ICE
TRUSTED IT PARTNER

ICE's Ultimate Guide to

EMBRACING A ZERO TRUST SECURITY MODEL

Embracing the Zero Trust Security Model

In the ever-evolving world of cybersecurity, a remarkable transformation has taken place. Traditional strategies relied upon by CISOs have been shaken up by two monumental events: COVID-19 and the SolarWinds attacks. The days of fortifying perimeters and building moats around castles are gone. Our rapidly changing landscape demands a more adaptable and comprehensive approach.

With the rapid adoption of cloud technologies, remote workforces, and the ubiquity of mobile devices, the attack surface has expanded beyond traditional boundaries. It's time to embrace a new mindset, a zero trust security strategy. In this guide, we'll explore the forces driving this necessity and dive deep into its implementation.
Are you ready to pivot towards a more proactive and secure digital future? Stay tuned as we embark on this crucial journey together.

The rise of remote work is compelling organizations to stay up-to-date with the changing times.

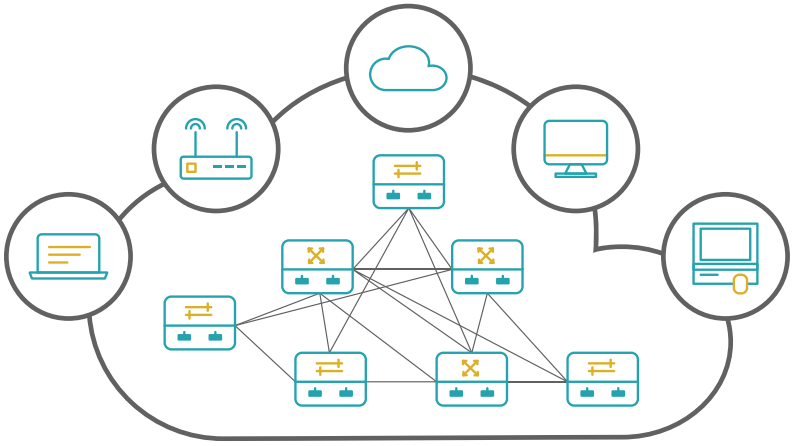
Since the COVID-19 pandemic began, the world has gone through significant changes. It's been a real wake-up call for organizations to speed up their transformation efforts. Suddenly, employees had to switch to remote work, which put a lot of strain on IT and security infrastructure. While virtual private networks (VPNs) were the norm for remote access, the sudden surge in workload and traffic made scalability a major challenge within a short timeframe.

This sudden shift also exposed organizations to new security threats. Legacy tools that relied on a "defense-in-depth" approach, with a strong enterprise perimeter, turned out to be insufficient during the pandemic. Once a threat found a way into the network, hackers had a field day exploiting vulnerabilities and gaining unauthorized access throughout the organization's systems, causing all sorts of damage.

With the migration to the cloud, user access now goes beyond the traditional boundaries, which presents visibility, control, and data security challenges. Given the ever-evolving threat landscape, organizations need to operate under the assumption that they've already been compromised and take appropriate measures to protect themselves. In this new security paradigm, every user, device, and service trying to access the organization's network is seen as a potential threat, regardless of their known status. Plus, it's crucial to recognize that not all data holds the same value. Effective security measures should consider the sensitivity and importance of different assets, especially when traditional boundaries dissolve and data traverses the organization.

Just moving to the cloud or updating infrastructure won't guarantee the desired outcomes if these issues aren't addressed. Companies must prioritize protecting their assets and fully embrace the potential benefits that technological advancements offer. To thrive in the era of remote work and beyond, organizations need a modern approach that goes beyond the old-fashioned perimeter-based security strategies.

TRADITIONAL NETWORK



Introducing a revolutionary security approach: Place your trust in no one.

By implementing a comprehensive system that considers all factors, including user, device, and resource, agencies can effectively minimize enterprise risk in a dynamic manner. Embracing a zero trust approach becomes crucial for continuously evaluating, adapting to changing conditions, and mitigating threats.

According to a recent Forrester Report, organizations must adopt the mindset of assuming they have already been compromised, even if they are unaware. This means moving away from the traditional "trust but verify" approach that often leads to crisis management. While zero trust may seem radical, it is a proactive and strategic architectural approach that aligns with the goal of enhancing security. Together, we can create a safer digital environment.