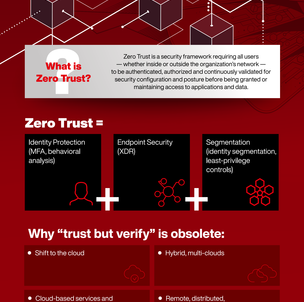
CROWDSTRIKE

Frictionless Zero Trust

“Never trust, always verify”

The traditional **“trust but verify”** method of protection, which automatically allows trusted users and endpoints to access the network, puts the organization at risk from a wide array of security threats.

To improve the security posture, organizations are turning to a **Zero Trust** security model. This approach enables the organization to continuously monitor and validate which users and devices are authorized to access applications and other resources, regardless of endpoint or network location.



What is Zero Trust?

Zero Trust is a security framework requiring all users — whether inside or outside the organization’s network — to be authenticated, authorized and continuously validated for security configuration and posture before being granted or maintaining access to applications and data.

Zero Trust =

- Identity Protection (MFA, behavioral analysis)
- \+ Endpoint Security (XDR)
- \+ Segmentation (identity segmentation, least-privilege controls)

Why “trust but verify” is obsolete:

- Shift to the cloud
- Hybrid, multi-clouds
- Cloud-based services and software-as-a-service (SaaS) applications
- Remote, distributed, global workforce
- Explosion of endpoints and connected devices
- User experience

90% of organizations have not completed their Zero Trust journey

33% in implementation phase

57% in planning phase

Source: July 2021 TechValidate survey of CrowdStrike customers and CrowdStrike Zero Trust webinars

In Pursuit of Zero Trust

5 Best Practices for Implementing a Frictionless Zero Trust Model

1: USE INDUSTRY DEFINITIONS

Vendors will come and go. Threats will change. But the core of the organization’s Zero Trust framework and its measurement of success should remain consistent yet flexible.

By that we mean that the framework must be capable of scaling to meet new needs and incorporating legacy systems and tools, while also minimizing both cost and complexity.

The National Institute of Standards and Technology’s Special Publication 800-207 (NIST SP 800-207) is the industry standard for establishing a Zero Trust framework that meets the needs of a cloud-first, work-from-anywhere world.

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

2: FOCUS ON FRICTIONLESS

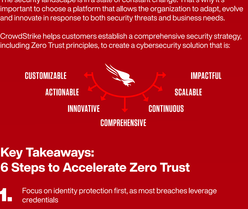
To ensure strong adoption — and, by extension, positive impact — the journey to Zero Trust must be efficient and easy to use for everyone including end users, IT and security personnel. In a word, Zero Trust must be *frictionless*.

How to go frictionless:

- Implement in stages to build maturity, justify costs and reduce complexity
- Leverage dynamic analytics to implement risk-based conditional access/MFA

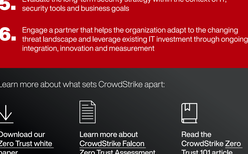
3: FOCUS ON THE JOURNEY, NOT THE SPRINT

Zero Trust is not a one-stop solution for enterprises but a set of principles that aims to move security closer to the resources that are being protected. Organizations must understand that the changes within the threat landscape mean that their security journey will also be an ongoing, iterative, adaptive process — though it should not require re-architecting the network.



4: EMBRACE THE CLOUD

Just as businesses leverage the cloud to reduce the cost and complexity of various transformation initiatives, so too can they rely on the cloud to simplify some aspects of the deployment, management, optimization and adoption of a Zero Trust security model.



5: CHOOSE PLATFORMS, NOT VENDORS

The security landscape is in a state of constant change. That’s why it’s important to choose a platform that allows the organization to adapt, evolve and innovate in response to both security threats and business needs.

CrowdStrike helps customers establish a comprehensive security strategy, including Zero Trust principles, to create a cybersecurity solution that is:

Key Takeaways: 6 Steps to Accelerate Zero Trust

1. Focus on identity protection first, as most breaches leverage credentials
2. Employ preventative techniques to protect identities, endpoints and application accesses
3. Enable real-time monitoring and policy controls to identify and halt malicious activity
4. Deploy cloud-native security to reduce security and management complexity
5. Evaluate the long-term security strategy within the context of IT, security tools and business goals
6. Engage a partner that helps the organization adapt to the changing threat landscape and leverage existing IT investment through ongoing integration, innovation and measurement

Learn more about what sets CrowdStrike apart:

Download our Zero Trust white paper

Learn more about CrowdStrike Falcon Zero Trust Assessment

Read the CrowdStrike Zero Trust 101 article

About CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world’s most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us:

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**