SECURITY COMPASS WHITEPAPER

Zero Trust Security: Moving From a Network-Centric Approach

Security Compass

Protecting sensitive information, defending applications against attacks, and securing organizational infrastructure has never been more challenging. Cloud migration has changed the roles of defenders, microservices and APIs have created a highly distributed threat surface, and the adoption of open source means more third-party code is included in applications.

While these technologies result in more agility and faster time to market, they also challenge traditional security policies.

One security strategy that is poorly suited to modern development approaches is network perimeter defense. This utilizes a "Moat and Castle" approach to defending assets; a strong perimeter defense keeps adversaries outside and allows "trusted users" unfettered access to resources once inside the castle.

There are several problems with this approach today:

- The Moat and Castle approach assumed all valuable resources and authorized users were within the castle. Today, these resources can be anywhere: on-premise, in the cloud, and virtualized. Furthermore, some of these resources may even include portions of a competitor's network. Creating network rules to manage this is complicated.

- Microservices and APIs result in interactions across full-time employees, contractors, competitors, and suppliers. Organizational network security controls do not scale well in this case.

- Employees today are increasingly remote and access the internet from networks not controlled by the organization. They use corporate devices and personal devices. Business continuity and security assurance is difficult in a network-centric paradigm.

- Attacks increasingly use phishing to steal legitimate credentials and exploit internal access. Once a user is authenticated at the network layer, they have access to sensitive resources by impersonating legitimate network traffic.

- Trust inside the network is ephemeral. Today's trusted user may be tomorrow's adversary. Insider attacks continue to grow, as disgruntled or compromised employees steal or share sensitive information. The 2019 Verizon Data Breach Investigation Report found that 34 percent of cyberattacks were perpetrated by insiders. Organizations must go beyond network security controls to manage this.

The traditional network perimeter is no longer enough. Today, teams need to go beyond the network into the application and data layers that define the security perimeter.

> **"You can't trust what is outside your perimeter — and now, all of your employees are outside your perimeter."**
>
> **Chase Cunningham, Forrester Research**

What is zero trust?

In 2010 an analyst at Forrester Research, John Kindervag, created a model called the "Zero Trust Architecture." Zero trust requires that a user's or system's identity and permissions be verified with each system interaction instead of verifying credentials once and trusting thereafter.

The idea is not entirely new. The Open Group's Jericho Forum instilled similar principles in the past.

Furthermore, security teams have long used the principle of least privilege; providing users with the minimum, explicit permissions while defaulting to deny permissions. Least privilege isn't explicit about "not trusting" users or systems. It simply states that there is no logical reason to extend "extra" permissions to users and systems that do not require them to perform a task.

Zero Trust takes this a step further — requiring users and systems to verify their identity and meet authorization requirements with each system interaction, then applying the least privilege access. Zero Trust takes the position that organizations must continue to operate even after a breach (an assumed breach strategy).

Zero trust eliminates traditional perimeter defenses

Zero Trust treats all users and systems as untrusted for each action, irrespective of their location or device.

With the proliferation of phishing attacks, known vulnerabilities in open source components, and insider attacks, it is safer to start with the assumption that adversaries have obtained a foothold and focus on a strategy of containment. This requires each component to perform its own validation of input, authentication, and authorization without any implicit trust in the network location or VPN.

A zero trust approach can help prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement.

Zero trust is data-centric

Instead of focusing on network defenses, zero trust architecture focuses on protecting critical data. The goal of most attackers is to steal or modify data, whether it is consumer information, financial information, or intellectual property.

Protecting sensitive data at all times — even in the event of a breach — is a core tenet of a zero trust architecture.

Protecting data starts by understanding and classifying the data each application manages and safeguarding it against unauthorized access or use throughout the application. This can mean adding requirements that data be encrypted at rest and in transit or requiring secondary authentication when the data is requested by a user or system.

Continuous security for applications

Traditional security establishes trust based on network location.

If a user is authenticated, allowed inside the castle, network, or application, they are trusted by all systems within the perimeter. This is poorly suited to today's development and deployment models which often lack a clear delineation of an application being inside or outside the perimeter.

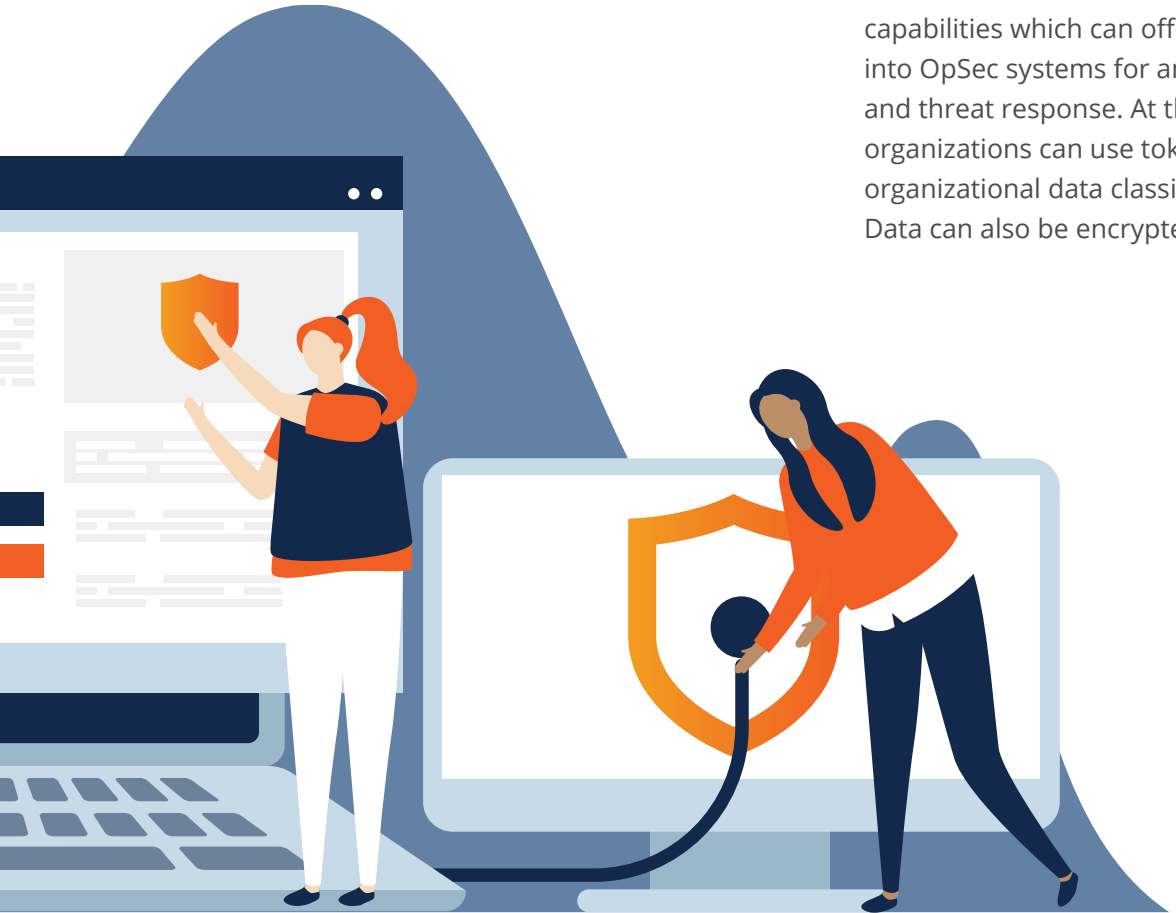
A zero trust architecture requires a user or system to verify trust with every access regardless of location.

Zero trust is layered security

Zero trust is not a single technology, but rather, a set of technologies that adhere to an application and data-centric security perspective. A zero trust architecture is built, layer by layer, on various technologies. Adaptive identity addresses the shifting roles of users.

For example, access control to specific applications and data are managed by policies rather than network rules, allowing for rapid and dynamic propagation of security controls to suit different contexts. This can mean building a profile of a user and her device then basing trust on each activity. It can require additional authentication when accessing an application from a new device or IP address.

From an application design standpoint, architects should consider building in audit capabilities which can offer a real-time feed into OpSec systems for anomaly detection and threat response. At the data level, organizations can use tokenization based on organizational data classification schemes. Data can also be encrypted for protection.



Expand the security toolbox to reduce threat scope

For applications to operate in a zero trust framework, the best approach is to start at the requirement phase of the development. This can include data classification, data security, multifactor authentication, encryption, and continuously validating a user or systems credentials and information requirements for real time auditability.

By anticipating threats to the application and including threat mitigation controls to the requirements document, development and security can build security into the process.

Verify, then trust

Zero Trust calls for 'no implicit trust' of a user or system until its identity and privileges are verified for each system interaction. It takes a layered approach which reduces risk from unauthorized systems or applications, compromised credentials, and malicious insiders as well as external adversaries.

It focuses on the protection of critical data.

Building security into an application from the beginning is far better than attempting to test for security in a completed application. The same is true with a zero trust architecture. By identifying critical data and requiring authentication and authorization before each use of data by a user or system, appropriate controls can be assigned and applied as the application is built.

Go Fast. Stay Safe.

Security Compass

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt balanced development automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on howorganizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
1001 Bayhill Drive
2nd Floor
San Bruno, California
USA 94066

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001