TechTarget | SearchSecurity

Expert Guide

PRO+ Content

Making Sense of Zero-Trust Security

In this expert guide:

Abstract:

By this point, you've probably discovered that many organizations are gravitating towards a zero-trust network architecture (ZTNA), but at the same time, many haven't even taken the first step towards it.

This is understandable – there seems to be a marked lack of both resources and overall consensus on what zero trust is and what looks like structurally. For some, this means zero trust is too big an undertaking.

Still, there's talk abound about how pioneering companies such as Google and Cisco were able to implement zero-trust models of their own, so how did they arrive there? What steps were taken as far as education on zero trust?

Welcome to our expert guide, *Making Sense of Zero-Trust Security*. In it, we will go into detail on:

- What zero trust is
- How zero trust differs from more commonly used security tools and architectures
- A real-life example of a security model built on zero-trust methodology
- Guidelines on designing your own zero-trust strategy

Let's get started.

In this expert guide:

Definition: zero-trust model (zero-trust network)

Margaret Rouse, Technical Writer – WhatIs.com

The zero-trust model is a security model used by IT professionals that requires strict identity and device verification regardless of the user's location in relation to the network perimeter. The model is based on the assumption that all users, devices and transactions are already compromised, regardless of whether they're inside or outside of the firewall. By limiting which parties have privileged access to each segment of a network, or each machine in a secure organization, the number of opportunities for a hacker to gain access to secure content is greatly reduced. A network that implements the zero-trust model is referred to as a zero-trust network.

The main tenet of zero-trust security is that vulnerabilities often appear when companies are too trusting to individuals or outsiders. Therefore, the model suggests that no user, whether inside or outside the network, should be trusted by default.

The term zero trust was introduced by an analyst at Forrester Research in 2010, with vendors like Google and Cisco adopting the model shortly after.

In this expert guide:

Importance of the zero-trust model

The traditional approach to network security is known as the castle-and-moat model. The focus of this concept is that gaining access to a network from the outside is difficult, but once inside, users are automatically trusted. This becomes harder to manage as organizations keep their data distributed across multiple locations, applications and cloud services.

The zero-trust model acknowledges that focusing only on perimeter security is not effective. Most data breaches occur when hackers successfully bypass an organization's firewall and are then granted authentication into internal systems. Therefore, the zero-trust model is a stronger approach to protecting important resources.

Fundamentals of the zero-trust model

While there are various technologies and principles that can be used to enforce zero-trust security, the basic fundamentals include:

- Eliminated trust - No user or device should be trusted by default
- Least-privileged access - Users should receive the minimum amount of access necessary

In this expert guide:

- Microsegmentation - Security perimeters and network components are broken into smaller segments with individual access requirements
- Risk management analytics - All network traffic should be logged and inspected for suspicious activity

How to implement the zero-trust model

Some best practices for introducing zero-trust security to an organization:

- Keep network security policies updated, review them for vulnerabilities and test their effectiveness periodically.
- Implement multi-factor authentication (MFA) for all users without exception.
- Validate all devices that try to log into the network and only allow access to those that meet security standards.
- Rely on network segmentation, microsegmentation and perimeter segmentation to secure individual aspects of the network.
- Maintain as much visibility as possible throughout the organization to avoid abuse of access that could lead to a data breach.
- Review the list of user accesses and administrators frequently.

Next Article

In this expert guide:

The 5 principles of zero-trust security

Andrew Froehlich, West Gate Networks

Perimeter security is no longer the best option for enterprise IT departments. A far more flexible architecture is needed that focuses on users, devices and services. The concept of zero trust was developed to take on current and future IT security threats by operating under the assumption that no person, device or service, inside or outside the corporate network, should be trusted.

Implementing the five principles of zero trust listed below will enable organizations to take full advantage of this security model, but an IT security team can't simply implement zero trust and then walk away. A continuous process model must be followed that cycles though each principle -- then it starts over again. The zero-trust model must continually evolve with business processes, goals, technologies and threats change.

Here are the five principles of zero trust that ensure the concept is successfully adopted into the long-term IT strategy.

In this expert guide:

1. Know your protect surface

An organization's IT protect surface consists of all users, devices, data and services. The protect surface must also include the means of transport -- the network-- that sensitive company data traverses. One of the main reasons why zero-trust architectures have become so popular is because the protect surface for most businesses now extends far beyond the protections of a corporate LAN. Traditional perimeter or edge security tools no longer have the same reach because many data flows no longer cross into the corporate network.

The change in data flows forces cybersecurity tools to be pushed out beyond the network edge to get as close to apps, data and devices as possible. Manual inventory processes should be supplemented with automated asset and service inventory tools. Combining these technologies helps teams identify what apps, data and devices are a security priority.

These tools are also used to understand where these critical resources are located and who should have access to them. This process effectively builds a map for security architects to help them understand where security tools would be best implemented.

In this expert guide:

In most cases, existing cybersecurity tools will not satisfy a complete, end-to-end zero-trust architecture model.

2. Understand the cybersecurity controls already in place

Once the protect surface is mapped, the next principle of zero trust is evaluating what cybersecurity controls are already in place. Many of the IT department's existing security tools will likely be useful when implementing a zero-trust strategy. However, they may be deployed in the wrong location or use an outdated perimeter architecture model. These evaluation exercises are useful when combined with the protect surface map because that enables IT security architects to see where existing tools can be redeployed or repurposed to reach the expanded areas where cloud and other internet-based resources now reside.

3. Incorporate new tools and modern architecture

In most cases, existing cybersecurity tools will not satisfy a complete, end-to-end zero-trust architecture model. Additional tools must be added to provide extra layers of protection where security gaps have been identified during zero-trust implementation. The good news is modern

In this expert guide:

security tools have been designed to pick up the slack where traditional tools fall short.

Examples of tools that enterprise IT shops commonly implement to meet zero-trust framework requirements include network microsegmentation, secure access control to all applications and data using single sign-on, and multifactor authentication. Additionally, advanced threat protection tools can be utilized to identify emerging threats and push security policy to resources precisely where they are needed across the protect surface.

4. Apply detailed policy

Once all the necessary technologies are in place to build a zero-trust framework, security administrators are tasked with putting those tools to use. This is accomplished by creating and implementing a zero-trust policy that can then be applied to the various security tools.

Zero-trust policies are rules that permit access to various resources based on a strict set of standards to only allow access when absolutely necessary. Policies should outline exactly which users, devices and applications should have access to which data and services and when. Once the high-level policies are built, administrators can then configure the security devices to adhere to the allowlist of permit rules, while denying everything else.

In this expert guide:

5. Monitor and alert

The last principle of zero trust is conducting necessary monitoring and using alerting tools. These tools give security staff the appropriate level of visibility into whether the implemented security policies are working and whether cracks in the framework have been exploited.

It's important to remember that nothing is completely secure, even with a zero-trust framework in place. Tools must still be used to capture when malicious activities occur so they can be quickly stamped out. Organizations should also perform root cause analysis to identify and fix any flaws in the existing security posture.

A distributed security architecture such as zero trust can be challenging to properly monitor by security operations center admins. Fortunately, modern cybersecurity monitoring tools exist that incorporate automation and AI capabilities to help ease that burden. Modern security monitoring tools, such as network detection and response and security orchestration, automation and response, help to cut down on the human resources required to identify security incidents, while also identifying root causes and remediation steps.

Next Article

In this expert guide:

SDP vs. VPN vs. zero-trust networks: What's the difference?

Michaela Goss, Associate Site Editor

To create a secure tunnel from one point to another or to make resources invisible to outside threats may seem like scenarios that require magic; in reality, they just need network security.

So begin the stories of VPNs, software-defined perimeter -- or SDP -- and zero-trust networks, three forms of corporate network security that present different approaches to security, with a shared goal of securing company resources. While VPNs have historically had a place in most network security plans, SDP and zero-trust networks are somewhat newer frameworks that aim to build off VPN capabilities and fill in the security gaps that VPNs miss. Still, VPNs have proven records of success in network security, while SDP and zero-trust models remain nascent.

Despite the differences between SDP vs. VPN vs. zero-trust networks, a shared goal for secure corporate networks ties the three technologies together, as does the increasing need for remote work support among organizations.

In this expert guide:

Defining SDP, VPN and zero trust

SDP. SDP is an overlay network -- or a network that sits atop another network connected with virtual or logical links -- that conceals network resources within a perimeter. Attackers and unauthorized users are unable to see or access the concealed resources, as the SDP acts as a cloud or an invisibility cloak to secure network resources.

SDPs use controllers to authenticate and connect authorized users to corporate network resources or applications through a secure gateway, based on identity policies, regardless of where the resources live in data centers, cloud services, etc. An organization may deploy SDP technology to reduce network-based attacks, which include denial-of-service or man-in-the-middle attacks.

VPN. VPN stands for virtual private network, and this technology encrypts tunnels between corporate networks and authorized end-user devices. With a VPN, remote employees can access network resources as if they were in an office directly connected to the corporate network. VPNs enable secure remote access for employees, regardless of whether they are in the office, at home or at a branch office location.

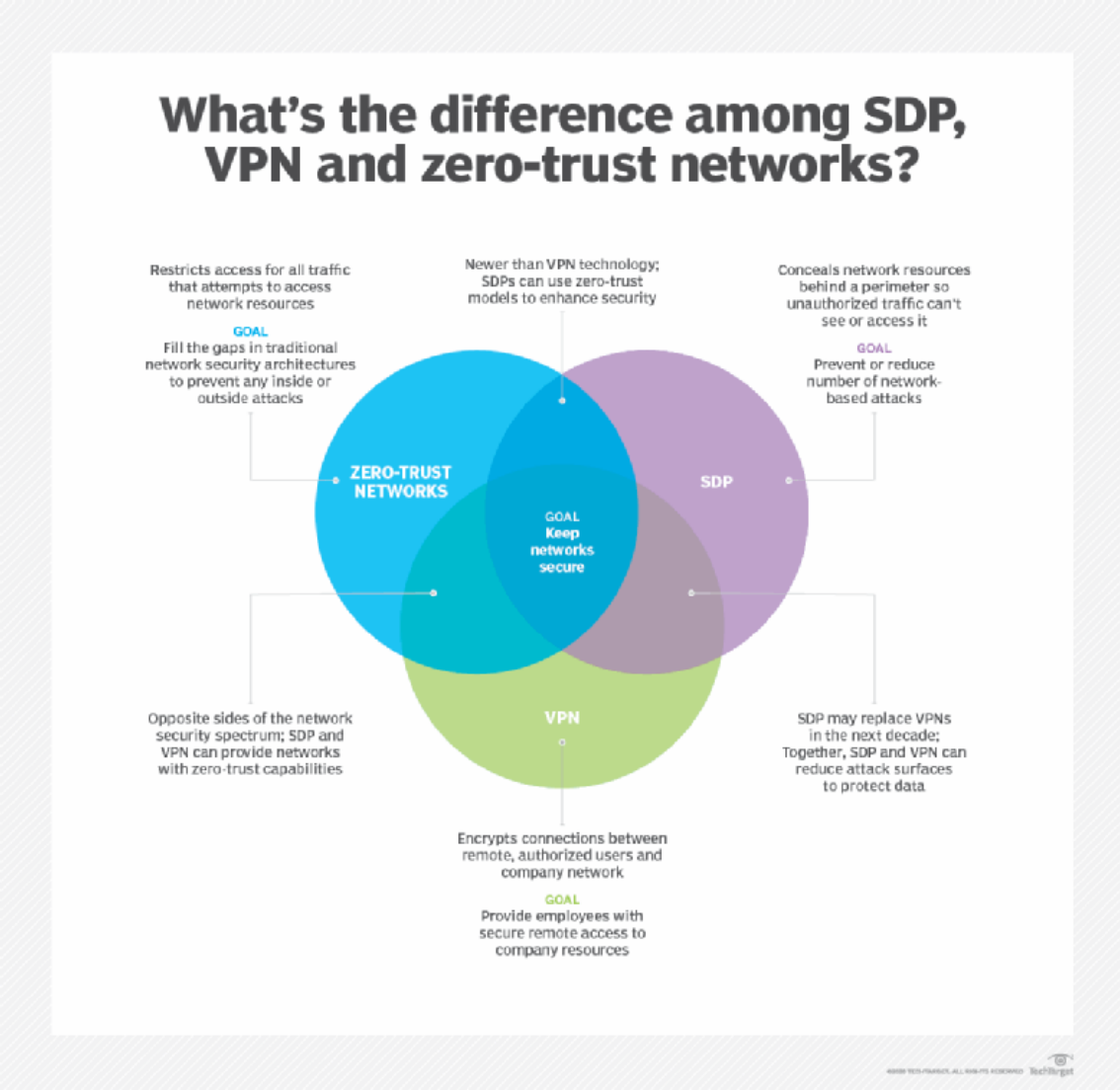
In this expert guide:

An organization may deploy VPN technology if it has a significant number of remote users or if it has more than one location for company resources to which employees require secure access. However, VPN shortcomings include a lack of support for diverse types of modern devices, such as IoT and mobile devices, that require network access.

Zero trust. Zero-trust networks trust no one. This means these models restrict every user's access to network resources, whether a user has accessed those same resources before or not. Any user or managed device that attempts to access resources within a zero-trust network must go through strict verification and authentication processes, even if that person or client is on premises in a company office.

Zero-trust models can expose potential gaps in traditional network security architectures, but these models can also introduce complexity in implementation, as the security framework can't have any gaps. Teams must also ensure the permissions and authorizations are constantly updated and accurate. Organizations that handle highly classified or sensitive data would benefit most from zero-trust network capabilities.

In this expert guide:



In this expert guide:

SDP vs. VPN

Vendors have touted that VPNs are irrelevant and SDP is the future of corporate network security. While SDP technology does attempt to take after VPN capabilities and improve upon VPN shortcomings, VPNs are still widely used -- especially after the novel coronavirus pandemic forced all companies into remote work, if the businesses were able.

However, SDP may still be the next natural progression in network security technology in the next decade. Instead of SDP vs. VPN, organizations may also consider deploying SDP and VPN together. SDP technology could fill security gaps in VPN services, which include the potential for credential theft and increasing the size of the network's attack surface.

VPN vs. zero-trust networks

VPN and zero-trust capabilities exist on opposite sides of the network security spectrum; VPNs enable connectivity for authorized remote users and managed devices, while zero-trust networks restrict access to all users at all times. As cyberattackers grow more advanced with their attacks on networks, VPNs may not be enough to stop them -- especially if the attackers somehow gain authorized access. With zero-trust capabilities,

In this expert guide:

attackers would still be restricted, regardless of whether they obtain authorized credentials.

However, it's possible for an organization to reap the benefits from both technologies. An organization may combine VPNs and zero-trust capabilities if it pairs SDP and VPN technology together, as SDPs can use zero-trust models to strengthen SDP security by delineating a clear network perimeter and creating secure zones within the network with microsegmentation.

SDP vs. zero-trust networks

Both SDPs and zero-trust networks are newer to network security than VPNs. This means these technologies have less proven success than VPNs do in the workplace, yet this also provides SDPs and zero-trust models with more room for innovation. As cyberattacks increase in volume and sophistication, enterprises can deploy SDP and zero-trust networks for more reliable and intuitive protection for modern networks.

SDP technology can use zero-trust capabilities to further protect network resources -- so, not only are users unable to see or access network resources hidden behind the perimeter, but those users will always go through strict authentication processes to access the resources.

In this expert guide:

One subset of zero trust is zero-trust network access (ZTNA), a Gartner-coined term for technology that creates a boundary, based on identity and context, around network applications or resources. Many experts use ZTNA and SDP interchangeably.

SDPs' and zero-trust networks' goals for stricter security will likely shape the future of network security for organizations.

Next Article

In this expert guide:

Google unveils BeyondCorp Remote Access as VPN alternative

Rob Wright, News Director

Google is extending its BeyondCorp service for zero-trust networks to aid remote works amid the COVID-19 pandemic.

The company introduced BeyondCorp Remote Access, which Google said will allow employees and extended workforce members to securely connect to internal web applications without using a VPN. In a blog post published Monday, Sunil Potti, vice president and general manager of Google Cloud, said BeyondCorp Remote Access will alleviate the burden on corporate VPNs, which have been overloaded in recent weeks as an increasingly large number of enterprise employees have been told to work from home.

Google's VPN alternative, Potti's blog post said, is designed to provide employees secure access to corporate web apps "from virtually any device, anywhere" by allowing enterprises to craft policies that grant conditional access to employees based on specific criteria. As an example, Potti described a scenario where HR recruiters working from home could only access an organization's document management system -- though nothing

In this expert guide:

else -- if their personal laptops' OS is up to date and has anti-phishing authentication like physical security keys.

Google first began developing its zero-trust network model for internal usage in 2011 with the goal of shifting security controls from the network perimeter to individual devices and their users. Instead of using firewalls and VPNs to protect web apps, the model allows Google employees, contractors and other authorized users to work from untrusted networks such as their homes, a hotel or an airplane.

The zero-trust network approach treats every device and user as untrusted unless they meet certain requirements about the device identity and configuration and the user's permissions and roles. Instead of a creating a private network connection between a device and the corporate environment, connections are run through components, including an SSO system to authenticate the user; an internet-facing proxy that applies encryption; an asset inventory database to confirm the identity of the device; and an access control engine that reviews the relevant information and enforces enterprise security policies before approving the connect.

In 2017, Google rolled out BeyondCorp, a commercial version of its own zero-trust network model, to other enterprises. BeyondCorp Remote Access is a variation of that model that focuses specifically on internal web apps that require VPNs for employees to access. Potti said Google plans to

In this expert guide:

expand the cloud service for "virtually any application or resource a user needs to access."

In addition to offering secure and reliable access, Potti said, BeyondCorp Remote Access can be deployed in enterprises more quickly and easily than client-side VPNs. Numerous reports have indicated VPN usage has skyrocketed in recent weeks during the coronavirus pandemic.

"With BeyondCorp Remote Access, we can help you do this in days rather than the months that it might take to roll out a traditional VPN solution, whether your applications are hosted in the cloud or deployed in your data center," he said. "Using BeyondCorp Remote Access, you can offload some of the strain on your existing VPN deployment, saving critical capacity for the users who already have access and need it most."

Potti added that Google is partnering with Deloitte Cyber Services to design and deploy the new offering. Deloitte did not respond to requests for comment at press time.

Next Article

In this expert guide:

How to find the right zero trust strategy

Paul McKay, Chase Cunningham & Enza Iannopollo, Analysts

In 2019, Forrester reported that zero trust (ZT) would hit the mainstream in Europe. Security and risk professionals in international organizations with European operations need to understand how to apply zero trust.

Forrester has developed a zero-trust extended framework to guide chief information security officers (CISOs) with their zero-trust strategies.

Zero trust is a conceptual architectural model that uses microperimeters and microsegmentation to secure corporate networks. The approach increases data security through obfuscation techniques, limits the risks associated with excessive user privileges, and dramatically improves security detection and response through analytics and automation.

Data knowledge

General Data Protection Regulation (GDPR) readiness means that firms today know more about their data: where it is, how it flows within and

In this expert guide:

outside their organizations, and how data access is governed. And these insights provide a substantial head start on your zero-trust implementation.

But acceptability of technical security controls varies dramatically by country. Forrester recommends CISOs pay attention to the local European cultural and regulatory norms wherever they are planning to implement the zero-trust model. Map out the regulations and stakeholders involved and build a plan to deal with them.

Examples of implementation issues when applying a zero-trust model

- DLP monitoring: France, Germany, Italy, Netherlands, Switzerland – strong resistance in workers' councils' countries
- PIM session monitoring: Central and Eastern Europe (CEE), France, Germany, Switzerland – resisted where seen as overbearing monitoring of employee activity and countries with aversions to surveillance given historical contexts
- Security analytics: France, Germany, Italy, Netherlands, Switzerland – resisted where seen as overbearing monitoring of employee activity and countries with aversions to surveillance given historical context
- User behavior analytics: Germany, Switzerland, CEE, whole of European Union (EU)/European Economic Area (EEA) – resisted where seen as

In this expert guide:

overbearing monitoring of employee activity and countries with aversions to surveillance given historical contexts

- Privacy regulations and data security: whole of EU – strengthened due to introduction of the General Data Protection Regulation.
- Cryptographic key management transfers out of EU/EEA to third countries with restrictions – seen when exporting encrypted data outside of EU/EEA to countries with requirements to issue cryptographic keys at government request.

For instance, countries with employee-led corporate governance resist employee monitoring. Standards of corporate governance in countries like France, Germany and the Netherlands emphasize employee participation. Workers' councils enjoy substantial authority to challenge management and protect employee interests, and they heavily restrict monitoring of employee actions and systems use. Thus, security leaders need to exercise care in monitoring employee actions when using security user behavioral analytics (Suba), data loss prevention (DLP), or privileged identity management (PIM).

You'll need to prove to the workers' councils that your plans don't degrade employee rights or intrude into employees' actions. As one supplier executive put it: "It used to be that we just didn't sell any DLP in Germany full stop. The conversation now starts with, 'How can we do it safely?' rather than an outright denial."

In this expert guide:

CISOs can take advantage of this shift to a more sophisticated understanding of the intersection of security controls and privacy laws. Your own efforts to engage stakeholders need to show that you have listened to their concerns and that you have taken their views into consideration.

Plan for explicit review and stakeholder approval steps in your ZT road map as you develop your reference architecture. Develop a risk mitigation plan showing how you will mitigate any privacy or cultural concerns.

Data regulations and restrictions

The GDPR defines personal information broadly, hampering security monitoring. The GDPR considers such data points as dynamic IP address, device identifier and authentication credentials, that are commonly collected during monitoring, to be personally identifiable information (PII).

Implementing visibility controls in the ZT model becomes harder as a result, particularly when your analytics platform is deployed outside of the European Union (EU) or European Economic Area.

Be prepared to discuss your employee monitoring program in the context of the overall security strategy with your data protection officer (DPO),

In this expert guide:

workers' councils and data protection regulators. Be clear on what you're collecting, why it's necessary and how you'll safeguard employees' privacy.

Review necessary

Forrester recommends that CISOs review international data transfers and cryptographic key management.

If you need to transfer personally identifiable information of EU residents to a non-EU country (such as the UK after Brexit), you'll likely need to implement additional frameworks such as model contract clauses or binding corporate rules.

Or if you're transferring data to the US, you'll need to comply with Privacy Shield. Be very clear about the locations where data is stored or processed, and work with your privacy and legal teams to determine the most appropriate measures. Also prepare to face the required disclosure to governments of even encrypted data.

For example, the Chinese Counter Terrorism Law requires firms to hand encryption keys to local authorities if they request them for decrypting information.

In this expert guide:

Where data is anonymized, the security visibility needed for zero trust is reduced. Data anonymization can mitigate some data protection concerns, but according to the GDPR, only completely anonymous data is not personal in nature.

Data is pseudonymized in most cases, meaning it's possible to re-identify individuals. However, the application of data anonymization techniques complicates ZT visibility by making it harder to identify the sensitivity or criticality of data in its anonymized form.

Colin McMillan, technical director for security at Cisco, says: "Data anonymization has been used by some European customers to deal with data sovereignty issues. But when implementing ZT, they still want visibility. Customers have implemented technical solutions in non-standard ways to get around this, making maintenance and support challenging for everyone involved."

Non-security executives think that zero trust is just a network security architecture. Network security decision-makers have driven zero-trust adoption in Europe thus far, with little discussion above the CISO level.

This could be a result of the high proportion (42%) of senior-most enterprise security decision-makers reporting into the CIO in Europe. Forrester recommends CISOs must emphasize the many elements of Forrester's zero-trust extended framework that reach beyond the network.

If CISOs don't elevate zero trust, their implementation efforts won't achieve their business and security goals.

This is an excerpt of Forrester's How to implement zero-trust security in Europe

Next Article

In this expert guide:

In this expert guide:

How to build and manage a zero-trust network in 4 steps

Andrew Froehlich, President – West Gate Networks

Zero-trust frameworks comprise multiple security elements, and one of those elements is the network. It is responsible for creating the physical and logical perimeter that separates the trusted infrastructure from untrusted devices and end users.

Network connectivity includes the LAN, wireless LAN, WAN and all remote access connectivity. The proper procedures, controls and technology must be put in place within each of these network segments to safely manage application and data access.

Let's look at a few ways network and security teams can accomplish zero trust within an enterprise network.

1. Identify users and devices

The first step in building a zero-trust network is to identify who is attempting to connect to the network. Most organizations use one or more types of

In this expert guide:

identity and access management tools to accomplish this goal. Users or autonomous devices must prove who or what they are, using authentication methods such as a password or multifactor authentication. For end users, it's important that this process be simple, seamless and uniform, no matter where, when and how they are connecting.

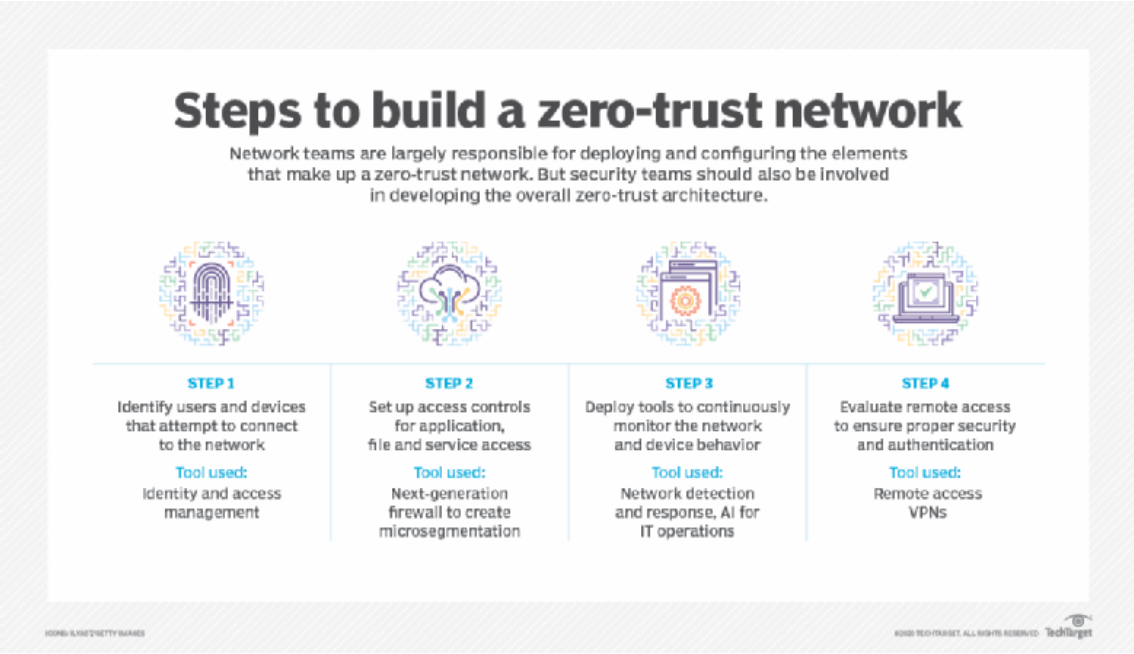
2. Set up access controls and microsegmentation

Once a zero-trust framework successfully identifies a user or device, it must have controls in place to grant application, file and service access to only what is absolutely required. Depending on the technology used, access control can be completely based on user identity, or it can incorporate some form of network segmentation in addition to user and device identification. This is known as *microsegmentation*, which is used to create highly granular and secure subsets within a network where the user or device can connect and access only the resources and services it needs.

Microsegmentation is great from a security perspective because it significantly reduces negative effects on an infrastructure if a compromise occurs. Next-generation firewalls are the most common technology used to create and control microsegmentations within a corporate network. These firewalls offer network visibility all the way to the application layer of the OSI

In this expert guide:

model, or Layer 7. Thus, teams can build and manage logical access policy around each application that runs over the network.



3. Deploy continuous network monitoring

Proper monitoring of device behavior is another aspect of a zero-trust network. Once access is granted, teams should deploy tools that

In this expert guide:

continuously monitor a device's behavior on the network. Knowing who or what the user or device is talking to and at what frequency can help determine whether things are operating normally -- or if some sort of malicious behavior is occurring. Modern tools, such as network detection and response or AI for IT operations platforms, can assist with network monitoring using AI, machine learning and data analysis.

4. Consider remote access

Remote access is an increasingly important part of any corporate network infrastructure. Legacy remote access VPN connectivity has proven cumbersome and inefficient in an era of hybrid cloud computing. Additionally, VPN access controls enabled far too much network access than what enterprises needed, turning remote access into a major security risk over the years.

To remedy this problem, suppliers have released new remote access methods and services to bring remote connectivity back in line with a zero-trust methodology. The benefits of these remote access methods include the following:

In this expert guide:

Security teams should develop and maintain the overall zero-trust architecture. That said, network teams should deploy and manage certain parts of the framework.

While enterprises still require remote access VPNs for secure connectivity, VPNs are drastically changing to meet the changing needs of an organization.

Who should manage a zero-trust network?

When enterprise IT organizations begin looking at how to build zero trust within their infrastructure, the first question they often ask is: Who should manage the zero-trust network components? This isn't an easy question to answer because much of the answer has to do with how the IT department is structured -- and who is more capable of handling certain tasks.

Security teams should develop and maintain the overall zero-trust architecture. That said, network teams should deploy and manage certain parts of the framework, such as network tools and services. The reason for this is the network team likely has more experience configuring and managing the network tools that make up the zero-trust network, including network switches, routers, firewalls, remote access VPN and network monitoring tools. While these roles and tasks may fall into the hands of the

In this expert guide:

network team, it's important that the security team perform regular audits to ensure the network properly adheres to all processes that make up the entire zero-trust framework.

Next Article

In this expert guide:

Explore the top 3 zero-trust certifications and training courses

Katie Donegan, Associate Site Editor

Traditional approaches to security historically included perimeter-based defenses and an implicit trust of network insiders. Zero trust, a wholly different approach to security, treats all users and resources, wherever they are located, as equally untrusted. Organizations will need all hands-on deck to implement zero trust, and that will require zero-trust certification and training.

"Zero trust is a team sport," said Holly Felicetta, senior product manager at Forrester, during the organization's 2020 Security & Risk Global summit.

A zero-trust team stretches across IT functions, including security, networking, applications and data, to finance, HR and C-suite executives because financial records and documents contain sensitive data that must be identified, mapped and safeguarded.

"People you have to involve in this may not be engaged in security. They may not even understand the value security has for the organization. But they do understand the value that their data has for the business," said Chase

In this expert guide:

Cunningham, principal analyst at Forrester. "You need to get them involved as allies.

Understanding zero trust

To facilitate this coordination among different departments, security practitioners must be able to communicate what a zero-trust strategy is and why it's important to the business. But buyer beware: The strategic aspect can get lost in the zero-trust "vendor hype."

Equipped with the right training, business and IT leaders will be able to make smart decisions about how zero trust can fit into their organization, and they might be surprised what already exists in their enterprise that can foster zero-trust security.

Explore this overview of how to build a zero-trust network and the tools you can use to help.

"You have been doing things that work to enable zero trust whether you realize it or not," said Cunningham, in reference to firewalls, data loss prevention, endpoint security, and identity and access management programs. "What you need to do is take a step back and look at this strategically and programmatically and ask, 'What do I need to have

In this expert guide:

to enable the concept of zero trust?' Focus on what you can fix at a micro level, and then work your way outward."

Zero-trust certification and training options

Organizations should invest in a specialized zero-trust training program to ensure the cross-functional team can speak the same language and collaborate on a comprehensive, enterprise-wide strategy.

You have been doing things that work to enable zero trust whether you realize it or not.

Here are the top three zero-trust certifications and training courses available for security practitioners and teams from Forrester, Cybrary and Pluralsight.

1. Forrester's Zero Trust Strategy certification

Forrester offers two versions of its Zero Trust Strategy certification, one for individuals and one for teams, both priced at around $2,000 per person. This comprehensive, on-demand program spans eight weeks and is designed for experienced technologists. Among the instructors are

In this expert guide:

Forrester principal analysts Chase Cunningham, Jinan Budge, Renee Murphy and Jeff Pollard, in addition to Stephanie Balaouras, vice president and group director, and research director Joseph Blankenship.

The six main topics covered in Forrester's Zero Trust Strategy program are the following:

1. the Zero Trust eXtended (ZTX) framework
2. five steps to a zero-trust network
3. the business case for zero trust
4. supporting zero trust
5. leading change
6. maturing zero trust

Successful completion of the program merits certification as a Forrester ZTX Associate (ZTX-AC) or a Forrester ZTX Strategist (ZTX-S). The ZTC-AC and ZTX-S certification requirements vary slightly. The participant's previous professional experience as a technology practitioner may determine which certification track to pursue.

To be awarded a ZTX-AC certification, one must do the following:

- earn the required 710 points; and
- complete the mandatory curriculum to-dos.

In this expert guide:

To become a certified ZTX-S, participants must do the following:

- earn the required 710 points;
- complete the required to-dos;
- complete three Strategist Assignments; and
- complete the Strategist Project.

Participants earn points by completing curriculum activities, watching course videos and engaging in discussions with other participant profiles. All exercises and assignments are submitted on Forrester's certification learning platform. The course also features a leaderboard, which displays top point earners to introduce competition in the learning process. Participants may also claim continuing professional education (CPE) credit with (ISC)^2 for the hours spent working toward certification. Forrester advises between nine and 18 hours of coursework as a minimum to claim CPE credit.

These certifications and training options can build on your security team's skills to enable successful zero-trust implementation.

Individuals seeking ZTX-AC should expect to spend one to two hours per week on the course requirements. Those seeking ZTX-S certification should expect to spend two to three hours per week and budget extra time to work on the Strategist Project independently. The additional Strategist Assignments and Strategist Project required of the ZTX-S certification are

In this expert guide:

designed to arm the participant with an actionable zero-trust strategy and timeline that are ready to implement at their organization.

Participants who enroll in the full Zero Trust Strategy course are entitled to the downloadable ZTX Toolkit and ZTX Strategy Workbook. These resources include frameworks, templates and workbooks to help facilitate zero-trust implementation, including a board presentation template and zero-trust security vision blueprint.

If the course is purchased for a team of technology practitioners, Forrester offers optional analyst sessions to provide an additional hour of instruction on zero-trust strategy. Forrester recommends two analyst sessions per team per course, but this may vary based on the team's needs and goals.

2. Cybrary's Zero Trust Networks training course

In Cybrary's Zero Trust Networks training course, students will learn the fundamentals necessary to securely manage trust on users, devices, applications and network traffic. This beginner-level training covers the principles of zero trust, in addition to best practices for implementing this model in the enterprise. The course is instructed by Mario Bardowell, who holds a master's degree in cybersecurity and information assurance, in

In this expert guide:

addition to CISSP, (ISC)² Systems Security Certified Practitioner and CompTIA Security+ certifications, among others.

Cybrary's Zero Trust Networks training covers the following topics:

- Module 1
  - 1.1 Introduction
- Module 2
  - 2.11 Defining Zero Trust Networks
- Module 3
  - 3.1 The Big Fundamentals, Part 1
  - 3.2 The Big Fundamentals, Part 2
  - 3.3 Zscaler Integration with Zero Trust, Part 1
  - 3.4 Zscaler Integration with Zero Trust, Part 2
  - 3.5 Trust Management, Part 1
  - 3.6 Trust Management, Part 2
  - 3.7 To Trust or Not To Trust, Part 1
  - 3.8 To Trust or Not To Trust, Part 2
  - 3.9 Pop Quiz and Summary

There is no prerequisite for this course; however, Cybrary recommends that students have a prior understanding of perimeter firewalls, traditional network security architecture, public key infrastructure and network zones. The training is best suited for individuals with the following IT roles: security

In this expert guide:

architect, network operations specialist, system administrator and information systems security manager, among others.

The course can be accessed for free with a Cybrary subscription. Upon completing all components of the three modules -- which typically takes one hour and 17 minutes -- participants will receive two CPE/continuing education unit credits and a Certificate of Completion.

3. Pluralsight's Zero Trust Networking (ZTN): The Big Picture course

This course covers foundational knowledge that students will need to bolster their organization's network and better combat both internal and external malicious actors. This course explains how traditional network and security designs are ineffective at mitigating the complex challenges of today's IT landscapes and how the zero-trust architecture can help. Students will also learn about the security benefits of software-defined perimeter and microsegmentation, both integral to any enterprise zero-trust journey.

Pluralsight's Zero Trust Networking (ZTN): The Big Picture training covers the following topics:

In this expert guide:

- course overview;
- why we need zero-trust networking;
- creating a new network and security architecture;
- understanding how zero-trust networking works; and
- the zero-trust projects.

The course is instructed by Pluralsight author and independent networking and security consultant at Network Insight Matt Conran. It can be accessed for free with a Pluralsight subscription.

About SearchSecurity

In this expert guide:

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit www.SearchSecurity.com

Images; Fotalia