ZERO TRUST SECURITY: A CHEAT SHEET

TechRepublic

TABLE OF CONTENTS

03 What is zero trust security?

04 Why is zero trust emerging as a new cybersecurity paradigm?

04 What are the necessary elements in zero-trust architecture?

07 How can businesses adapt their security posture to a zero trust one?

ZERO TRUST SECURITY: A CHEAT SHEET

Zero trust means rethinking the safety of every bit of tech on a network. Learn five steps to building a zero trust environment.

BY BRANDON VIGLIAROLO

There are times when paranoia is justified, and nowhere is that more the case than with cybersecurity. Devices are compromised, laptops are infected, and smartphones are hacked all the time--a trusted laptop could leave a business network and return compromised, with the user none the wiser that they were the source of a major security breach.

Current cybersecurity practices are woefully unprepared to meet the complexities of modern networks. Cloud services, remote users, personally-owned devices, mobile company assets, and other forms of tech regularly move from outside the network in, and a once-safe device can't be assumed to be safe again.

It's here that a new paradigm in cybersecurity thinking emerges: Zero trust. In essence, a zero-trust approach to security assumes that every network is breached, every machine is compromised, and every user is (unwittingly or not) at risk.

No one and nothing on a zero-trust network can be trusted until it proves it's not an undercover threat to organizational security.

It might sound paranoid, but it might also be the best plan to secure networks against ever-evolving threats that can strike at any time.

WHAT IS ZERO TRUST SECURITY?

The US National Institute of Standards and Technology (NIST), in its current draft of standards for zero trust architecture, defines zero trust basically as "Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated."

Additionally, NIST adds, there is a distinction to be drawn between zero trust and zero trust architecture. "Zero trust (ZT) provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised."

Zero trust architecture, on the other hand, "is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies."

A holistic view of zero trust security is further defined by NIST as "the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan."

Zero trust security is, therefore, not only a product or an approach--it's a web of connected policies, practices, software, and hardware that create an entire zero-trust ecosystem.

Much like other kinds of digital transformation, zero trust isn't a plug-and-play solution to the shortcomings of current cybersecurity practices: It's a total commitment to a process that alters large swaths of an organization's structure.

WHY IS ZERO TRUST EMERGING AS A NEW CYBERSECURITY PARADIGM?

We need to be honest with ourselves: The current way of thinking about cybersecurity isn't working. Spending on cybersecurity continues to increase, but so does the rate of breaches. 2019 alone was packed with breach stories from January to December that compromised the personal information of hundreds of millions of people.

Elevated risks of, and recovery from, breaches is taking its toll not only on the reputations of affected organizations, but on the people that work there, too. Nearly one in three breaches lead to C-suite executives being fired, and all while common refrains are sounded when the reason for breaches are uncovered: Its accidents and unwitting employees that are repeatedly ground zero for major cybersecurity incidents.

The rise in remote workers, satellite offices, cloud services, and mobile devices has led to networks that are so complex that they "[have] outstripped traditional methods of perimeter-based network security as there is no single, easily identified perimeter for the enterprise," NIST said.

Zero trust's emergence as an alternative to traditional "castle-and-moat" security doesn't mean that those traditional tools will go away--quite the opposite, in fact. NIST's draft zero trust standard argues that it's the very tools we currently have that will become part of the architecture of a good zero trust plan.

"When balanced with existing cybersecurity policies and guidance, identity and access management, continuous monitoring, and best practices, a ZTA strategy can protect against common threats and improve an organization's security posture by using a managed risk approach."

WHAT ARE THE NECESSARY ELEMENTS IN ZERO-TRUST ARCHITECTURE?

Zero trust starts from an obvious position: All network traffic and nodes are assumed untrustworthy until proven otherwise, every time they access a network. That said, there's a lot that goes into building a zero-trust network that maintains security without burdening users.

NIST's outline of the logical components of a zero trust network (**Figure A**) shows the basics of what is required to build a zero-trust network (objects inside the circle) and the types of data that feed into a policy engine to make determinations about what and who are safe to allow access (objects outside the circle).

Figure A

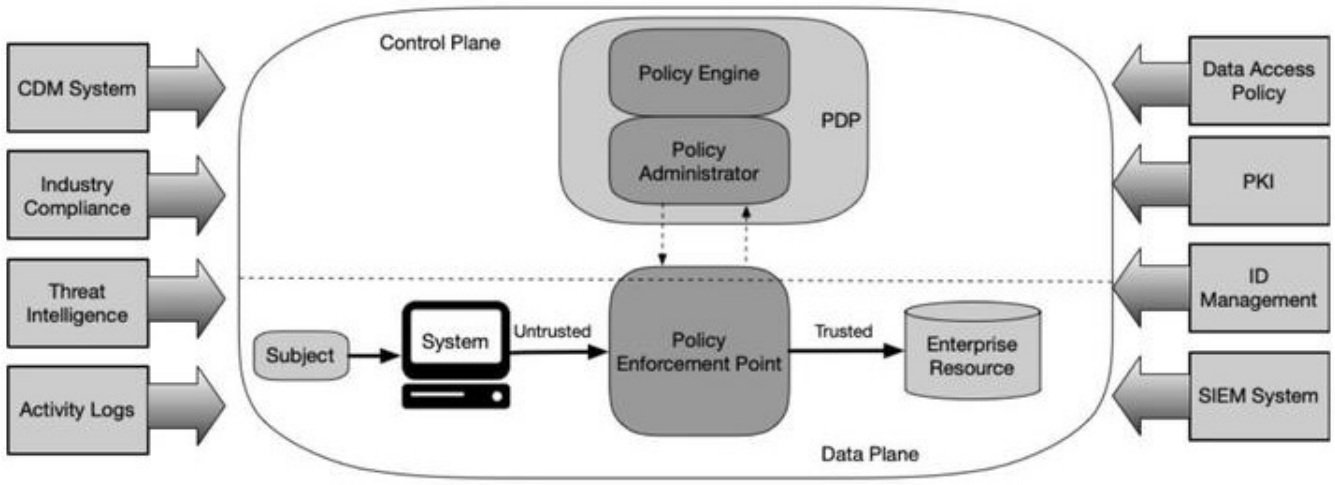

IMAGE: NIST

AN EXAMPLE OF ZERO TRUST ARCHITECTURE.

NIST calls the model in Figure A a conceptual ideal, but it's worth remembering that all of the elements pictured are necessary for a good zero-trust network, and that all of them are tools or procedures that already exist.

To better understand how an ideal zero trust network works, it can help to break it down into a few different elements, as illustrated in Figure A, starting with the components of the policy decision point (PDP).

The policy engine (PE) and policy administrator (PA) decide that a machine or web traffic is safe, and grant or revoke access, respectively. The two work in tandem and can be part of the same software service.

The policy engine uses external data sources (outside the larger circle in Figure A), and any other data applicable to an organization's needs, to make safety determinations based on security policies. External data can include:

- Continuous diagnostic and mitigation (CDM) systems, which gather information about an asset's current security state, update the device's OS and security software as needed, and communicate that state to the PE;

- Industry compliance checks that ensure traffic and assets are behaving within industry and organizational compliance rules;
- Threat intelligence feeds, like blacklists, malware engine definitions, CVE entries, and other up-to-date security resources;
- Activity logs that can indicate unusual activity from particular assets, IP addresses, and other sources;
- Data access policies, which in a zero-trust system would be tightly designed and dynamically adjusted for each individual and asset to eliminate lateral movement possibilities for a network intruder;
- Public key infrastructure (PKI) that validates certificates issued by an organization to its assets and validate them against a global certificate authority; and
- Security information and event management (SIEM) systems that collect security-related data and use it for later analysis to improve the rest of the zero trust system.

This complex process happens constantly behind the scenes; the average user will experience something quite different, as shown at the bottom of Figure A in the section of the diagram labeled Data Plane.

From a user perspective, nothing obvious occurs in a zero-trust system that would make it feel different from existing cybersecurity. Data is pulled from the various sources listed above, the policy engine makes a security decision, and the policy administrator grants access, blocks it, or revokes access if the device or its web traffic seems atypical or suspicious.

This is only one of various models NIST provides as an example of zero-trust framework. Others, also based on existing technologies that can be easily adapted into a zero-trust system, include:

- Using micro-segmentation to build a zero trust network;
- Using software-defined perimeters and network infrastructure;
- A device agent/gateway model;
- Enclave-based deployment;
- Using a resource portal for each separate business function; and
- Device sandboxing.

That's only some of the possible ways to build a zero-trust network. Suffice it to say, there are incredibly diverse ways to implement it. At the most basic, the essential elements of building a zero trust network are:

- A wide variety of data sources to ensure your zero-trust model covers all possible security bases
- A robust zero-trust policy that makes the objectives, design, and enforcement of zero trust possible

- A system that can both make determinations about asset trustworthiness and implement those determinations
- An enforcement point (or points) that each asset has to pass through before any access to an enterprise resource is granted

There's a lot that goes into building a zero-trust network, but doing so isn't insurmountable. By combining the right technologies, planning, and employee training any organization worried about the capabilities of modern cybersecurity products can improve their networks.

HOW CAN BUSINESSES ADAPT THEIR SECURITY POSTURE TO A ZERO TRUST ONE?

The NIST zero-trust framework that is the basis of much of this guide has some good tips and strategies to help organizations interested in zero-trust security transition their networks, but if you're looking for a starting place it can be a bit hard to pick through to figure out the absolute basics.

For that, IT services provider CDW has an excellent list of five steps to building a zero trust environment that can apply to any organization.

Keep in mind that there will be growing pains when implementing zero trust: It's a total overhaul of cybersecurity that will involve a lot more asking for permission than many users are used to. Once in place, however, zero trust will be just as simple to work alongside as current security products and policies.

Step 1: Segment the network

Traditional cybersecurity has a single boundary of trust: The edge of the enterprise network. Zero trust is less castle, more secure government facility: Users have to constantly request access to areas they need to be, and if there isn't an absolute need for them to be there then security keeps them out.

Network segmentation is a lot like that government facility: There are lots of security boundaries throughout a segmented network, and only the people who absolutely need access can get it. This is a fundamental part of zero-trust networking, and eliminates the possibility that an attacker who gains access to one secure area can automatically gain access to others.

Step 2: Implement access management and identity verification

Multi-factor authentication (MFA) is a fundamental part of good security, whether it's zero trust or not. Under a zero trust system users should be required to use at least one two-factor authentication method, and possibly different methods for different types of access.

Along with MFA, roles for employees need to be tightly controlled, and different roles should have clearly defined responsibilities that keep them restricted to certain segments of a network. CDW recommends using the principle of least privilege (POLP) when determining who needs access to what.

Step 3: Extend the principle of least privilege to the firewall

Zero trust isn't concerned only with users and the assets they use to connect to a network: It's also concerned with the network traffic they generate. POLP, likewise, should be applied to network traffic both from without and within a network.

Establish firewall rules that restrict network traffic between segments to only those absolutely needed to accomplish tasks. It's better to have to unblock a port later on than to leave it open from the get-go and leave an open path for an attacker.

Step 4: Firewalls should be contextually aware of traffic

Rules-based firewall setups aren't enough: What if a legitimate app is hijacked for nefarious purposes, or a DNS spoof sends a user to a malicious webpage?

To prevent problems like those it's essential to make sure your firewall is looking at all inbound and outbound traffic to ensure it looks legitimate for an app's purpose as well as checking it against blacklists, DNS rules, and other data described in Figure A above.

Step 5: Gather, and actually analyze, security log events

Zero trust, just like any other cybersecurity framework, requires constant analysis to find its weaknesses and determine where to reinforce its capabilities.

There's a lot of data generated by cybersecurity systems, and parsing it for valuable information can be difficult. CDW recommends using SEIM software to do a lot of the analytics legwork, saving time on the tedious parts so IT leaders can do more planning for future attacks.

These five steps are the basics of implementing zero trust, and they don't touch on the more detailed elements of NIST's model or other types of fully conceived zero-trust architectures. It's somewhere to start, though, and can help organizations lay the groundwork and see how far their zero-trust journey will be.

CREDITS

Editor In Chief
Bill Detwiler

Editor In Chief, UK
Steve Ranger

Associate Managing Editors
Teena Maddox
Mary Weilage

Editor, Australia
Chris Duckett

Senior Writer
Veronica Combs

Senior Writer, UK
Owen Hughes

Editor
Melanie Wolkoff Wachsman

Staff Writer
R. Dallon Adams

Associate Staff Writer
Macy Bayern

Multimedia Producer
Derek Poore

Staff Reporter
Karen Roby

TechRepublic

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Cover Image: milo827, Getty Images/iStockphoto