Zero Trust Approach

SURAKSHA
INFORMATION SECURITY

Zero **Trust**

Zero Trust monitoring and protection go hand in hand for a complete SOC solution. Workshop provides a complete 360 degree AYCE** model for all the eight pillars of "Zero Trust Architecture" (ZTA) User, Device, Network, Infrastructure, Application, Data, Visualization & Analytics and Orchestration.

Zero Trust Transformation

A holistic approach to Zero Trust should extend to your entire digital estate – inclusive of identities, endpoints, network, data, apps, and infrastructure. Zero Trust architecture serves as a comprehensive end-to-end strategy and requires integration across the elements.

Although the ZT approach is primarily focused on protecting data and services, it protects all enterprise resources (devices, infrastructure components, applications, virtual and cloud components) and targets (end users, applications, and other non-human entities) can and should be extended to include to include information from sources).

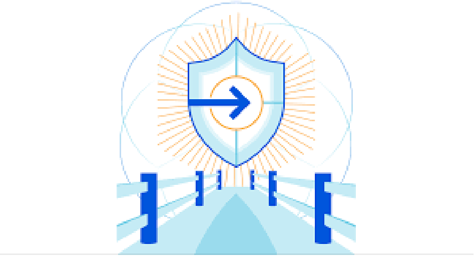
Zero Trust, principle is to **verify explicitly, apply least privileged access** and **always assume breach.**

This workshop is to enable you to transform into a Zero Trust Architecture for your organization.

Start the gap analysis

1. Establish business objectives and safeguard surfaces

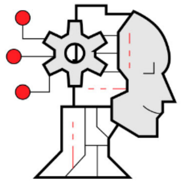
Complete gap analysis



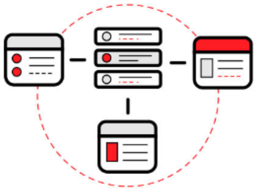
Develop full roadmap

Zero Trust security layers
Full knowledge workshop

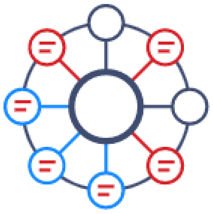
Zero Trust



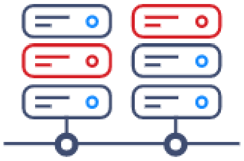
User Identity



Device - Endpoints

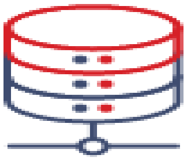


Network



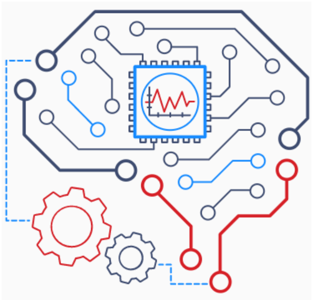
Infrastructure

Applications



Data

Visualization



Orchestration

Forensics

User Identity

Zero Trust starts with **identity**, verifying that only the people, devices and processes that have been granted access to your resources can access them.

Device - Endpoints

Next comes asssessing the security compliance of device **endpoints** - the hardware accessing your data - including the IoT systems on the edge.

Network

Next, there are protections at the **network** layer for access to resources – especially those within your corporate perimeter.

Infrastructure

Followed by the **infrastructure** hosting your data on-premises and in the cloud. This can be physical or virtual, including containers and micro-services and the underlying operating systems and firmware.

Applications

This oversight applies to your **applications** too, whether local or in the Cloud, as the software-level entry points to your information.

Data

And finally, protection of the data itself across your files and content, as well as structured and unstructured data wherever it resides

Visualization & Analytics

And finally, protection of the data itself across your files and content, as well as structured and unstructured data wherever it resides

Orchestration & Automation

And finally, protection of the data itself across your files and content, as well as structured and unstructured data wherever it resides

Define Business Goals & Protect Surfaces

Module 1

The Objective: Align corporate objectives with surface protection.

Important Results Attained

A greater comprehension of how corporate objectives can be translated to important protect surfaces and their related SoCAS components.

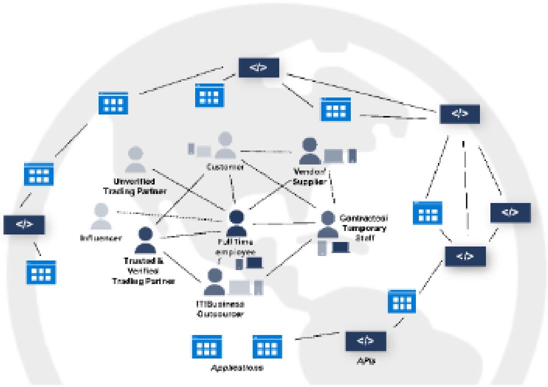
Activities\Outputs
Recognize the plans and strategies for business and IT. Establish business objectives.

Identify the five key protection surfaces and the SoCAS components that go with them. Chart business objectives and shield surfaces

Business objectives are mapped to critical protect surfaces and the SoCAS components that go with them.

SURAKSHA
INFORMATION SECURITY

Module 2 Begin Gap analysis



The Objective

Choose and specify zero-trust initiatives. Important Results Attained a roadmap with a prioritised list of zero trust objectives.

- Identity
- Location
- Application
- Device

Need to know basis

SURAKSHA INFORMATION SECURITY

Activities\Outputs

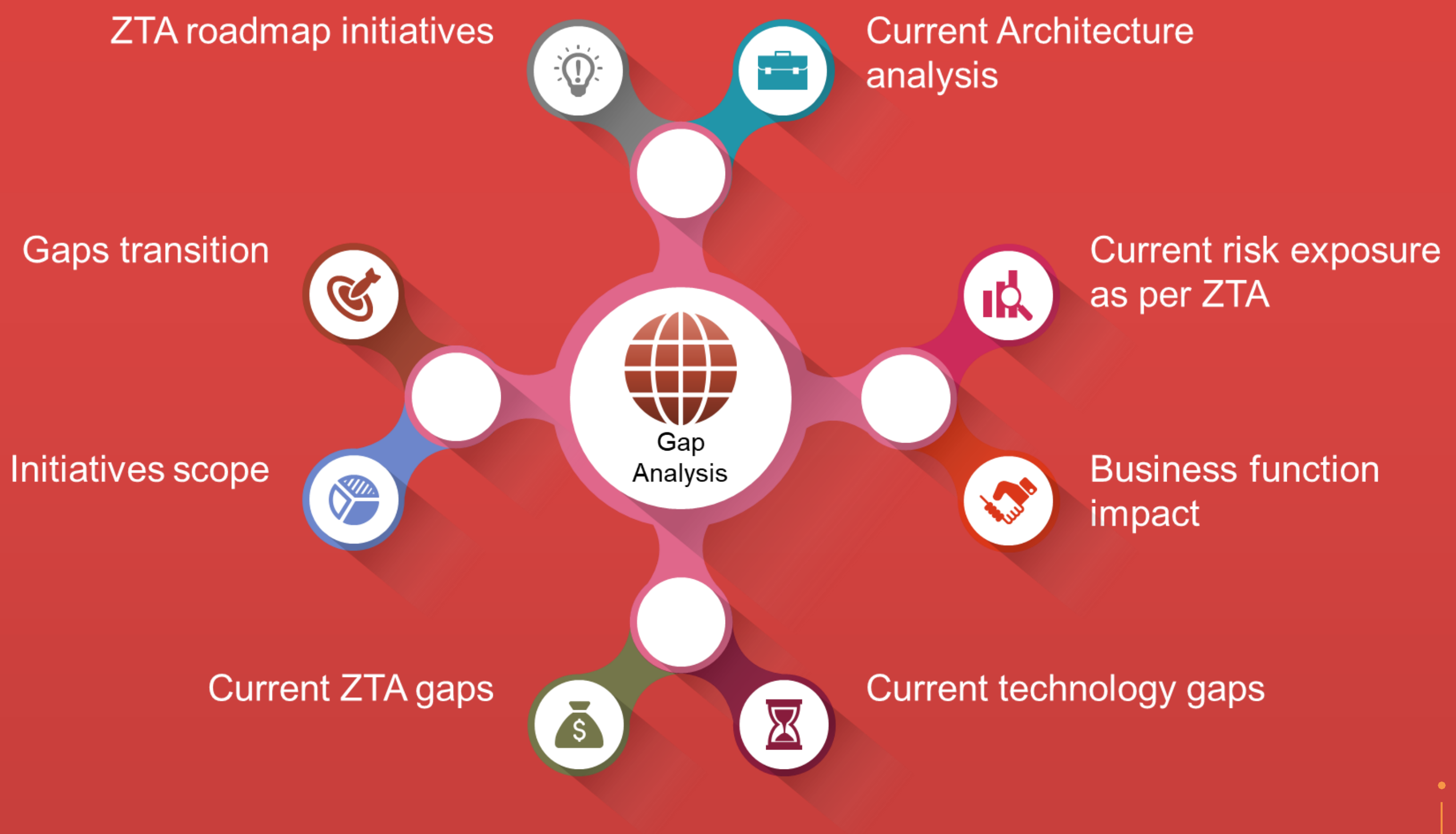
2.1 Determine the zero trust target state for a set of controls and evaluate the current security capabilities.

- Assessment of the existing status of security capabilities
- Target goal of zero trust

2.2 Choose actions to fill in maturity gaps.

- Activities to close maturity gaps

2.3 Assign duties to efforts promoting zero trust.



Gap analysis and ZTA transition steps

Module 2

A detailed gap analysis of all aspects of ZTA will be carried out for your organization with interactive participation.

A group session with peer participants will assist in determining the gaps.

A comprehensive gap analysis with ZTA based solution and roadmap elements to fill them will be developed.

Interactive workshops to develop gap analysis

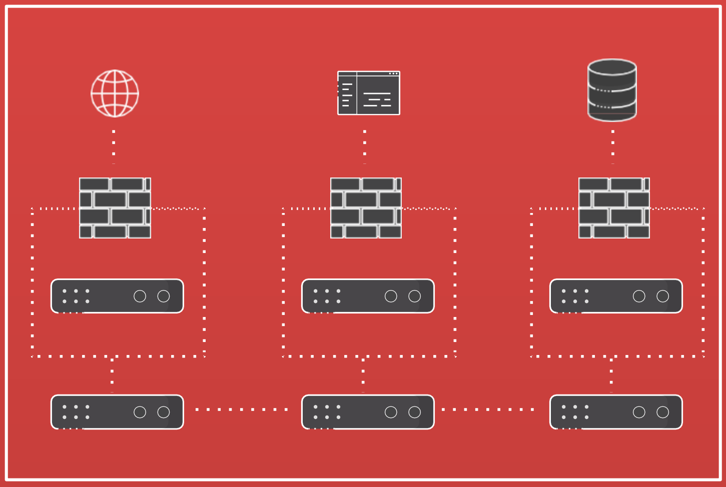
Zero Trust SOC and solutions protecting your organizations.

Transform to Zero Trust

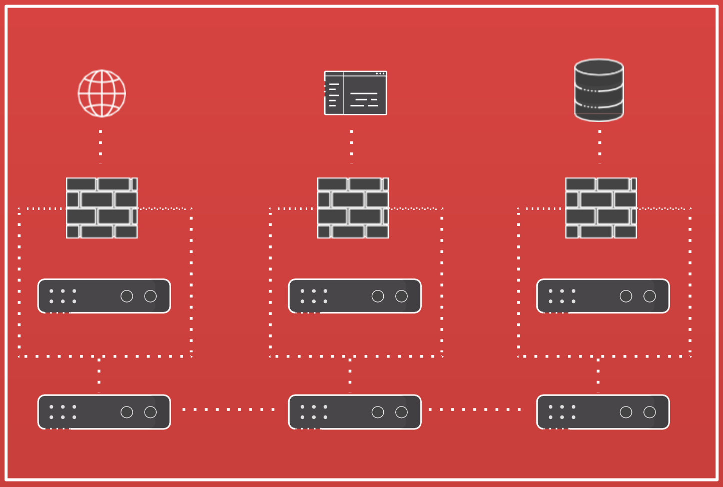
SURAKSHA INFORMATION SECURITY

Module 3 Complete Gap Analysis

Objective: Finish the study of the zero trust gap and set priorities for the zero trust activities

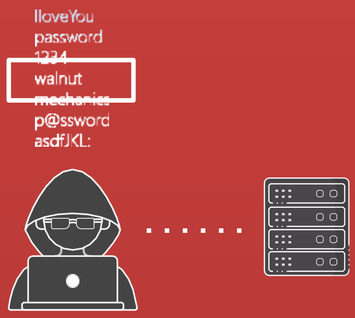


ZTA Lv1 & 2

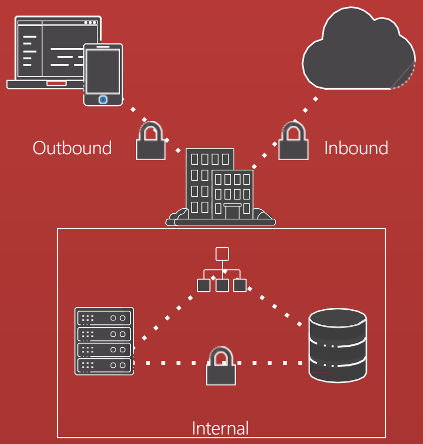


ZTA Lv 2-3

ZTA Lv 4



ZTA Lv 5



ZTA Lv 6-8

2 Important Results Attained
a prioritised list of zero trust projects that are in line with corporate objectives and important security points.

Activities\Outputs
3.1 Align initiatives with important safety surfaces and business objectives
- A zero trust initiative list that is aligned with company objectives and important defence points

3.2 Analyze the costs and benefits of zero-trust programmes.
3.3 Give initiatives a priority.
- Setting zero trust initiatives as a priority

SURAKSHA
INFORMATION SECURITY

The Objective

Complete the zero trust roadmap and start developing zero trust guidelines for roadmap projects.

Module 4 Finalize Roadmap & Formulate Policies

Important Results Attained

A roadmap with 0% trust for the most important projects.

ActivitiesOutputs

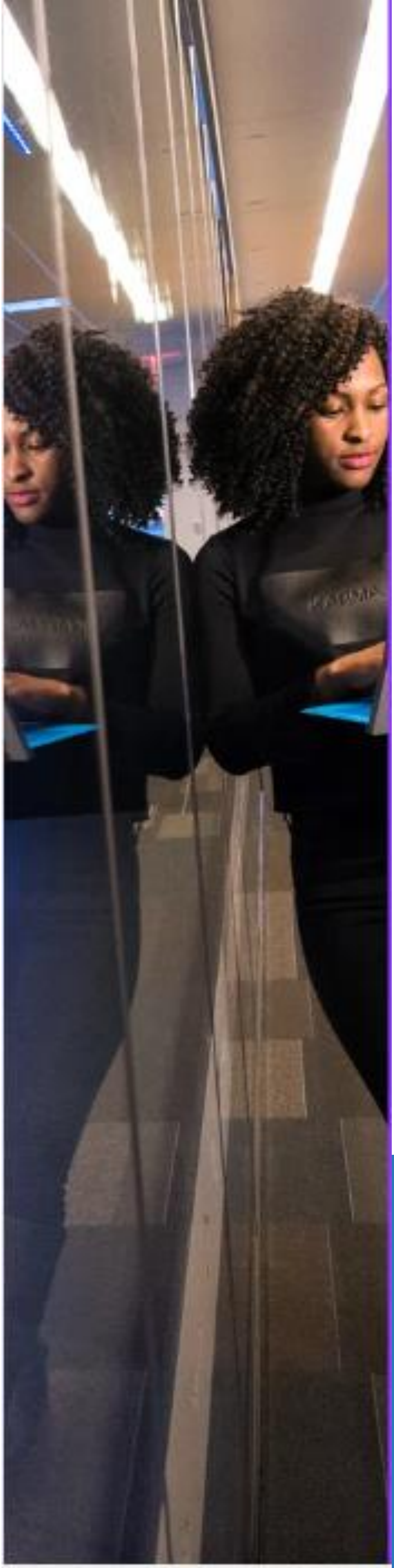
4.1 Define the criteria for the solution
4.2 Name potential answers.
4.3 Consider potential answers.
4.4 Complete the road map.

- Zero-trust strategyCreate policies for essential DAAS components
- Zero trust guidelines for crucial protection surfaces
- Technique for creating zero-trust guidelines for potential solutions

4.6 Create metrics for projects with high importance.

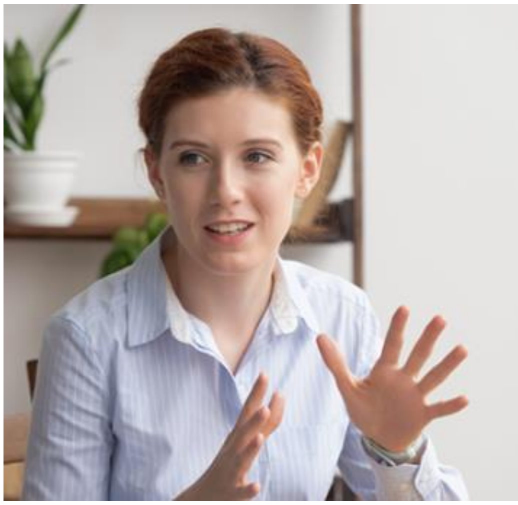
- High-priority initiative metrics

SURAKSHA INFORMATION SECURITY



KEY TAKE AWAYS

1. Customized ZTA road map
2. Draft business plan including
   - Initiatives
   - Budgets
   - Time table of implementation
   - Benefits
3. Workshop notes
4. Presentation copies
5. Customized Goals and objectives
6. Customized Gap analysis



Financial services
Banking
Insurance
Investment Houses

Health
Hospitals
Community centres
Field emergency

Critical Infrastructure
Electricity
Water
Airports
Infrastructure
Telecommunications

Government
Departments
Agencies
Statutory authorities

Defense
Airforce
Land force
Navy

Who:
CEO
CIO
CISO
IT MANAGERS
AUDIT
NETWORK ENGINEERS
SOC/NOC OPERATORS
BUSINESS MANAGERS
DATA CENTRE STAFF

zta@suraksha.com.au