KEEPER®

How to Implement Zero Trust in Your Organization

Introduction

The COVID-19 pandemic upended traditional perimeter-based network security models as organizations of all sizes scrambled to enable armies of remote workers. Prior to COVID-19, only about 6% of employees worked primarily from home; in the immediate aftermath of the pandemic lockdowns, this skyrocketed to 29%. Among professional occupations (including education, computer and mathematical, and legal occupations), 75% of employees were sent home to work.[1]

Meanwhile, the cyberthreat environment kept growing increasingly dangerous. Lone-wolf cybercriminals, cybercrime cartels and nation-state threat actors are more skilled, covert, persistent and financed than ever before, which has radically increased both the number of attacks and successful network intrusions.

Zero trust is the only realistic framework for securing modern, cloud-based data environments and distributed workforces. Yet a recent study by CRA Business Intelligence found that only about 35% of security professionals are familiar with zero trust, and about the same percentage say they've implemented it at their organizations. However, nearly half say they plan to implement it within the next 12 months.[2]

Keeper Security has put together this guide to cut through the noise, clear up confusion and misconceptions surrounding zero trust, explain its core principles and help organizations plan successful zero trust implementations.

[1] NCCI [2] SC Media

What Is Zero Trust?

Zero trust is an "assumed breach" security model created for cybersecurity solution architects, system integrators and DevOps teams to integrate essential cybersecurity capabilities into a pervasive IT environment that empowers cybersecurity planning and decision-making.

Before: Trust Everyone Inside the Network Perimeter

Historically, organizations used a "castle and moat" model to ensure network security. All users and equipment located inside the network perimeter were trusted by default, which meant that they didn't need to be authenticated before accessing organizational resources. Only users and devices located outside of the network perimeter were required to authenticate. This was a logical framework when virtually all employees and equipment were located within the confines of an office building – ensuring a clearly defined network perimeter.

Even prior to the COVID-19 pandemic, cloud computing and mobility were chipping away at the concept of a "network perimeter." The aftermath of pandemic lockdown orders destroyed it completely. To enable all of their newly remote employees, organizations were forced to accelerate their digital transformation plans by months or years. Businesses rapidly migrated to cloud-based environments (most multi-cloud or hybrid) so that their employees could access work resources from anywhere. This meant that the number of endpoints, websites, systems, databases and applications requiring authentication and end-to-end encryption multiplied exponentially.

IT administrators attempted to shoehorn disparate solutions built for homogenous, on-prem infrastructures into heterogeneous, cloud-based environments, but they found it impossible to achieve comprehensive visibility, security and control of networks and endpoints. The castle-and-moat model crumbled, and cyberattacks soared as threat actors took advantage of organizations' insufficient security defenses.

Today: Trust No One

In contrast to the castle-and-moat model, zero trust does not trust any human users or devices, regardless of where they are located. In a zero-trust environment, all users and devices must be authenticated before they can access organizational resources. Instead of **relying** on **where** users are, zero trust makes them **prove who** they are.

Implemented properly, zero-trust network access provides IT administrators with full visibility into all users, systems and devices. People, apps and services can communicate securely, even across network environments. It doesn't matter if users are connecting from their homes, hotels, coffee shops or airports, or even if they're using their own devices. Administrators can see exactly who's connecting to the network, from where and what they're accessing – and users can't get in at all until they've explicitly proven they are who they claim to be.

Three guiding principles form the core of zero-trust security:

1. **Assume Breach**. Any human or device could potentially be compromised, even if they're connecting from inside the office, which is why the second guiding principle says to…

2. **Verify Explicitly.** All humans and machines must prove that they are who they say they are before they can access network resources. And that's not all…

3. **Ensure Least-Privilege.** Even once a user has been verified explicitly, they should have only the minimum amount of network access they need to perform their jobs and not one iota more.

The 6 Pillars of Zero-Trust Security

Microsoft recommends planning your zero-trust implementation around the following six pillars, all of which must be assessed, then updated or replaced accordingly.[3]

Identity

In a zero-trust model, every user, both human and machine, must have a unique digital identity. Whenever this identity requests access to a resource, the system must verify it with strong authentication, backed up with behavioral analysis to ensure that the access request isn't anomalous for that user. Once the identity is authenticated, its network access must follow least-privilege principles.

To achieve this, ensure that all of your users are using strong, unique passwords for every account and enabling multi-factor authentication (MFA) wherever it is supported. Additionally, deploy real-time detection, automated remediation and connected intelligence solutions to monitor for account compromise and respond to potential problems.

Endpoints

Only compliant and trusted apps and devices should be permitted to access data. Before allowing employees to access company apps on mobile devices, require them to enroll their devices in mobile device management (MDM) and have them validated for general health and compliance with company security policies. MDM solutions also give administrators visibility into device health and compliance and the ability to enforce policies and security controls, such as blocking copy/paste or download/transfer.

Data

In today's cloud-based environments, data resides everywhere, and it must be governed everywhere it resides. This involves strictly controlling and restricting data access according to least-privilege principles and ensuring that data is encrypted both at rest and in transit.

Applications

Application access and privileges must be controlled and restricted as rigorously as data. Gate access to apps, monitor app usage for anomalous behavior and use role-based access control (RBAC) to ensure that users' in-app permissions are appropriate and follow least-privilege principles.

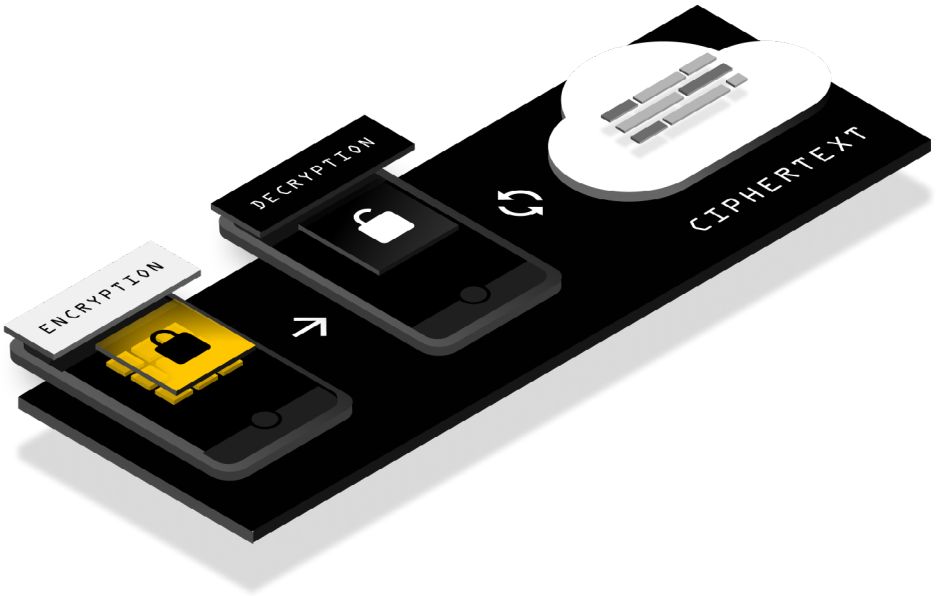
Infrastructure

Managing permissions for both on-prem infrastructure and cloud-based VMs, containers and microservices can be challenging. Automate as many processes as possible. Use just-in-time (JIT) access to harden defenses, deploy security analytics to detect anomalies and attacks and automatically block and flag risky behavior for further investigation and remediation.

Network

Segment networks to prevent threat actors from moving laterally and accessing sensitive resources. Utilize "in-pipe" network security controls to enhance visibility, including tools for real-time threat protection, end-to-end encryption, monitoring and analytics.

[3] Microsoft



Best Practices for Deploying a Zero-Trust Architecture

One of the biggest challenges to implementing zero trust is knowing where to begin. Zero trust has a lot of moving parts, and there are no universal "zero-trust implementation" standards. Here are a few best practices for mapping out your organization's zero-trust journey.

Realize that zero trust is a long-term commitment, not a one-time fix. As technology, workflows and the threat environment all shift and change, so will your zero-trust architecture.

Make sure you have buy-in from upper management. Zero trust requires an "all or nothing" mindset and firm commitment by all levels of leadership and teams. Support from upper management was a commonality among CRA's "champions" – while a lack of support was the top stumbling block cited by organizations continuing to struggle with adopting zero trust.[4]

Start small. To avoid business disruptions, NIST recommends starting a zero-trust deployment by first migrating low-risk business resources, then segueing to more critical resources after your team has more experience with zero trust.[5]

When in doubt, focus on IAM first and foremost. Among CRA's zero-trust "champions," Identity and Access Management (IAM) was the most frequently implemented component of zero-trust, with 86% having applied zero-trust strategies to their IAM processes and controls.[6]

[4,5,6] Ibid

Best Practices for Choosing Zero-Trust Solutions

Some people call zero trust a paradigm, while others call it a philosophy, a framework, a model or even a movement. Whatever it's called, the takeaway is that the end goal of zero trust is not to deploy specific products but to achieve desired outcomes. In this respect, zero trust is to cybersecurity what DevOps is to software development: a fundamental shift in how organizations approach security.

There are many zero-trust-compatible solutions on the market, but not all of them are suitable for your specific data environment and business needs. NIST[7] recommends taking the following into consideration when choosing zero-trust tools:

- **Does the solution require that components be installed on the client asset?** Client-side solutions could limit business processes and impede productivity. They also create additional administrative overhead for your IT team.

- **Does the solution work in cases where business process resources exist on premises?** Some solutions assume that requested resources reside in the cloud (so-called north-south traffic) and not within an enterprise perimeter (east-west traffic). This poses a problem in hybrid cloud environments, where legacy line-of-business apps that perform critical functions may be run on-premises because migrating them to the cloud isn't feasible.

- **Does the solution provide a means to log interactions for analysis?** Zero-trust access decisions depend heavily on the collection and use of data related to process flow – especially for privileged access accounts.

- **Does the solution provide broad support for different applications, services and protocols?** Some solutions may support a broad range of protocols (SSH, web, etc.) and transports (IPv4 and IPv6), but others may only work only with web or email.

- **Does the solution require changes to subject behavior?** Some solutions may require additional steps to perform a given workflow, which could require your organization to make changes to your existing workflows.

[7] NIST

How Keeper Can Help Your Organization Adopt Zero Trust

Keeper's zero-trust, zero-knowledge cybersecurity suite enables organizations to adopt zero-trust remote access for their distributed workforces, with strong authentication and granular visibility and control. By unifying Enterprise Password Management (EPM), Secrets Management (SM) and Privileged Connection Management (PCM), Keeper provides IT administrators and security teams with a pervasive, single pane of glass to track, log, monitor and secure every user on every device from every location, as they transact with all permitted sites, systems and applications.

- Keeper's enterprise password management platform provides organizations the total visibility and control over employee password practices that they need to successfully implement a zero-trust security model. IT administrators can monitor and control password use across the entire organization and enforce security policies and controls, such as MFA, RBAC and least-privilege access.

- Keeper Secrets Manager provides DevOps, IT security and software development teams with a cloud-based platform for managing all of your infrastructure secrets, from SSH and API keys to database passwords and RDP credentials. All servers, CI/CD pipelines, developer environments and source code pull secrets from a secure API endpoint. Each secret is encrypted with a 256-bit AES key, and then encrypted again by another AES-256 application key. The client device retrieves encrypted ciphertext from the Keeper cloud, and secrets are decrypted locally on the device -- not on the server.

- Keeper Connection Manager is an agentless remote desktop gateway that provides DevOps and IT teams with effortless zero-trust network access (ZTNA) to RDP, SSH, databases and Kubernetes endpoints through a web browser. All users and devices are strongly authenticated before they are permitted to access organizational resources.