Deloitte.

The need for Zero Trust is **NOW**

In this era of evolving business models, shifting workforce dynamics, and dynamic technology trends, many organizations are prioritizing the adoption of the **Zero Trust** model.

---

**Zero Trust is a conceptual framework that helps organizations secure the ubiquitous nature of modern enterprise environments.**

At its core, Zero Trust commits to a risk-based approach to enforcing ‘least privilege’ across users, networks, data, devices, and workloads.

---

Business drivers accelerating the need for Zero Trust

**COMPLEX IT ENVIRONMENTS**
The increasingly global vendor landscape creates complexities as companies manage risks across a wide range of information and operational technology environments and expand to emerging markets / higher risk geographies.

**EMPHASIS ON BRAND AND REPUTATIONAL CONCERNS**
Damage to an organization’s brand can cause as much financial setback as regulatory fines. The effort and cost of regaining customer trust and dealing with regulatory impacts after an incident can be mitigated with proactive measures.

**INCREASED OUTSOURCING OF “CORE” SERVICES**
Organizations are continuing to expand not only the amount of business operations that are outsourced, but also activities that are considered critical services, in an effort to achieve desired efficiencies and flexibility—including cybersecurity services.

---

**INCREASED NEED FOR WORKFORCE MOBILITY AND FLEXIBILITY**
Many businesses are moving to remote and virtual working models, increasing the need for transparent and strong approaches to identify, manage, and reduce risk.

**PUSH TOWARDS DIGITAL TRANSFORMATION**
Increased use of emerging technologies, such as cloud and machine learning, increase the surface area for potential vulnerabilities and the need to keep security at the heart of modernization.

**INCREASED SCALE, COMPLEXITY, AND FREQUENCY OF CYBERATTACKS**
Data breaches are often a top concern for executives who worry about the security of highly confidential information. Increasingly, cybersecurity and cyber resilience are two of the top trending topics on board agendas.

---

Deloitte can help enable clients to overcome these challenges by providing **objective perspectives** on how to leverage existing and planned technology spend to align to the Zero Trust framework. Taking an iterative and use case-driven approach that is tied to business objectives leads to greater success in the adoption journey and concurrence from relevant stakeholders.

Guiding principles define our vision across each pillar of the Zero Trust framework and our vast ecosystem and alliance relationships enable us to recommend best-of-breed approaches for our clients.

Deloitte offers Zero Trust services across the following engagement models:
- Assess
- Strategize
- Architect
- Implement
- Manage / Operate
Deloitte’s Zero Trust framework

A Zero Trust model is built upon strong foundational capabilities across five fundamental pillars: users, workloads, data, networks, and devices. Data protection is the goal and is represented centrally in our framework. Organizations should have an understanding of what data exists, the classification and criticality of that data, who and what should be able to access that data, the mechanisms by which that data should be accessed, and the appropriate security controls to protect it – both at rest and in transit.

**PROGRAM GOVERNANCE**
- IT service management
- Policies and standards
- Business drivers
- Regulatory requirements

**TELEMETRY & ANALYTICS**

**AUTOMATION & ORCHESTRATION**

**USERS**

**WORKLOADS**

**DATA**

**NETWORKS**

**DEVICES**

**GUIDING PRINCIPLES**

**FOCUS ON THE FUNDAMENTALS**
Foundational cyber hygiene is crucial to the successful adoption of a Zero Trust framework (e.g., IT asset management, data inventory, patch and configuration management).

**PRIORITIZE BUSINESS NEEDS OVER TECHNOLOGY**
Adopt Zero Trust through relevant business drivers and areas of transformation, rather than focusing on technology implementation and adoption.

**CENTRALIZE AND FEDERATE IDENTITY SERVICES**
Centralize identity governance, authentication, and authorization services to help enforce granular, real-time, least privilege principles for access to networks, systems, workloads, and data.

**MINIMIZE DISRUPTION BY STARTING WITH LOW RISK TARGETS OR ENVIRONMENTS**
Take an incremental approach to Zero Trust adoption. Fundamental changes to security controls, processes, and technologies can be disruptive; start with a low risk environment before attempting to apply Zero Trust to your crown jewels.

**GAIN CONSENSUS**
The Zero Trust journey can be long and complex. It typically involves multiple stakeholders and parts of the business. It’s important to gain consensus from relevant parties before embarking on the journey.

**ESTABLISH ASSET, USER, AND DATA INVENTORIES**
Mature system, application, identity, and data inventories are necessary to support foundational capabilities such as asset management, data classification and tagging, and identity governance.

**DEFINE POLICIES AND STANDARDS**
Well-defined policies and standards provide consistent guidance, facilitate compliance, and streamline the Zero Trust journey in alignment with the organization’s risk tolerance.

**MINIMIZE DISRUPTION BY STARTING WITH LOW RISK TARGETS OR ENVIRONMENTS**
Take an incremental approach to Zero Trust adoption. Fundamental changes to security controls, processes, and technologies can be disruptive; start with a low risk environment before attempting to apply Zero Trust to your crown jewels.

**INTEGRATE ACROSS THE TECHNOLOGY ECOSYSTEM**
Provide integration and application programming interface (API) support across the technology ecosystem to enable automation and orchestration capabilities across the Zero Trust pillars.

Kieran Norton
Principal | Deloitte Risk & Financial Advisory | Cyber & Strategic Risk
Deloitte & Touche LLP
Tel/Direct: +1 415 302 2027
kinorton@deloitte.com | www.deloitte.com

Andrew Rafla
Principal | Deloitte Risk & Financial Advisory | Cyber & Strategic Risk
Deloitte & Touche LLP
Tel/Direct: +1 201 499 0580
arafla@deloitte.com | www.deloitte.com

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, ‘Deloitte’ means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2020 Deloitte Development LLC. All rights reserved.