Ebook

Forcepoint | Powered by ConversationalGeek

Your Path to Zero Trust

Practical Steps to Achieve a Continuous Zero Trust Model

Introduction

Zero Trust is more than a buzz phrase. It's a new paradigm way of implementing cybersecurity that has taken on new urgency as increasingly distributed organizations deal with a growing onslaught of complicated and sophisticated threats that result in data breaches.

In a business world without perimeters, finding a balance between easy collaboration and data security can be challenging. The sudden increase in remote working has added layers of complexity, with users and data operating outside of traditional IT defenses that implicitly trust people who are inside of the network.

A modern Zero Trust approach follows the mantra "Never trust, always verify." Static all-or-nothing assumptions about who users are and what they can do are replaced by dynamic, explicit decisions made every time someone tries to access a resource or use data from it. How such data moves around, and what people do with it, are continuously monitored to spot anomalies and risky behavior quickly before they turn into breaches.

This guide takes you through the Zero Trust paradigm and what to look for in a Zero Trust solution. In this ebook, you'll find out:

- → How remote working is turning the cybersecurity landscape upside down
- → How using VPNs for remote workers creates so many problems
- → Why controlling how data is used is as important as controlling how it's accessed
- → The pillars of modern Zero Trust: explicitly granted access and ongoing control of data usage—tied together with continuous monitoring to validate trust and risk levels
- → Why Zero Trust is getting so much attention now (such as from SASE, NIST, and others)
- → What to look for when procuring Zero Trust solutions

"Never trust, always verify. Every time."

The World—and Cybersecurity—Turned Upside Down

History will look back on 2020 as the year a global pandemic rapidly changed the way people throughout the business world work.

While remote working isn't new, the sudden spike in people working from home has challenged organizations worldwide. Stanford University describes the U.S. as having become a 'working from home economy' with 42% of the U.S. workforce working from home during the pandemic.[1]

Supporting a remote and flexible workforce requires your organization to make business-critical data readily available without exposing it to misuse or theft. With more people, applications, and data than ever operating beyond the bounds of the traditional enterprise, corporate perimeters based on internal networks have disappeared. It used to be that you could create a firewalled garden that had everybody operating "inside" (even if they were connected from the outside), behind various network-based defenses. Now, with so many of your people "outside," and with apps and data moving to the cloud, processes and infrastructure that were designed for a handful of remote people rapidly get overwhelmed.

[1] Stanford University

Collaboration is more difficult when people are no longer in the same location. Employees still need the web content, SaaS cloud apps, and internal applications they used when they were in the office. But how they get to those resources and how you protect them often changes dramatically. Relying on your users to understand and follow best practices for keeping information safe is dangerous, especially when there are different levels of control outside versus inside. As they say, "hope is not a strategy."

WFH and BYOD

The Working From Home (WFH) movement has taken advantage of the long-standing Bring Your Own Device (BYOD) shift. A Syntonic report into enterprise BYOD use found that 77% of organizations expect BYOD usage will increase year-on-year.[2] Gartner predicts that by 2023, 30% of IT organizations will enhance their BYOD policy to allow new devices such as smart watches to join the corporate network.[3]

While this flexibility enables people to be more productive, it complicates the old approach to security that assumes that people and devices inside the network are implicitly trusted and safe.

An Enterprise Mobility Exchange (EME) survey found that respondents expressed concern about:[4]

- → The threat of fake Wi-Fi networks (28%)
- → Malicious mobile apps presenting a major security risk (25%)
- → Concern about phishing attacks on mobile devices (20%)

This gets even harder when unmanaged devices are used remotely in home networks or public Wi-Fi hotspots where IT security teams lack visibility and control.

Detecting a breach via a mobile device on a network is difficult. Thales researchers found almost half of companies still cannot detect a breach via a mobile device on a network.

[2] Syntonic
[3] Gartner
[4] Enterprise Mobility Exchange

The Trouble with VPNs

Virtual Private Networks (VPNs) were originally developed to connect distant sites so that they could appear to be part of the same, often internal, network. Software versions were developed to enable "road warriors" and remote workers to connect into the corporate network back when only a fraction of the workforce was working off-site. But, with the pandemic, many organizations turned to VPNs as a quick way for newly remote users to still be protected by existing on-premises defenses and to get to internal applications. Unfortunately, VPNs which were designed for connecting sites and often sized for relatively small numbers of users, created new headaches when used at previously unheard of scale.

For one thing, VPNs change how people work. Users must have the right software on their endpoint devices and know how and when to use it. VPNs are notoriously slow for modern, interactive cloud apps like Microsoft Office 365, so people often avoid using them if possible. But this forces them to remember which apps are "internal" and need the VPN versus which don't, leading to frustration and lost productivity.

Personal use of VPNs also drive up business costs. As people fled their offices, many organizations had to quickly buy and deploy additional VPN hardware, upgrade network paths, and add helpdesk staff to handle the increased problems that users were running into.

But the biggest long-term impact is likely to be the increased risks that arise from exposing internal networks, servers, and applications to potentially compromised users, devices, and remote networks. Some authorities have even warned against VPNs for remote users. The National Security Agency (NSA) recently issued an advisory on the security implications of poorly configured VPNs, noting, "Maintaining a secure VPN tunnel can be complex and requires regular maintenance."[5]

This is just the beginning of the problem. Seeing and controlling what remote workers do with sensitive data once they get it is often an even bigger challenge.

"Maintaining a secure VPN tunnel can be complex and requires regular maintenance."

[5] NSA advisory, July 2020

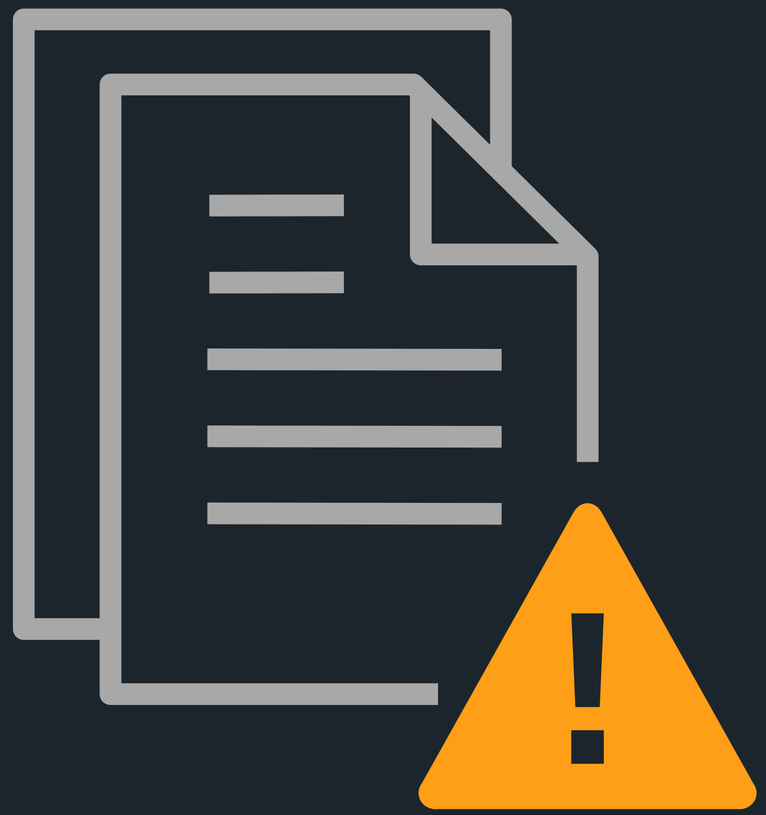
Where Old "Implicit Trust" Approaches Break Down

Change is a constant in business. Unfortunately, security often struggles to keep up, making data easier to steal or to accidentally expose.

With the rapid shift to remote working, criminals are taking advantage of the expanded connectivity to get inside organizations where often they're automatically trusted and given free reign to sneak into different applications, databases, and other resources.

The data drain

In 2019, the number of data records exposed reached 15.1 billion, the largest number in history.[6] Between January 1 and June 30, 2020, 27 billion records were exposed.[7]



[6] Risk Based Security
[7] Risk Based Security: Opt. In

A web of threats

Hackers love internet connections and communications as they offer open doorways into a corporate network. Attack methods such as phishing, malvertising (ad-based malware), and infected websites end up contaminating countless devices. Researchers have estimated that 1 in every 100 online ads are infected with malware.[8] Microsoft Office 365 is the most spoofed brand for phishing campaigns that target login credentials.[9]

Get stuffed

Once login credentials are stolen, they can be used to access corporate apps and portals using a technique called "credential stuffing." Akamai observed over 100 billion credential stuffing attacks between July 2018 and June 2020.[10]

Lost IDs

All security begins with determining who the user is—their identity. With stolen credentials, criminals can often impersonate employees, including C-suite executives, to gain access to sensitive information.

$240k

Cybercriminals are sophisticated and make use of emerging technologies like AI: A British director was tricked out of $240,000. The director was asked by the CEO of the parent company to make a money transfer. The voice at the end of the line was not of his boss, but most likely, a deep fake voice specifically created to carry out the fraud.

Internalized pain

Sometimes, employees and other internal staff expose or misdirect sensitive information. Such insider risks can be malicious, accidental, or the result of compromised credentials. A 2020 survey from Apricorn found that 57% of companies believe remote workers increase data exposure risk.[11]

The end(point) is (not) near

By definition, remote working means endpoint devices are physically distant from IT systems and staff who could otherwise help investigate and resolve issues quickly. Most enterprises use a variety of security defenses beyond basic endpoint antivirus software to protect the use of web content and cloud apps. But, if these security gateways are deployed on-premises, remote users are unprotected whenever they are connected directly to the internet (and not using a corporate VPN).

Even experts get it wrong

Misconfiguration is behind many of the world's biggest cyberattacks. Responding quickly to changing environments can put additional strain on IT teams as they work to find and fix security issues that are created as people work from new locations.

[8] MediaPost
[9] VadeSecure
[10] Akamai
[11] Apricorn

The Time Before Zero Trust

Zero Trust has been talked about for a number of years, so why is it taking off now? A (very) brief history of how we got to where we are in cybersecurity helps set the stage.

In the beginning

Computer security arguably began with the humble password. The first instance of the modern form of a computer password is attributed to the Massachusetts Institute of Technology (MIT). In 1961, MIT had one of the world's first computers systems that supported multiple terminals, used by various people, each with their private files. The system used a password as a lock to control access to each set of files.

Passwords persist but are not perfect by any means. As the number of devices and applications each person has to deal with explodes, setting and updating passwords becomes unmanageable. While alternatives to passwords are becoming common, it will be a long time before passwords go away.

86%

The Pew Research Center found that 86% of users memorize passwords. The researchers also found that 49% write passwords down on paper. A study by LastPass shows that the average person has to keep track of 191 passwords.

Everything, good and bad, is just one click away

More than any other technological innovation, the internet has changed the arena of security threats and countermeasures. As the internet became ubiquitous, new forms of communication such as email rapidly spread throughout society. Soon after, email started to become a conduit for viruses. As internet usage expanded, measures like firewalls and antivirus tools were adopted to manage cyberthreats.

Enter the web and cloud

The web and cloud-based applications were the next big step in computing to disrupt the threat landscape. Cybercriminals often used web-borne attacks to get malicious code into users' browsers, which then became launching pads for spreading throughout the enterprise. Social engineering techniques made it even easier for cybercriminals to target individual people, allowing them to manipulate our human instincts and use 'trust' that others would implicitly give them to gain entry or otherwise access to controlled systems.

99% of cyberattacks need human input to succeed.

Zeroing in on Zero Trust

When Darwin talked about "survival of the fittest," he referred to specific abilities; for example, a superior perception of smell gives a creature an advantage in a given environment. The history of cybersecurity threats and countermeasures ends up along the same lines.

Computer technologies, the ways we work, and the cybersecurity landscape have all interacted and co-evolved over time. We can see this playing out in the development of passwords and encryption as well as the shift from closed enterprise perimeters to cloud networks. Today, we find ourselves at an intersection of remote working patterns, hyper-connectivity across disparate devices, and sophisticated malicious actors. The result is a need for a more flexible and proactive way of dealing with cyberattacks.

Zero Trust has emerged as one of the leading ways of combating these threats and keeping sensitive information safe.

An overnight sensation that was 10 years in the making, it addresses a confluence of trends that are dramatically reshaping how business is done:

- → Ubiquitous, fast internet connectivity is available almost everywhere.
- → The shift to flexible and remote ways of working has been accelerated by the COVID-19 pandemic.
- → Organizations are striving to gain visibility and control for data everywhere—especially on remote devices and in the cloud.
- → Reducing complexity through automation has become critical to efficiency and security.
- → The battle against sophisticated cyberattacks that jump from one system to another is heating up.

Using Zero Trust to Secure Data Access And Usage—Continuously

The idea of Zero Trust security was first proposed by Forrester analyst John Kindervag in 2009/2010.[12] Rather than leaving applications, databases, and other resources open to anybody in the network, Zero Trust brings together several principles to make protecting information easier and more predictable:

- **It all starts with data** – Data is the most valuable asset of a modern organization, and breaches can put your entire organization in jeopardy. How data is protected depends upon the risks that would arise if it were exposed. To keep information safe, you must go beyond simply controlling access to enforce limits on what users can do with data they receive.
- **Never trust, always verify** – Zero Trust is all about vigilantly eliminating static all-or-nothing assumptions about what people are allowed to do based simply on where they are, replacing them with dynamic decisions that explicitly grant permission to access and use sensitive data.
- **Continuously monitor** – Keeping track of data as it moves throughout the enterprise, and of the actions taken by people who interact with it, enables you to validate that people are who they say they are and that they are not misusing your resources.

[12] Forrester details on Zero Trust
[13] NIST SP 800-207

Shifting away from implicit trust based on network or location

The National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-207[13] defines Zero Trust as:

- "Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.
- Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).
- Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments."

Zero Trust puts data at the center

Implementing Zero Trust begins with identifying what information is important. In fact, "Know your data" permeates the Forrester papers (and subsequent derivatives) on Zero Trust. This "data-centric" approach focuses on:

- → Knowing the "what," "where," and "why" of data across the data lifecycle, and …
- → Mapping the flow of data across a network and beyond

Forrester updated its Zero Trust model in 2018. The new version is called "The Zero Trust eXtended Ecosystem (ZTX)."[14] It extends the Zero Trust approach to people, devices, and data, making all of them intrinsically untrusted.

In Zero Trust, each user must be reliably identified and have explicit permission every time a resource is requested. Data is still the central axis on which the elements—people, devices, networks, and workloads—turn. No assumptions are made based on where users are connecting from, and permission to access or use a resource may be revoked at any time. For example, somebody might download a file from an application to their laptop, but then be denied the ability to copy it to an email message, USB stick, or cloud account.

Doing this dynamically requires continuous monitoring of people's actions. Modern Zero Trust solutions are even taking this a step further, looking for patterns of behavior to constantly validate that users are who they claim to be and whether those actions present a risk that would merit immediately limiting what the user is allowed to do.

Forrester emphasizes that enterprises must change how they "trust" data transactions across a network. As a starting point, they advise that all network traffic should be seen as "untrusted"—people at the other end of a connection must prove that they are who they say they are and they must have explicit permission to receive and use the data that gets transmitted.

[14] The Zero Trust eXtended Ecosystem

To help enterprises establish a Zero Trust environment, Forrester developed a five-step process[15] in which "zones" of control (which they call "micro-perimeters") for sensitive data are established:

Step 1: Identify

Knowing what data is important to control is the foundation for any Zero Trust approach. Forrester offers a "simplified data classification model" with three fundamental classes:

- → Public
- → Internal
- → Confidential

Forrester suggests looking at how and where 'chunks' of data are used that can be organized into zones that are controlled consistently.

Step 2: Map

Understanding where your sensitive data resides and how it flows enables you to more accurately map out potential risks and appropriate security measures.

Step 3: Architect

Designing your security so that the right set of controls—physical or virtual—are applied to each flow of data makes it easier to optimize your security, reduce the burden on your operations teams, and prevent breaches.

Step 4: Continuously Monitor

Modern Zero Trust approaches put strong emphasis on continuously monitoring the actions that affect the movement of data in each Zero Trust ecosystem. Behavioral and security analytics technologies enable anomalies and potential risks to be caught early before they turn into breaches.

Step 5: Automate and Orchestrate

Automation policies and security automation and orchestration (SAO) tools can help to establish and operate a Zero Trust infrastructure.

[15] Forrester

NIST provides framework for applying Zero Trust

In addition to defining Zero Trust, NIST Special Publication 800-207 also describes a variety of best practices for applying Zero Trust principles to devices, people, and assets. In particular, it talks about the importance of having reliable authentication (establishing that people are who they say they are, such as by logging in with passwords and multi-factor authentication technologies) and authorization (permission that's explicitly granted each time to perform some action, such as accessing or manipulating a resource).

The publication also lays out the importance of ongoing tracking of what is happening to resources such as data and to the people and programs that are manipulating it. Continuous monitoring not only provides confirmation that security policies are being followed, it also enables anomalous behavior to be spotted quickly. Human-centric approaches like this provide a much faster understanding of the risk each individual's actions might pose. As a result, mitigations such as increased authentication (asking people to re-confirm their identity, perhaps through other means than they initially used) or enforcement of more stringent security policies can be applied automatically.

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

NIST SPECIAL PUBLICATION 800-207

SASE incorporates Zero Trust Network Access (ZTNA)

A Zero Trust approach to security can be applied in a variety of ways. Gartner has explicitly incorporated it into their Secure Access Service Edge (SASE) architecture.

SASE brings web, cloud, private application, network, and data security together as a converged set of services, delivered from the cloud. It specially calls out Zero Trust Network Access (ZTNA) as the right way to give remote users secure access to private applications in internal data centers or private clouds. Sometime called a "software-defined perimeter," ZTNA gives people the information they need to get their job done without the complexities, bottlenecks, and risks of using VPNs.

SASE also emphasizes the use of data protection technologies, enabling organizations to go beyond access to securing usage of data.

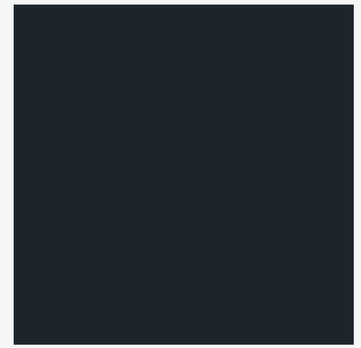
Zero Trust's "Secret Sauce": Continuous monitoring and control

Zero Trust is all about replacing implicit assumptions about who is trusted with explicit decisions made every time someone—or something—attempts to access or use sensitive resources. Early on, this was focused on controlling access in networks (a process known as microsegmentation) and requiring users to login to every app or server to gain access. This relatively simple approach provided an initial foundation for better security, but was too static and still left people with free reign over resources once they gained access.

Rather than stopping once access is granted, modern Zero Trust systems go much further. To keep information safe, decisions about what someone can do with sensitive data must be dynamic—made every time an action is taken. As a result, Zero Trust now incorporates the idea of continuous monitoring and control. In essence, users wanting to use particular resources are given temporary permission that can be revoked at any time.

A growing number of organizations are using data loss prevention (DLP) technologies to control how sensitive data is used. Most DLP systems are able to examine data in motion and at rest in the network, in cloud applications, and in users' endpoint devices. Any attempts to violate corporate data usage policies can be automatically blocked, even for remote workers.

A new generation of Zero Trust solutions are even applying user and entity behavioral analytics (UEBA) technologies to look for patterns in people's actions that could indicate potential risk to sensitive data. Such systems can connect the dots across digital, physical, and other systems outside of the data to determine when controls on how data is accessed and used should be automatically tightened.



[14] The Zero Trust eXtended Ecosystem

What to Look for in A Zero Trust Solution

When you take the plunge into procuring a Zero Trust solution, what are some of the important things to look for?

Cloud-native security-as-a-service

Whether you're moving to a SASE architecture or just taking incremental steps, cloud-based security greatly reduces the burdens in safeguarding your people wherever they work.

Control over usage as well as access

All Zero Trust solutions talk about securing access. But that's no longer enough. Even if you think your people always are who they claim to be and never are hijacked by imposters who have stolen credentials, giving them free reign to use your sensitive data however they please, puts you at risk.

Continuous monitoring of users and data

Modern Zero Trust solutions, particularly ones that follow the NIST model, dynamically examine how your users and data interact. This gives you ongoing assurance that people are who they say they are and makes it possible to automatically personalize security enforcement to each individual's own actions.

Practical, Real-World Solutions for Zero Trust

Forcepoint has incorporated Zero Trust principles throughout its product lines, enabling you to give your workers anywhere safe access to web, cloud, and private apps while keeping advanced threats out and sensitive data in. Its unique approach brings together SASE control and protection, cutting-edge data security, and the industry's first behavior-based system for dynamically personalizing security enforcement according to each user's own actions.

Forcepoint Private Access (PA)

Cloud-delivered Zero Trust Network Access for giving remote workers safe access to private applications without the complexities, bottlenecks, and risks of VPNs.

Forcepoint Cloud Security Gateway (CSG)

Cloud-delivered SASE protection for safeguarding use of web and cloud applications, complete with true enterprise-class data loss prevention technology in the cloud.

Forcepoint Data Loss Prevention (DLP)

Industry-leading protection for sensitive data and intellectual property everywhere—in the cloud, in networks, and on users' endpoint devices.

Forcepoint Dynamic User Protection (DUP)

The industry's first user activity monitoring solution delivered as a cloud service gives organizations visibility into risky user behavior and mitigate loss at the earliest point of detection.

The Big Takeaway

From least privilege to Zero Trust: A transition to data- and human-centric security

The rise of the data-centric economy combined with a complex threatscape is driving a dire need for better approaches to security. With traditional access control tools becoming ineffective, Zero Trust is emerging as a leading way to better secure enterprise assets against data breaches.

A recent McKinsey study on the impact of COVID-19 on businesses and employees found that 85% of respondents said their businesses have:

"Somewhat or greatly accelerated the implementation of technologies that digitally enable employee interaction and collaboration, such as videoconferencing and filesharing."

Zero Trust is more than just a security fad. It's playing a key role in enabling organizations to support remote working for the long term.

Across all industries, 15% of executives said at least one-tenth of employees will work remotely two or more days a week post COVID-19. In the information technology sector, this figure is 34% of employees. Pre-COVID-19, the average figure was just 8%.

With a mantra of "Never trust, always verify. Every time." and a mission of protecting data, Zero Trust replaces implicit assumptions that people "inside" the enterprise are safe with continuous, explicit decisions made about who can access enterprise resources and what they can do with them. That's why Zero Trust is rapidly becoming one of the leading ways that organizations are ensuring that their data remains safe in a rapidly changing world.

"Never trust, always verify. Every time."

[14] The Zero Trust eXtended Ecosystem

Forcepoint

forcepoint.com/contact

About the Author

Dr. Christine Izuakor, CISSP, is the CEO of Cyber Pop-up, an on-demand cybersecurity service platform. Christine has over a decade of enterprise-level experience leading cybersecurity functions within Fortune 100 businesses, managing everything from global security strategy and awareness programs impacting 90,000 employees in over 300 locations, to owning vulnerability management of thousands of enterprise assets.

Izuakor earned a Ph.D. in security engineering, becoming the youngest and first African American woman to do so, holds a master's degree in information systems security, and regularly writes, speaks, and advises on cybersecurity issues.

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.