DLT
A TECH DATA COMPANY

Boost Security with Zero Trust in 2021

Why Zero Trust?

Widespread breaches by hostile actors, the rising number of remote employees and bring-your-own-device (BYOD), the growth of software as a service (SaaS), and cloud migration have rendered perimeter-based security obsolete. The Zero Trust approach to cybersecurity — now mandated by a Presidential Executive Order — is growing rapidly in the public sector. Zero Trust shifts security away from the perimeter, and closer to an organization's most valuable assets.

60%
of enterprises accelerated their Zero Trust networking strategies due to the **pandemic** (Gartner).

275%
year-over-year **growth** in the number of North American organizations that have or plan to have a defined zero trust initiative on the books in the next 12-18 months (Gartner).

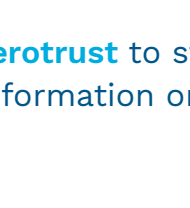
60%
of organizations in North America are **currently working** on zero trust projects (Enterprise Management Associates (EMA)).

Seven Challenges Zero Trust Solves

Network Architecture, Monitoring, Access Control

76% of enterprises have seen an increase in the number of personally owned devices connecting to their networks during the pandemic, with 33% characterizing this increase as significant (EMA).
A new network architecture would provide monitoring and access control.

Automated Response



61% of enterprises reported that pandemic-related changes to their businesses have directly led to an increase in security issues (EMA). This increased rate of cyber incidents has led to greater need for automated response.

Threat Intelligence

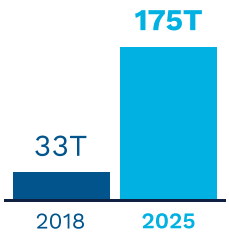
70% of organizations get their threat intelligence feeds from specific threat intelligence vendors. About the same number say that threat intelligence information is integrated into their defense and response systems via threat intelligence platforms.

Visibility

59% In a 2020 SANS survey of Network Visibility and Threat Detection, **59%** of respondents rated the risk posed by a **lack of visibility into devices** on their networks as High or Very High.

30% of respondents ranked **identifying unknown or unauthorized devices** as a top security challenge.

Data Protection

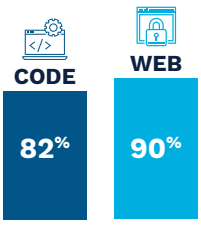


The collective sum of global data is predicted to grow from **33 trillion** gigabytes in 2018 to **175 trillion** gigabytes in 2025 (International Data Corporation (IDC)/Seagate).

Identity and Access Management

71% of those with Zero Trust initiatives reported that they had increased the security requirements of their network-access policies during the pandemic (EMA).

Application Security



82% of known vulnerabilities are in application code, with **90%** of web applications vulnerable to hacking (Positive Technologies).

Sponsored by:

aws FIREMON IBM

DLT
A TECH DATA COMPANY

Visit **dlt.com/zerotrust** to stay updated on the latest information on Zero Trust.