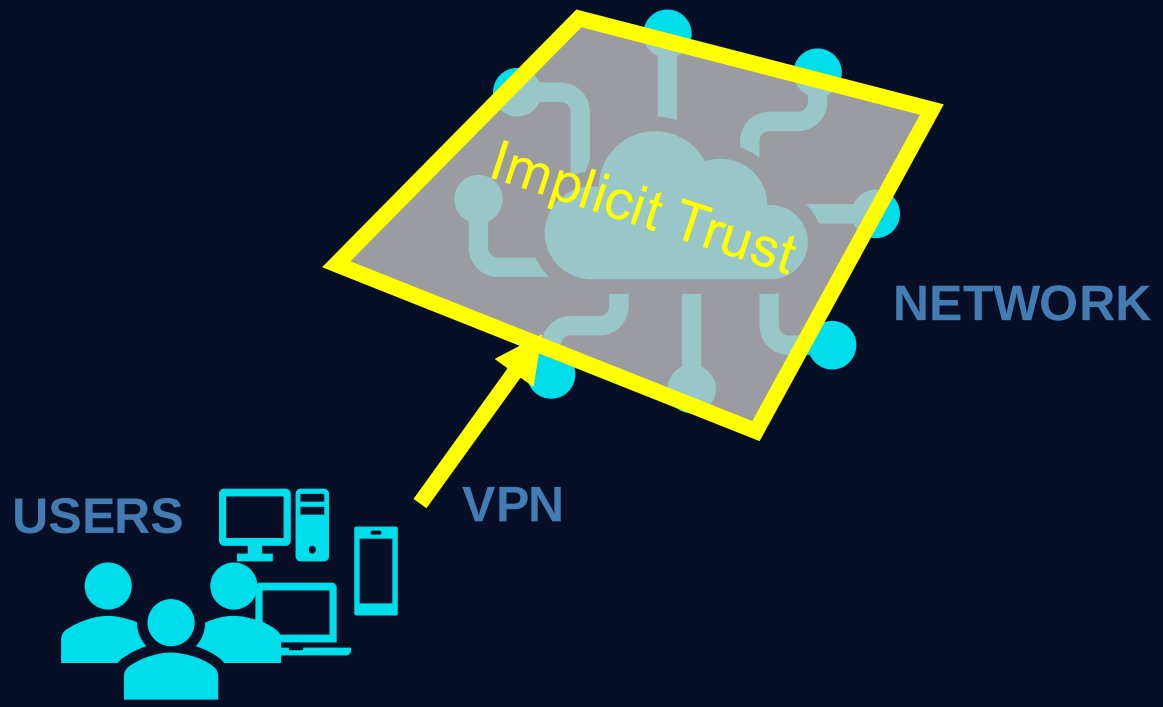
This implicit trust means that once on or in the network, users – *including threat actors and malicious insiders* – are free to move laterally and access or exfiltrate sensitive data due to a lack of granular security controls.

Trust in the Castle – was Implicit

- A VPN solution into your network was commonly used during the lockdowns, it allowed remote working but gave the same level of trust outside of the network to those inside.



The road into the castle is like the VPN tunnel.

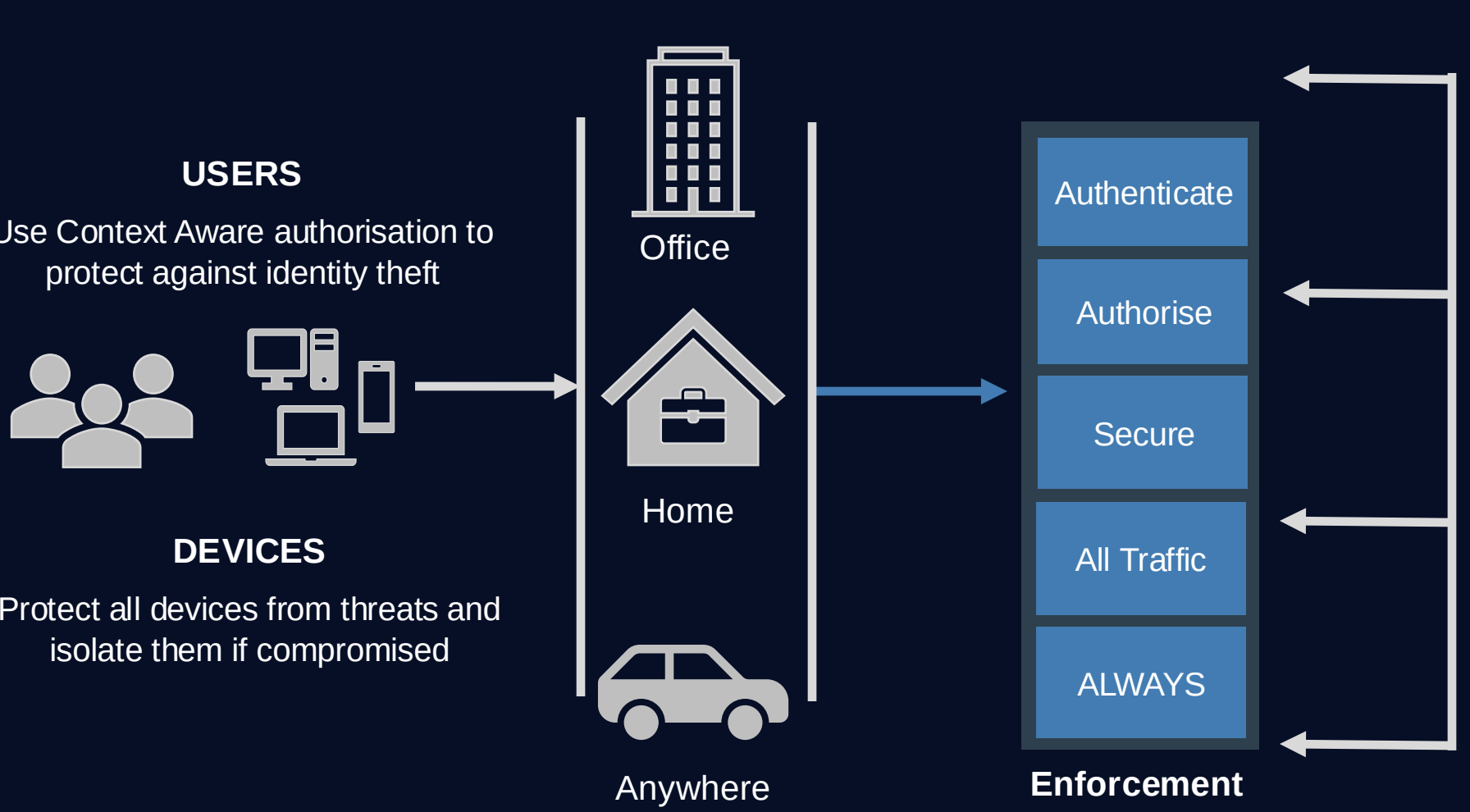


Zero Trust – in an Airport

- Imagine what would happen if implicit trust was allowed at an airport? Once you are inside you could go anywhere, get on any plane, fly to any destination or get in the cockpit

Airports require identification (passport) and authorization (ticket) – for the traveler it gives us access to public areas, the gate, the plane and our seat. They go further than that too, they have roles – that identification allows access to different areas. Such as offices, baggage, security handling or the runways.

Zero Trust – Introduction - a logical view of the Enterprise



DATA

Classify protect and encrypt your data wherever it is

APPLICATIONS

Protect your applications from leaking valuable data

WORKLOADS

Protect your workloads with extended visibility and adaptable policy

NETWORKS

Prevent malicious lateral movement with segmentation and NDR

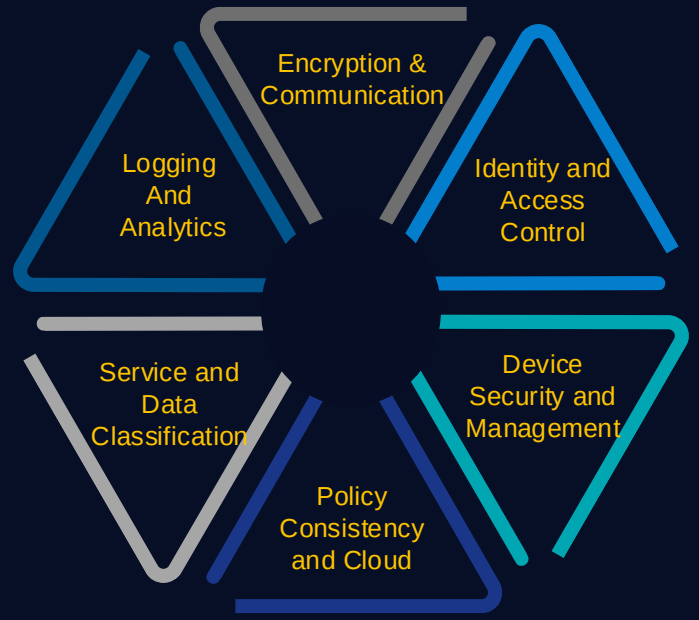
Zero Trust Thought Principle – The Kipling Method

Criteria	Description
Who	Asks for the asserted identity of the *user or entity* that attempts resource access.
What	Identifies the application used or the *data being accessed*.
When	Tracks the time of data access. Time limits can be established for access based on Who, What, Where, Why and How.
Where	Allows security solutions to track where accessed data resides.
Why	An analysis of the context of data access attempts. This relates to data classification
How	Asks about data access methods. Access methods can be controlled based on the who, what, when, where, and why of an access request.

Zero Trust Architecture Guiding Principles

- All communications must be encrypted. Any exceptions must be deliberate (e.g., DNS).

- Network traffic metadata must be logged and enriched with identity context.
- Network traffic must be able to be examined for security and data loss purposes.
- Automation must include identity-centric details to provide efficient and effective incident response.
- Logs must be included in analytics tools for effective and dynamic enforcement of policies.



- System must be able to enforce access controls for all types of resources. Access control mechanisms must be driven by identity-centric and contextual policies.
- Data resource protections should be able to use identity and contextual policies to control access.
- Access to any network resource must be explicitly granted by policy. No user or device should inherently have broad network access.

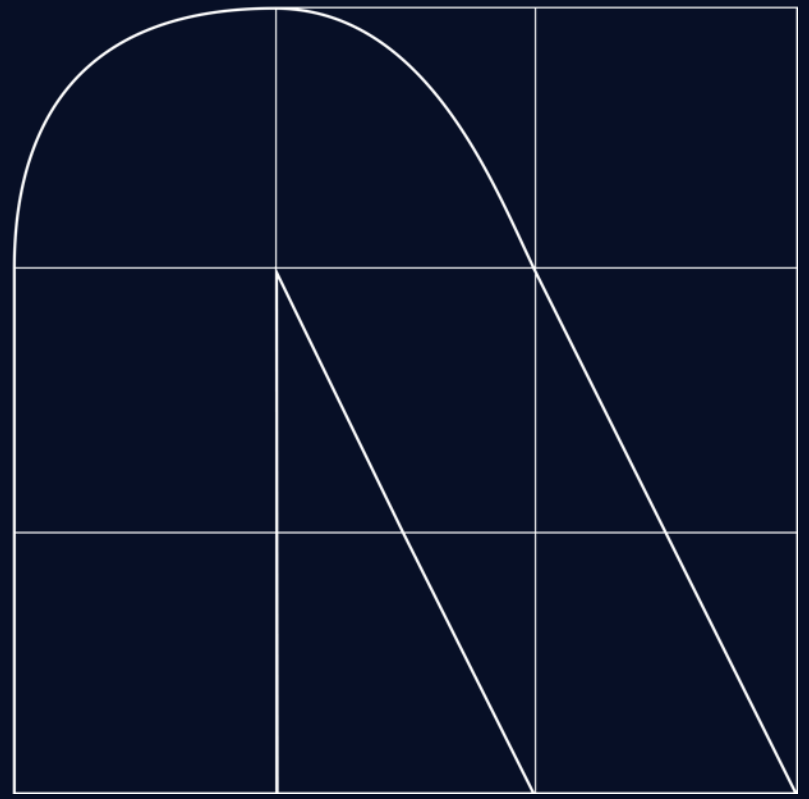
- Access controls must be able to distinguish between different services on the same network resource. For example, access to HTTPS must be granted separately from access to SSH.
- Access to specific data elements contained within applications or containers that have different classifications must be enforced based on business policy.

- Devices must be able to be inspected for their security posture and configuration prior to being granted access, and periodically thereafter.
- It must be possible to distinguish BYOD from corporate-managed devices and control the level of access accordingly.

- System and policy model must support securing all users in all locations. Policy model and controls must be consistent for remote and on-premises users.
- Workloads transferred into the cloud should include the same access control policies as defined by on-premises solutions.

Source: NIST 800-207
Source: Zero Trust Security: An Enterprise Guide – Jason Garbis, Jerry W. Chapman

Zero-Trust Architecture Approach

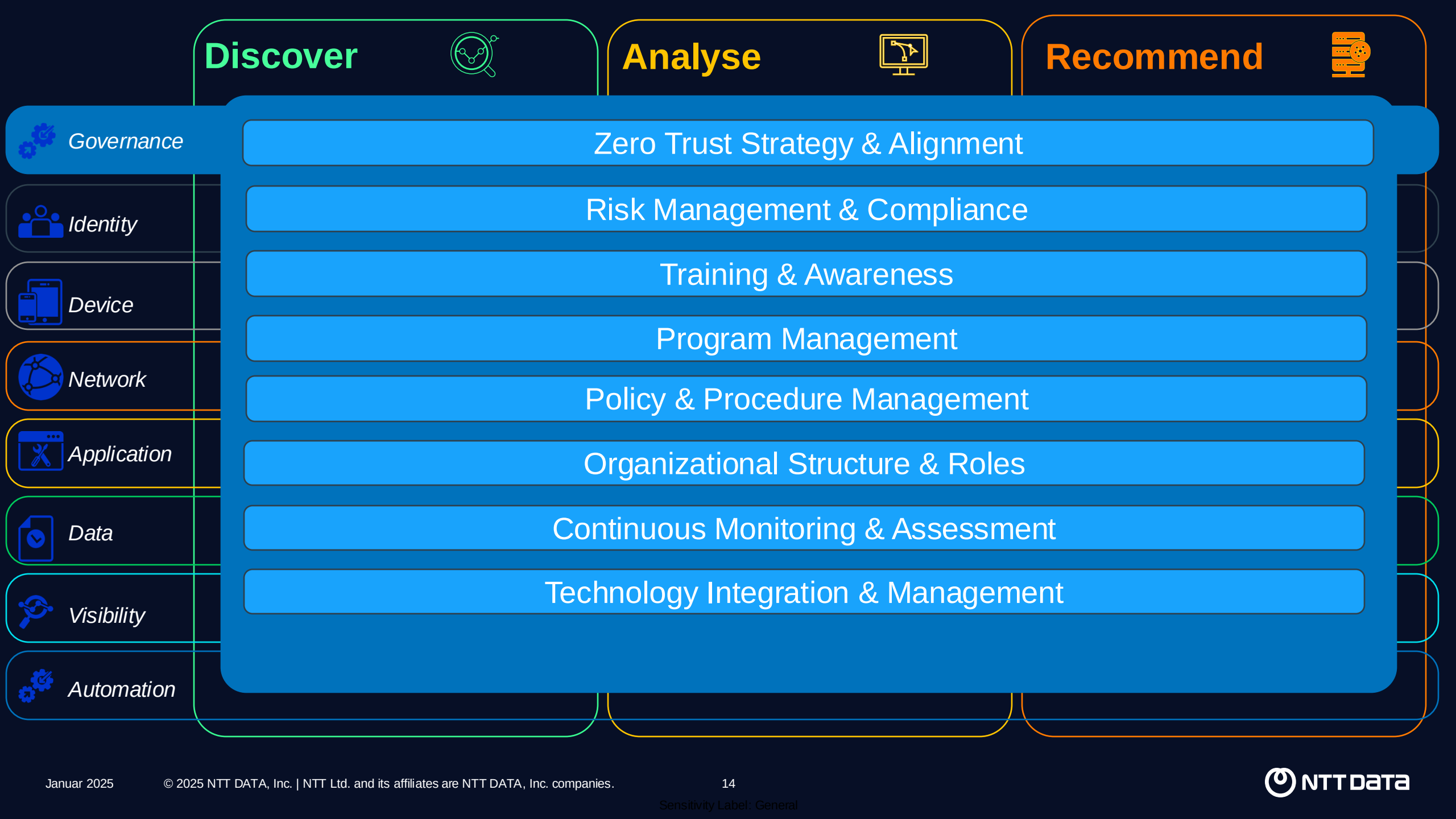


	Discover	Analyse	Recommend
Governance			
Identity			
Device			
Network			
Application			
Data			
Visibility			
Automation			

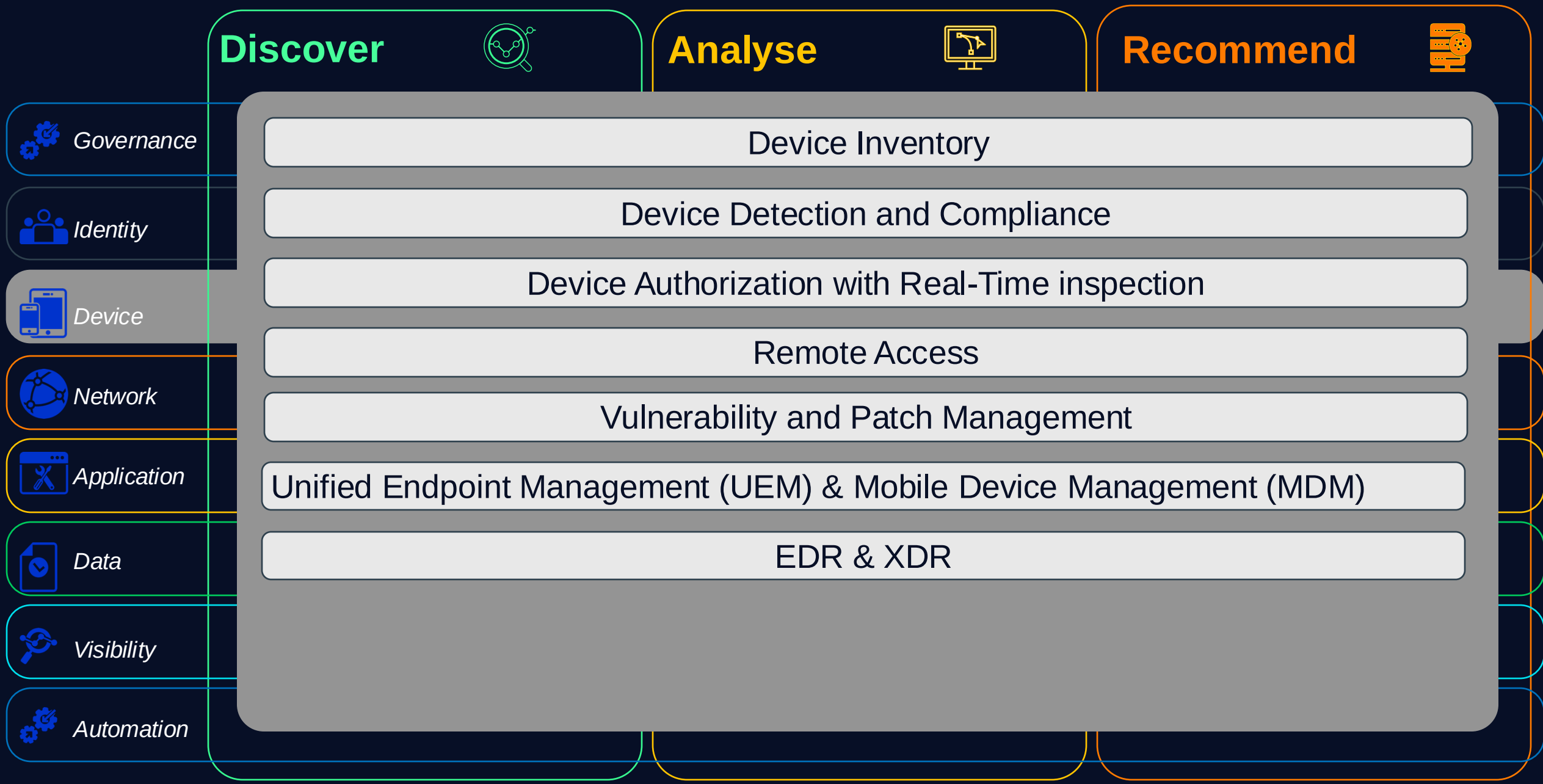
	Discover	Analyse	Recommend
Governance	Review risk management, policies, procedures, and compliance measures to ensure alignment with regulatory requirements and best practices		
Identity	Evaluate current identity and access management (IAM) practices to ensure only authorized users have access to resources.		
Device	Review the security posture of all devices accessing the network to identify and mitigate risks from compromised or non-compliant devices		
Network	Inspect network segmentation and traffic monitoring to prevent unauthorized access and detect suspicious activities.		
Application	Assess the security measures in place for applications to protect them from vulnerabilities and attacks.		
Data	Analyze data protection strategies and encryption practices to safeguard sensitive information from breaches and leaks.		
Visibility	Evaluate incident response and monitoring capabilities to ensure effective detection, response, and recovery from security incidents		
Automation	Integrate automated processes and tools to enhance efficiency, reduce human error, and ensure consistent security practices		

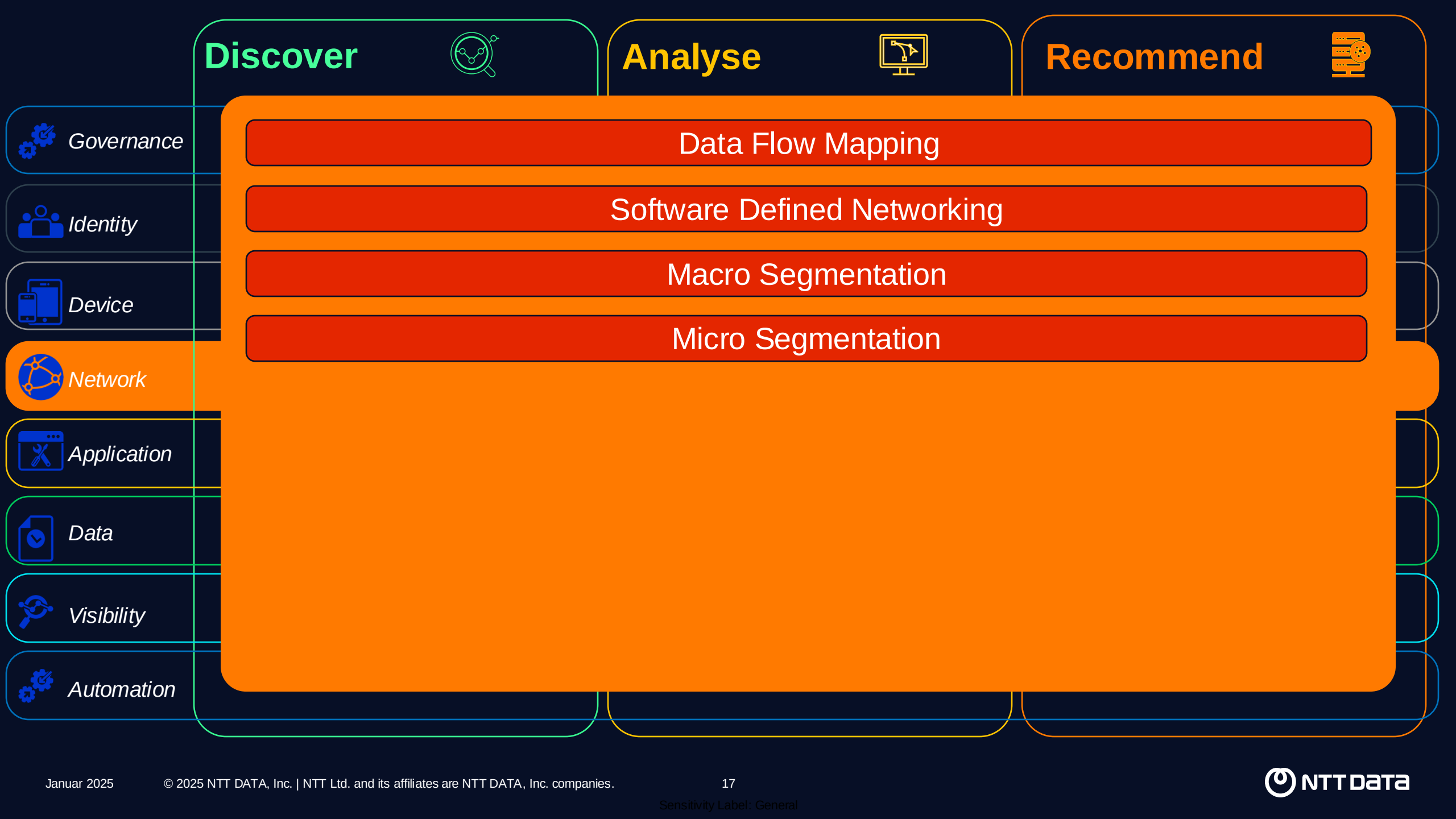
	Discover	Analyse	Recommend
Governance	Review risk management, policies, procedures, and compliance measures to ensure alignment with regulatory requirements and best practices	Capture new requirements from the customer, Zero Trust best practices, and open frameworks like NIST 800-207	
Identity	Evaluate current identity and access management (IAM) practices to ensure only authorized users have access to resources.	Conduct a gap analysis to identify discrepancies between current state and desired state.	
Device	Review the security posture of all devices accessing the network to identify and mitigate risks from compromised or non-compliant devices	Detect dependencies and prioritize actions based on impact and feasibility.	
Network	Inspect network segmentation and traffic monitoring to prevent unauthorized access and detect suspicious activities.	Draft a high-level architecture for each Zero Trust pillar to guide implementation.	
Application	Assess the security measures in place for applications to protect them from vulnerabilities and attacks.		
Data	Analyze data protection strategies and encryption practices to safeguard sensitive information from breaches and leaks.		
Visibility	Evaluate incident response and monitoring capabilities to ensure effective detection, response, and recovery from security incidents		
Automation	Integrate automated processes and tools to enhance efficiency, reduce human error, and ensure consistent security practices		

	Discover	Analyse	Recommend
Governance	Review risk management, policies, procedures, and compliance measures to ensure alignment with regulatory requirements and best practices	Capture new requirements from the customer, Zero Trust best practices, and open standards like NIST 800-207	Propose the final versions of the architecture for each Zero Trust pillar, ensuring they align with customer requirements, best practices, and frameworks.
Identity	Evaluate current identity and access management (IAM) practices to ensure only authorized users have access to resources.	Conduct a gap analysis to identify discrepancies between current state and desired state.	Develop a prioritized roadmap to guide the implementation of the recommended solutions.
Device	Review the security posture of all devices accessing the network to identify and mitigate risks from compromised or non-compliant devices	Detect dependencies and prioritize actions based on impact and feasibility.	Provide detailed recommendations for addressing identified gaps and dependencies.
Network	Inspect network segmentation and traffic monitoring to prevent unauthorized access and detect suspicious activities.	Draft a high-level architecture for each Zero Trust pillar to guide implementation.	Outline actionable steps and timelines for achieving the desired security posture.
Application	Assess the security measures in place for applications to protect them from vulnerabilities and attacks.		
Data	Analyze data protection strategies and encryption practices to safeguard sensitive information from breaches and leaks.		
Visibility	Evaluate incident response and monitoring capabilities to ensure effective detection, response, and recovery from security incidents		
Automation	Integrate automated processes and tools to enhance efficiency, reduce human error, and ensure consistent security practices		



	Discover	Analyse	Recommend
Governance			
Identity	User Inventory	Conditional User Access	Multi-Factory Authentication
Device	Privileged Access Management	Behavioral Contextual ID and Biometrics	Least Privileged Access
Network	Continuous Authentication	Integrated ICAM platform	
Application			
Data			
Visibility			
Automation			





Discover

Analyse

Recommend

- Governance
- Identity
- Device
- Network
- Application
- Data
- Visibility
- Automation

Application Inventory

Secure Software Development & Integration

Software Risk Management

Resource Authorization & Integration

Continuous Monitoring and Ongoing Authorizations

	Discover	Analyse	Recommend
Governance			
Identity			
Device			
Network			
Application			
Data	Data Catalog Risk Assessment	Enterprise Data Governance	Data Labeling and Tagging
Visibility	Data Monitoring and Sensing	Data Encryption	Data Loss Prevention
Automation	Data Access Control		

Discover

Analyse

Recommend

- Governance
- Identity
- Device
- Network
- Application
- Data
- Visibility
- Automation

Log All Traffic (Network, Data, Apps, Users)

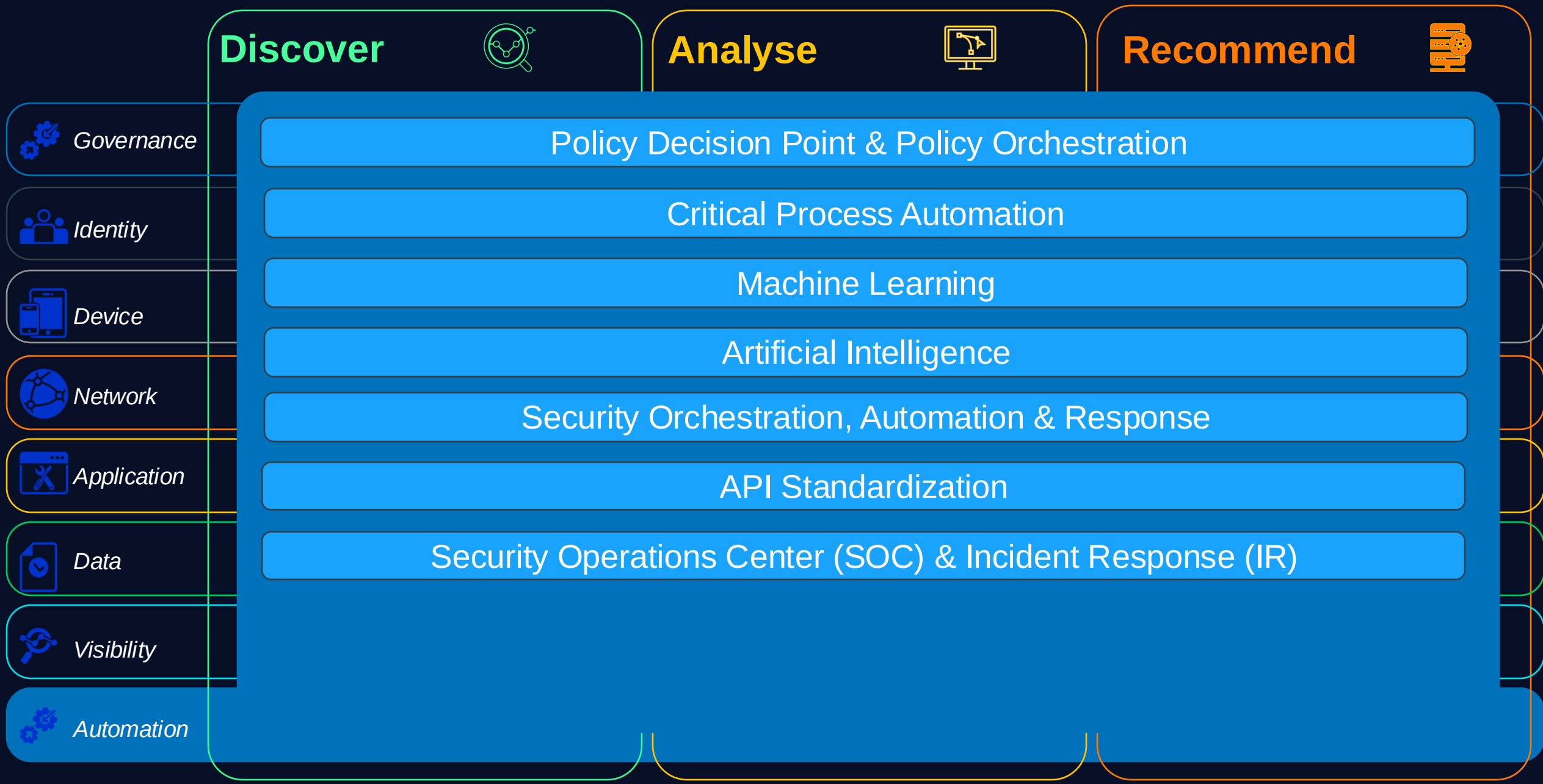
Security Information and Event Management (SIEM)

Common Security and Risk Analytics

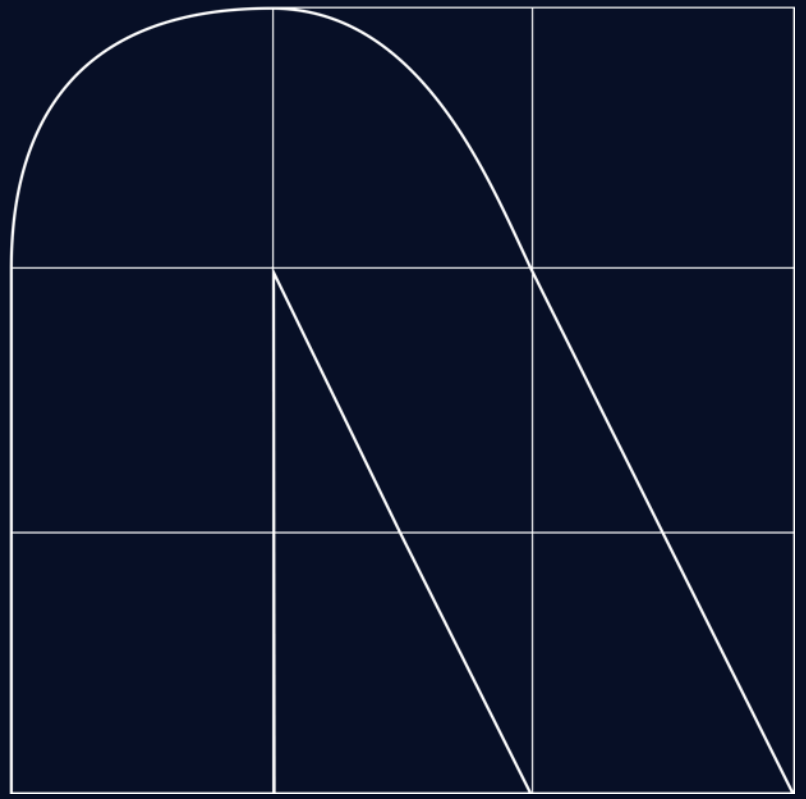
User and Entity Behaviour Analytics

Threat Intelligence Integration

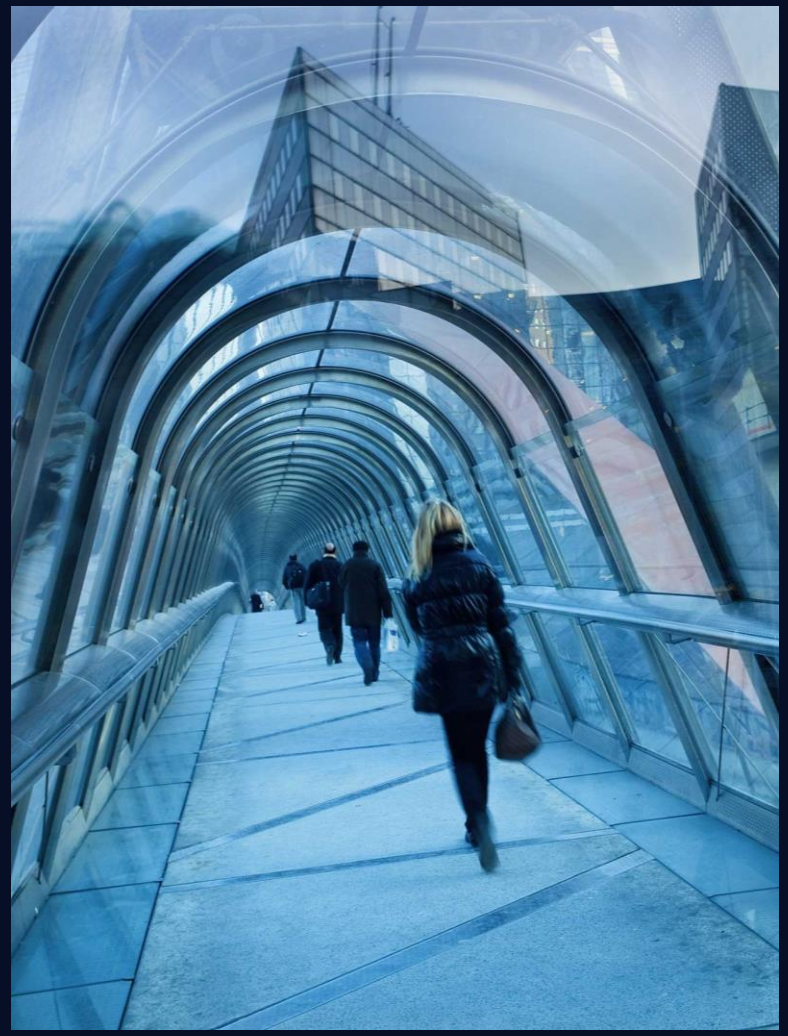
Automated Dynamic Policies



Zero Trust Case Studies



Introducing the cases



Case 1

- Media Sector
- > 1.200 employees
- Europe Based
- Serious cybersecurity incidents took place
- Transitioning to cloud
- Technical Debt
- IT and OT (Printing) scope

Case 2

- Food Industry
- > 13.000 employee
- > 60 factories worldwide
- Difficulties in defining an overarching security vision
- IT and OT (food production) scope

Customer Concerns

"Embrace the Zero Trust Architecture approach"

"Respect the install base"

"Step away from static, network-based perimeter security "

"Reduce the likelihood of security incidents to occur and when it does occur, to limit the impact"

Dynamic, secure access of authorized and verified users and devices to your assets and data

"Guidance in the journey towards a Zero Trust Architecture"

NTT DATA

Mission

- This customer was well aware that embracing the **Zero Trust Architecture** approach can offer many advantages to the organization. The main philosophy of Zero Trust Architecture is that one ***steps away from static, network-based perimeter security*** but instead focusses on granting ***dynamic, secure access of authorized and verified users and devices to your assets and data***.
- The main driver to adopt zero trust architecture is to ***reduce the likelihood of security incidents to occur and when it does occur, to limit the impact***.
- Zero trust architecture is an evolving set of cybersecurity paradigms that spans many parts of IT infrastructure. In this offer we propose the NTT consulting approach to guide this customer on the **journey towards a Zero Trust Architecture**.

NTT Data Approach

Engage

- Scope the mission
- Offer
- Assemble the teams

Discover

- Gather organizational context. Collect the vision, strategy and pains of the CISO, CIO, Enterprise Architects
- Discover the current state and pains for the pillars
  - Identity
  - Device
  - Network & Environment
  - Data
  - Visibilty & Analytics
  - Automation and Orchestration

Sources: Workshops, Design documents, Policies&Procedures

Analyse

- Process the collected data
- Create high-level architecture of the recommended desired state
- Gap analysis
- Identify key initiatives to close the gaps
- Gather budgetary information for the key initiatives
- Create a roadmap

Recommend

- Present the outcomes to the stakeholders:
  - High-Level Architecture
  - Prioritized roadmap
  - Budgetary information on the key initiatives

Next Steps

- Customer based the budget for the next 5 years upon the Zero-Trust Architecture Study
- Customer is executing the roadmap in collaboration with NTT Data
  - Project Definition per item on the roadmap
  - Primer (Scope, budget, purchase, HLD, LLD, implement, transition to support)

Follow-up

Customer based the budget for the next 5 years upon the Zero-Trust Architecture Study

Identify the client's business needs and objectives

Propose an appropriate Solution

Finalise the contractual terms and conditions

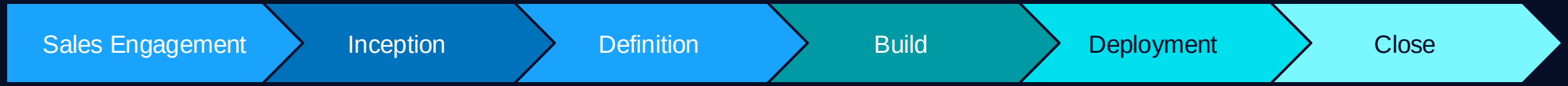
Define
and document the detailed Solution requirements

Plan
the Project in accordance with the requirements

Deploy the tested Solution in its operational environment.

Perform Acceptance Testing.

Operationalise the accepted Solution and hand over to the identified operational, support and maintenance agents



Initiate
a Project to deliver the Solution

Review
the proposed high level Solution

Establish
the Project team roles and responsibilities

Design
the Solution in accordance with the specified requirements.

Create the Solution in accordance with the approved design

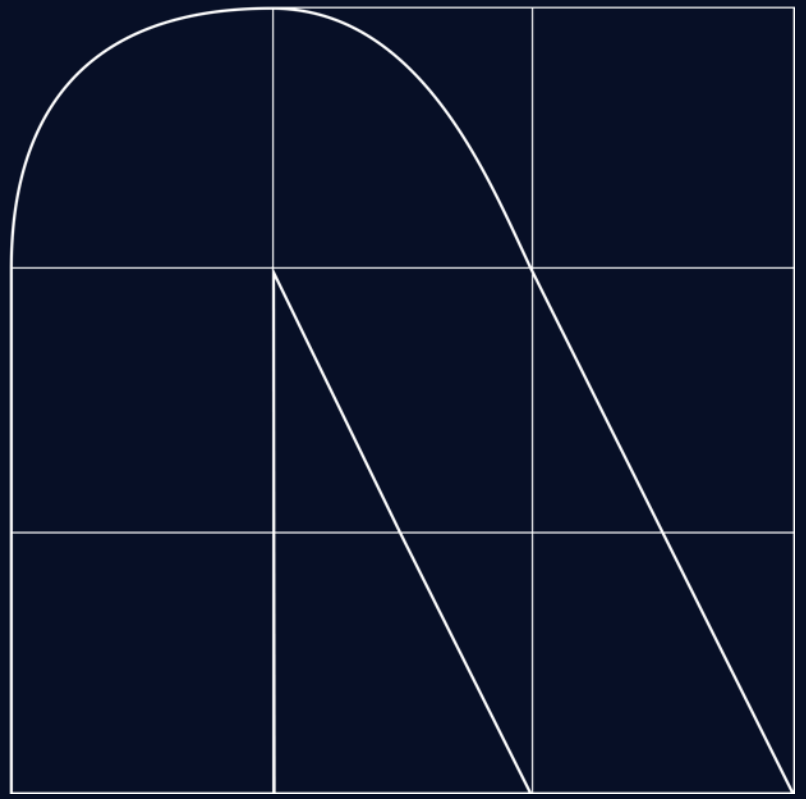
Perform Verification Testing of built Solution.

Perform Final Billing

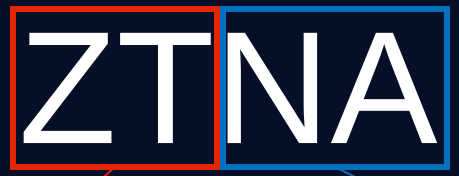
Review
the operationalised Solution

Close
the Project and dissolve the Project team

Zero-Trust Network Architecture



ZTNA



Zero-Trust

- Identity
- Enforcement
- Encryption
- Application-Targeted

Network Access

- Remote Access
- Network Access Layer

SASE, ZTNA, SSE, Zero Trust?

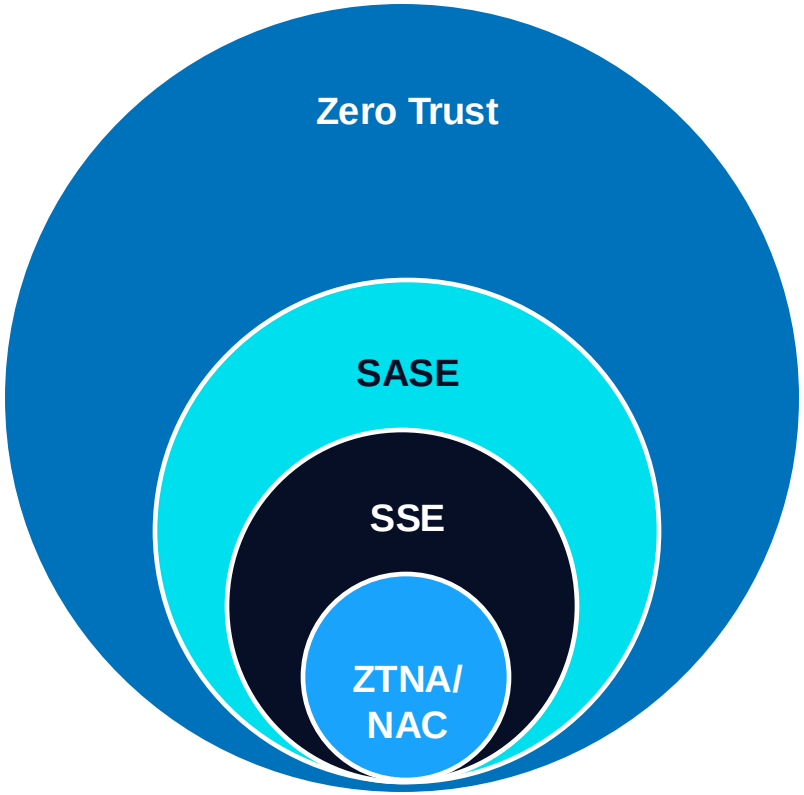
Understanding the key differences between **ZTNA** (Zero Trust Network Access), **SSE** (Security Service Edge)**, SASE** (Secure Access Service Edge), and the overarching **Zero Trust** Security model is key. Each of these concepts plays a vital role in a modern cybersecurity strategy

Key differences

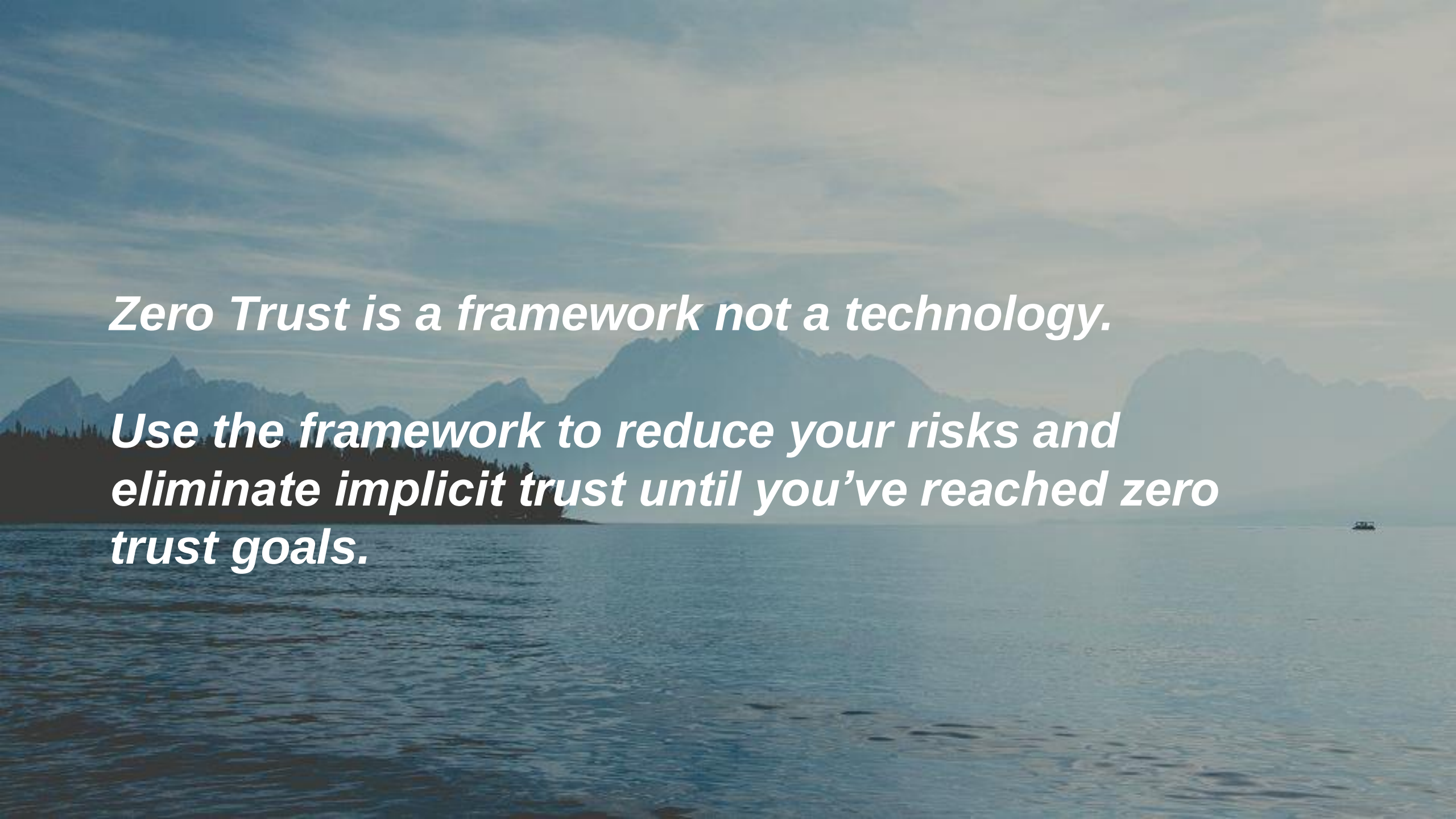
ZTNA vs. Zero Trust: ZTNA is an application of Zero trust principles focused specifically on Network Access Control (NAC).

SSE vs. SASE: SSE is a subset of SASE, focusing solely on Security functions, while SASE includes both, network and security services

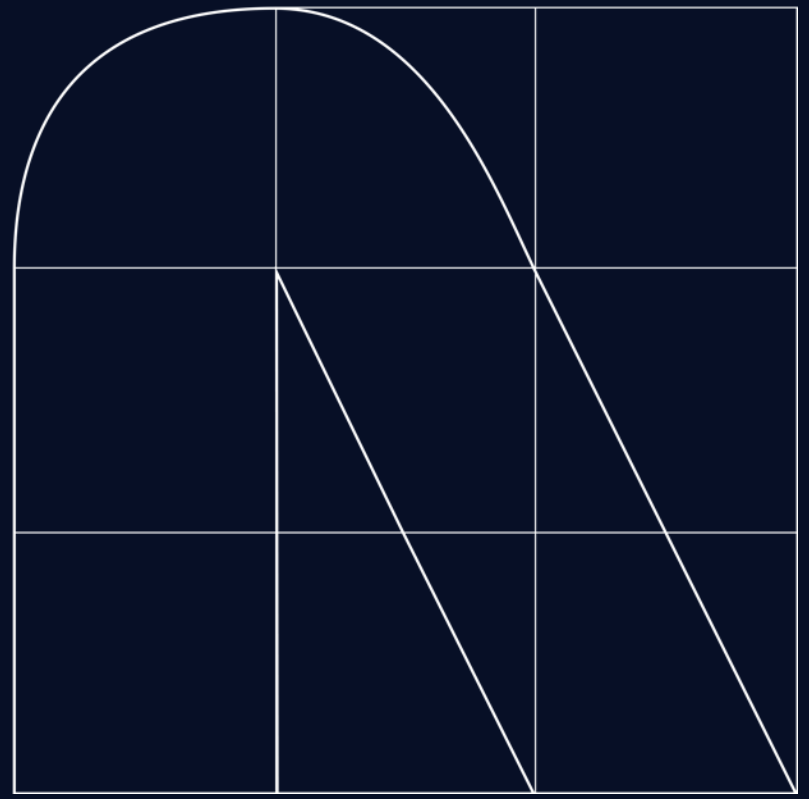
SASE vs. Zero Trust: SASE is an architecture that can implement Zero Trust across network and security services. Zero Trust itself is not tied to any specific technology or architecture but is a guiding principle for cybersecurity strategies.



- **Zero Trust Network Access (ZTNA):** ZTNA enforces strict identify verification for every access request, applying a “never trust, always verify” principle to Network Access, enhancing security regardless of user location.
- **Secure Service Edge (SSE):** SSE, part of SASE focuses on security functions like SWG, CASB and FWaaS, offering robust, cloud-based protections that secure data and users everywhere.
- **Secure Access Service Edge (SASE):** SASE merges networking and security into cloud services, enabling dynamic, secure access management across diverse environments, streamlining operations and enhancing security.
- **Zero Trust:** Zero Trust is an overall cybersecurity strategy and requires continuous verification of everything (users, devices and application) with no assumption of trust, ensuring comprehensive security across all system interactions.


Zero Trust is a framework not a technology.
Use the framework to reduce your risks and eliminate implicit trust until you've reached zero trust goals.

Beyond Firewalls: Embracing Zero Trust for Modern Cybersecurity



Stefaan Hinderyckx
Senior Vice President Cybersecurity