Zero Trust Journey

The New Business Security Lifestyle

Who invented the term?

2010

In 2010, then Forrester Principal Analyst John Kindervag coined the term “Zero Trust”

John Kindervag

FORRESTER®

“A new model that allows us to build security into the DNA of the network itself.”

NETWORK

1 Read >

2023

Zero Trust Today

Deloitte.

2 Read >

Definition

It's not one solution, but a set of controls and design principles guiding decision-making in security architecture.

Breach

The concept of Zero Trust is to always treat your infrastructure as if it's breached.

No Trust

It assumes that no user, workload, device or network can be inherently trusted.

Key Drivers

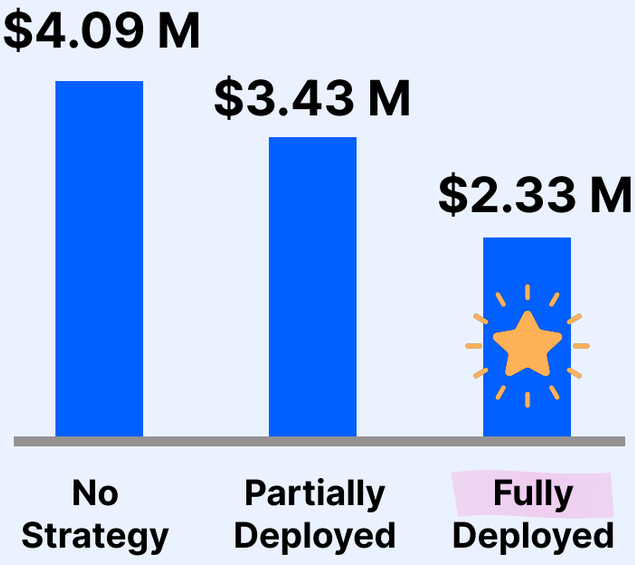
More Cloud Apps

Geopolitical Tention

Remote Workforce

Sophistication of Attacks

Zero Trust Value



IBM Security

Average Cost of a Breach

3 Read >

4 Zero Trust Areas

4 Read >

Users

Identify & Verify Users with Identity Provider (IDP) & MFA Solutions

IDP
MFA
Need To Know Basis
Least Privilege

Software

Vendor Risk Management & Restricted Cloud/ Local Apps

DLP
Data Exfiltration
Approved Vendors

Logs

SIEM Security Incident & Event Management

Log Retention

Endpoints

Endpoint Protection & Validation of Compliance at Login

MXDR
Unknow Devices
DLP

Networks

Local Network & Remote/Home Communication Security

Software Defined Perimeter
Gateway VPN

Steps to Zero Trust

1. Understand Zero Trust in your organization
2. Identify areas for Zero Trust implementation
3. Develop implementation plan and gap analysis
4. Select solutions, train, and implement
5. Learn, improve, and celebrate!

CNBC

Regardless of the approach, it seems that Zero Trust as a cybersecurity approach is here for the long haul.

5 Read >

Summary

GSA

A Company-Wide Initiative

- All resources must be accessed in a secure manner.
- Access controls should be on a need-to-know basis.
- Do not trust people, verify who they are and what they are doing.
- Inspect all log traffic coming in on the network for malicious activity.
- Design networks from the inside out.
- Create policies to enforce zero trust which ultimately align with regulatory compliance.
- Educate and train employees, boards, vendors and extended networks.

6 Read >

Source

1. Dark Reading, Forrester Pushes 'Zero Trust' Model For Security, September 2010
https://www.darkreading.com/perimeter/forrester-pushes-zero-trust-model-for-security

2. Deloitte, Article: Zero Trust – never trust, always verify, 2021
https://www2.deloitte.com/nl/nl/pages/financial-services/articles/zero-trust-never-trust-always-verify-tech-trends-banking.html

3. IBM, Cost of a Data Breach Report 2021
https://www.ibm.com/downloads/cas/OJDVQGRY

4. FCI Identify & Zero Trust Solutions, 2022
https://fcicyber.com/identify/

5. CNBC, Why companies are moving to a 'zero trust' model of cyber security, March 2022
https://www.cnbc.com/2022/03/01/why-companies-are-moving-to-a-zero-trust-model-of-cyber-security-.html#:~:text=Research%20firm%20Markets%20and%20Markets,data%20protection%20and%20information%20security

6. GSA, Zero Trust Architecture (Zerto Trust Buyer's Guide), June 2021
https://www.gsa.gov/cdnstatic/Zero%20Trust%20Architecture%20Buyers%20Guide%20v11%2020210610%20(2).pdf

FCI

888 434 6443
www.fcicyber.com
info@fcicyber.com