wipro

Deciphering zero trust architecture

Cyber threats are ever evolving and hackers are getting more sophisticated; adopting newer techniques ranging from social engineering attacks to APTs (Advanced persistent threats), malicious threat actors seeking to gain unauthorized access to networks and systems, or exfiltrate sensitive information that could result in operational, financial and reputational damages to any organization. This article focuses on what zero-trust architecture is, or in other words, a security-focused approach explained in a simple enterprise architecture view point, and how it can help in curbing the above-mentioned risks by imposing access validation and control at every layer.

Conceptual representation of a zero-trust model

The fundamental principle behind zero-trust architecture is tailored behind one key principle i.e. deny by default and allow only if authenticated and on a ‘need to know’ basis. Additionally, continue to monitor for anomalies, and where possible, remove human intervention.

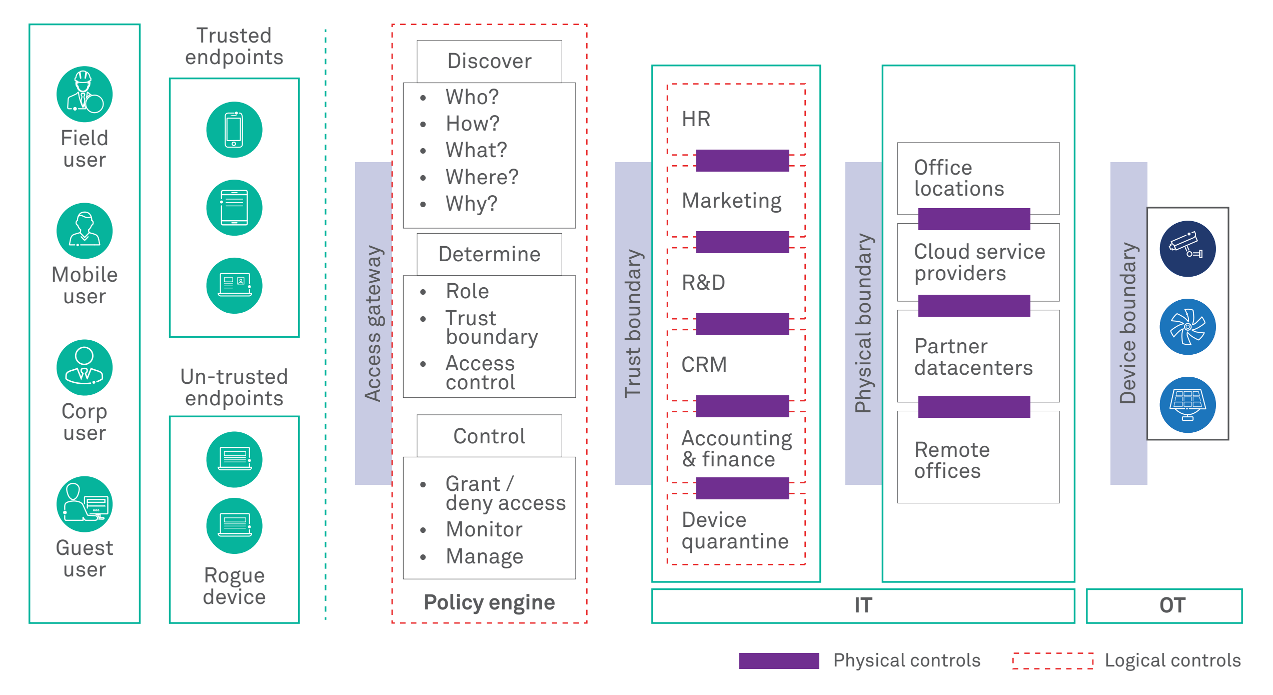
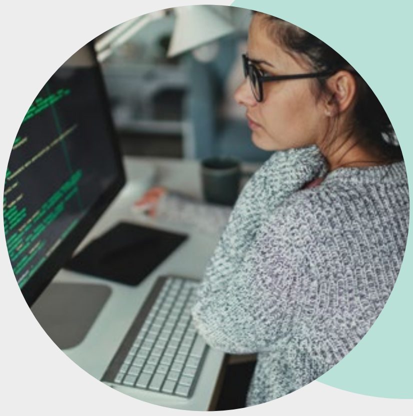


Fig 1: Target Network posture



The journey of successful implementation of zero trust architecture requires meticulous planning.

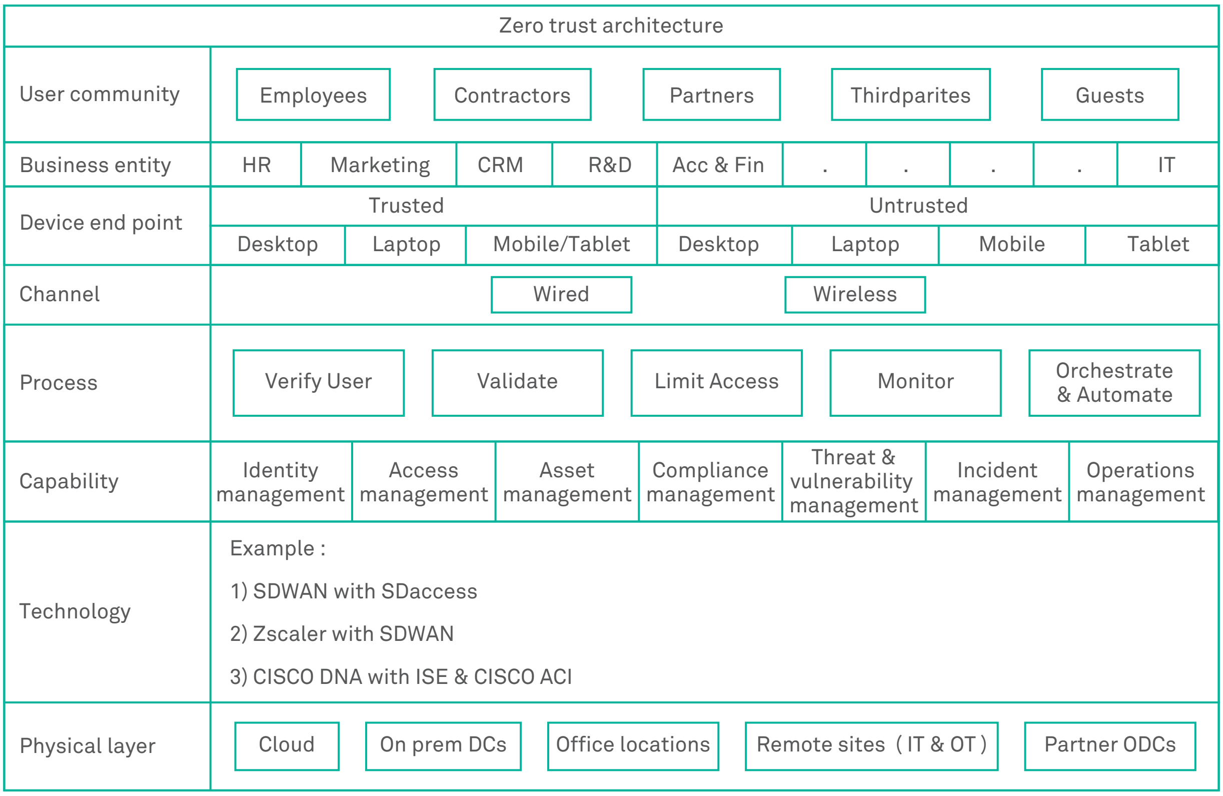
The core of the architecture that delivers the zero-trust is the centralized control pane (in the above diagram the policy engine). Fundamentally, this transforms the traditional model from a full mesh (any to any) type of configuration to a typical hub-and-spoke model where the control pane is centralized. The benefit of this approach is the visibility, ease of administration and control. Rules are defined at the policy engine that enables this journey to a zero-trust architecture. Every request to access is now validated at the centralized control pane and access is granted or denied based on access rules that are continuously monitored for every event.

Let us look at a use case where Wipro was engaged as a consulting partner to enable the transformation to zero-trust model. The client was a large utilities organization in the UK that had multiple business units and each one of them carrying a varied risk appetite. So, one common security policy was not sufficient to control and govern the security posture. Containment of risk was the paramount consideration in this case. Wipro's vast experience and knowledge -- both from an enterprise architecture perspective and from a security architecture perspective -- about the current landscape of the customer combined with industry experience and technology expertise was very crucial to devise the strategic architecture.

The journey of successful implementation of zero trust architecture requires meticulous planning that consists of four important steps:

- Identify the data – It is important to understand what data is important and where and how it is spread within an organization. Ultimately, it is the data that has the utmost value to any digital organization.
- Discover the assets – Next in line is discover the assets. The word "asset" is a broad term and this includes end users belonging to specific business groups, devices such as mobiles, laptops, printers, EPBAX and network equipment, OT devices and applications, locations, etc.
- Map the dependencies – Identifying the assets and related dependencies such as application interfaces, user tagging, device mapping etc.
- Tailor the rules – Last but perhaps the most time-consuming step that requires a lot of attention to detail is to create the permit/deny rules. No organization would want to take a big-bang approach and cause disruption to their business. This is where the role of automation and orchestration could be very handy, to enable and monitor mode for a stipulated period, visualization, dry run, and then implimentation to production.

The following section highlights the capability architecture (Enterprise architecture view) that enables a zero-trust model



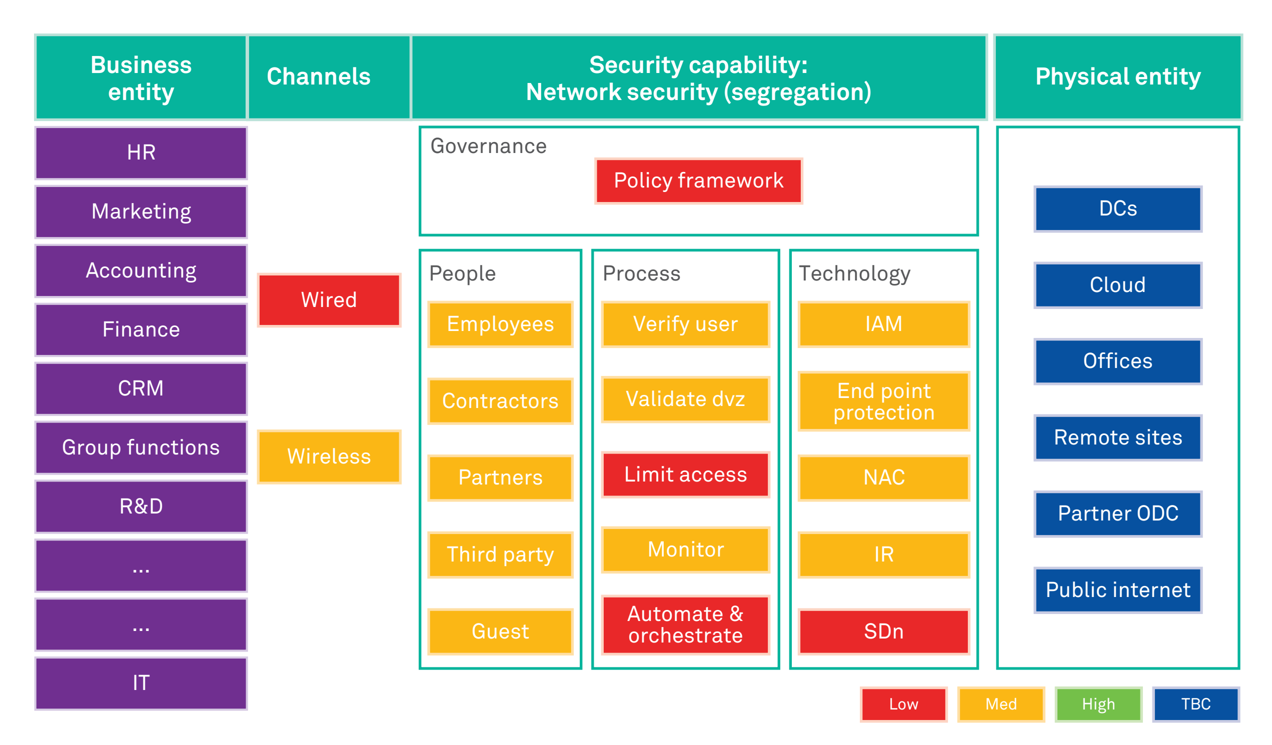
Zero trust architecture	
User community	Employees Contractors Partners Thirdparites Guests
Business entity	HR Marketing CRM R&D Acc & Fin . . . . IT
Device end point	Trusted: Desktop Laptop Mobile/Tablet Untrusted: Desktop Laptop Mobile Tablet
Channel	Wired Wireless
Process	Verify User Validate Limit Access Monitor Orchestrate & Automate
Capability	Identity management Access management Asset management Compliance management Threat & vulnerability management Incident management Operations management
Technology	Example : 1) SDWAN with SDaccess 2) Zscaler with SDWAN 3) CISCO DNA with ISE & CISCO ACI
Physical layer	Cloud On prem DCs Office locations Remote sites (IT & OT) Partner ODCs

Fig 2: Capability architecture

The most critical building block in the above diagram is ‘the process layer’ that consists of 5 key processes:

- Verify user – Objective is to validate that user is the person who he claims to be and has the necessary privileges to request access of a resource
- Validate the device / time – to validate whether compliant or not and intent
- Restrict access – The fulcrum of the zero-trust architecture that controls access
- Monitor – A process that continuously keeps tabs on ongoing events and alerts on anomalies
- Automate and orchestrate – To reduce human error

Capability architecture defines the underpinning technology layers that can enable a fully functional zero-trust architecture. It is vital to strengthen the capabilities that can support the objective of the five pillars. A good starting point is to perform a capability maturity assessment that looks at people, process, policy framework and technology perspective as to what is the current state within an organization and build the target state in a modular fashion.



Business entity

HR

Marketing

Accounting

Finance

CRM

Group functions

R&D

...

...

IT

Channels

Wired

Wireless

Security capability: Network security (segregation)

Governance

Policy framework

People

Employees

Contractors

Partners

Third party

Guest

Process

Verify user

Validate dvz

Limit access

Monitor

Automate & orchestrate

Technology

IAM

End point protection

NAC

IR

SDn

Physical entity

DCs

Cloud

Offices

Remote sites

Partner ODC

Public internet

🟥 Low 🟨 Med 🟩 High 🟦 TBC

Fig 3: Capability maturity assessment

Summary

Zero-trust model is the way forward for organizations that are banking on it as a security measure to identify, detect, protect and contain access risks that could potentially result in breaches. Fundamentally, the model equips organizations to validate every access request and permit or deny based on business rules. In principle, it is important to identify the data, assets, map dependencies and create rules.

A meticulous approach to enable successful implementation of the zero-trust model is to look at it from a people, process, policies and technology perspective. However, it is also important to highlight the importance of the changing dynamics of the IT landscape in any organization that really calls out for an automated approach to discover assets, design and implementation.

About the author

Shivakumar Ramachandran
Principal Consultant,
Wipro Limited.

Shivakumar Ramachandran MBCS, CISSP, TOGAF is a Principal Consultant with Wipro's modern application services: consulting practice and possesses a wealth of experience working on strategy and architecture engagements as an enterprise architect, enterprise security architect, in digital consulting and cloud computing, for clients across UK and Europe.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at
info@wipro.com