CROWDSTRIKE

Accelerate Your Zero Trust Security Journey

Zero Trust is not a one-stop solution. It's a journey that should cover the important entities - your endpoints, identities and workloads, to maximize protection. The Zero Trust strategy should reduce security complexity, improve user experience, and also scale up as your business grows.

The following highlights the results from the July 2021 TechValidate survey of CrowdStrike customers and poll results from participants in CrowdStrike Zero Trust webinars in the same period.

What are the most worrisome threats?

Over 80% consider ransomware as the most worrisome threat

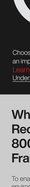
Over 50% are very concerned about Active Directory (AD) threats - AD hygiene and AD vulnerabilities

With traditional approaches and siloed security tools, accomplishing Zero Trust security to stop ransomware and modern attacks can be hard.

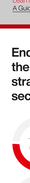
Where are organizations in their Zero Trust journey

90% are in the Zero Trust security journey - **57%** in planning phase and **33%** in implementation phase.

What aspects influence the Zero Trust decision making process for organizations?



On an average, over 80% consider **identity protection** - i.e. behavior, segmentation/ least privileges, as the most important aspect in Zero Trust to limit the attack surface



66% consider **"least friction"** continuous verification is a very important aspect in Zero Trust

45% consider **attack path visibility** across endpoints, identity stores, workloads and containers very important to accomplish Zero Trust

According to Forrester[1], **80%** of the attacks are from compromised credentials. The 2021 Cost of Data Breach report[2] highlights that **compromised credentials** caused the most breaches.

1 The Forrester Wave™: Privileged Identity Management Q4 2018
2 Cost of a Data Breach Report 2021

Which Zero Trust Framework is the most preferred?

- 50% of the organizations are undecided about the Zero Trust framework
- 35% are adopting the NIST 800-207 framework
- 10% considering Gartner's CARTA framework
- 5% considering the Forrester ZTX framework

Choosing the right Zero Trust framework is an important first step in the journey.

Learn more:
Understanding the United States' Zero Trust Mandate

Why CrowdStrike Recommends the NIST 800-207 Zero Trust Framework

To enable security in the cloud-first, work-from-anywhere environment, the CrowdStrike Zero Trust solution most closely follows the NIST 800-207 framework, widely adopted in the public and private sectors.

Key principles of the NIST Zero Trust framework:

- Understand Behavioral Data
- Limit the Attack Surface With Segmentation
- Automate Security Tied to Context
- Continuously Verify Access With the Least Friction

Learn more:
A Guide to Frictionless Zero Trust for Modern Enterprises

Endpoints and identities are the top focus areas when strategizing the Zero Trust security initiative

Endpoints - including managed and unmanaged

Workforce identities, including human and service accounts, across multi-directory identity stores

38% consider on-premises and cloud workloads the most important focus area

35% consider container security the most important focus area

Learn more:
Modern attacks, like ransomware or supply chain attacks, don't typically follow the cyber kill chain in a linear manner

Reducing security complexity is one of the most important success metrics in operationalizing Zero Trust security

Reduce security complexity

Improve mean time to detect and respond for security teams

Enhance user experience

Learn more:
Frost & Sullivan White Paper: ROI Strategies with Frictionless Zero Trust

Accelerate your Zero Trust Security Journey with CrowdStrike

- **Reduce security complexity** - unified management console for maximum coverage across endpoints, identities, workloads and containers
- **Adopt the widely accepted NIST 800-207 Zero Trust framework for your cloud-first, work from anywhere environment**
- **Improve deployment speed and alert fidelity with CrowdStrike's 100% cloud-native approach**

© 2021 crowdstrike.com. All rights reserved.

Learn more: www.crowdstrike.com/zero-trust