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

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

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

- Endpoints and identities are the top focus areas when strategizing the Zero Trust security initiative
- Over 80% consider identity protection—i.e. behavior, segmentation/least privileges, as the most important aspect in Zero Trust to limit the attack surface

Why CrowdStrike Recommends the NIST 800-207 Zero Trust Framework

- Reducing security complexity is one of the most important success metrics in operationalizing Zero Trust security
- The NIST 800-207 framework closely follows the key principles of Zero Trust

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.
- 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

Which Zero Trust Framework is the most preferred?

- 66% consider ’least friction’ continuous verification as 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

Over 80% of the attacks are from compromised credentials. The 2021 Cost of Data Breach report highlights that compromised credentials caused the most breaches.

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