- Enterprise -
Zero Trust Strategy & Journey Map

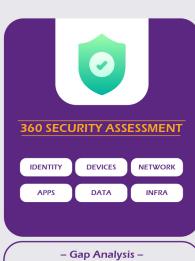| IDENTITY | DEVICES | NETWORK | APPS | DATA | INFRA |

John Keells IT has an established Zero Trust practice to provide Cloud Security services to local and international clients. We have helped organizations to commence the Zero Trust Strategy & Journey and have maintained Cloud Security Best Practices with them. By the year 2021, we were able to complete Zero Trust deployment, covering all six pillars (Identity, Endpoint, Network, Application, Data, Infra) for the largest listed conglomerate (Retail, transportation, Leisure, Finance and Insurance, Property, IT) company in Sri Lanka.

▶ OUR APPROACH   NOT JUST DEPLOY SIEM

Our holistic approach to Zero Trust will extend to your entire digital estate – inclusive of identities, endpoints, networks, data, apps, and infrastructure. Zero Trust architecture serves as a comprehensive end-to-end strategy that will provide you integration across all elements. To help your firm attain its intended Zero Trust state, John Keells IT will leverage the existing maturity to create a strategy and roadmap that includes planning, budgeting, prioritization, time management, and the implementation of strategic initiatives.
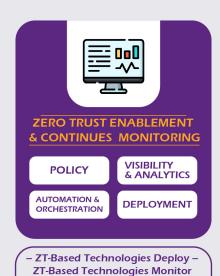
DISCOVERY & ADAPTATION SESSION/WORKSHOP

- Workforce/ Commitment
- Advisory Consultancy
- Awareness/Training

– Security Posture –
An on-site/Remote discovery workshop is conducted to gather information on the current security posture of your information security program and C-Level Cloud Security Advisory Consultancy & BCP&DR Advisory Consultancy.

360 SECURITY ASSESSMENT

| IDENTITY | DEVICES | NETWORK |
| APPS | DATA | INFRA |

– Gap Analysis –
Information discovered within each of the 6 pillars are used to analyze the organization's alignment with the Zero Trust.

MATURITY MODEL

| IDENTITY | DEVICES | NETWORK |
| APPS | DATA | INFRA |

– Incorporate Practices –
A maturity assessment is conducted on the organization's capabilities within each of the pillars, as well as the overall security program, to understand required changes necessary to align with Zero Trust.

ZERO TRUST JOURNEY MAP

- ARCHITECT
- WBS/PLAN
- INTEROPERABILITY

– Roadmap –
To help your firm attain its intended Zero Trust state, JKIT will leverage the existing maturity to create a strategy and roadmap that includes planning, budgeting, prioritization, time management, and the implementation of strategic initiatives.

ZERO TRUST ENABLEMENT & CONTINUES MONITORING

- POLICY
- VISIBILITY & ANALYTICS
- AUTOMATION & ORCHESTRATION
- DEPLOYMENT

– ZT-Based Technologies Deploy –
ZT-Based Technologies Monitor
Zero Trust execution integrates with Department-level and Component-level processes resulting in seamless and coordinated ZT execution initiatives.

STRATEGIC OUTCOMES

- ▶ The ability of a user to access required data from anywhere, from any authorized and authenticated user and device, fully secured
- ▶ Secured and protected information systems facilitating the Department's evolution into a more agile, more mobile, cloud-supported workforce
- ▶ Reduced attack surface risk profiles through protective actions enabled by micro segmentation of the Enterprise network
- ▶ Threats to Cloud, Artificial Intelligence (AI), Command, Control, Communications, Computers, and Intelligence remediated through risk-based cybersecurity protocols and policies
- ▶ Effective damage containment, mitigation, and remediation when a device, network, user, or credential is compromised
- ▶ Consistent, aligned, and effectively resourced ZT capabilities for advanced cybersecurity operations
- ▶ A resilient Enterprise that recovers rapidly from attacks and minimizes damage through enablement of ZT

✉ info@johnkeellsit.com   📞 +94.11.2318319   🌐 www.johnkeellsit.com