

# ZERO TRUST FOR MSPs


---

The Zero Trust  
Roadmap Managed  
Service Providers  
Should Follow



---

# Table of Contents

<b>Introduction</b>	2
<b>01. Crash Course: What is Zero Trust?</b>	4
What is and isn't Zero Trust?	5
Benefits of Implementing Zero Trust (For Clients)	7
Increased Security	7
Better User Experience	8
Cloud Compatibility	8
Benefits for Implementing Zero Trust (For You)	9
Lead By Example	9
Trust Building	9
Easier for You to Manage as an MSP	9
Opportunities to Monetize	10
<b>02. How to Get Zero Trust Buy-In from Your Clients</b>	11
Demonstrate Benefits Beyond Cost Savings	12
Take your Client's Security Pulse	12
Address any Objections	15
Share the Benefits	17
Develop a Marketing Plan	18
A Few Top-Ranking Industry Podcasts	19
<b>03. How to Implement Zero Trust with Your Clients</b>	21
Initial Strategy and Development	22
Implementation Stages	23
 Become a Stronger MSP with Zero Trust	26

## INTRODUCTION

# As a Managed Service Provider (MSP), you are your clients' go-to for all things IT.

---

**If you want to offer them the best security framework possible, you need to implement Zero Trust.**

Whether your clients are small, medium, or large enterprises, they rely on you to provide the resources and security necessary to run their business.

Zero Trust is a security concept that enables you to offer your clients the pinnacle of protection while increasing your market share and perceived value. In this whitepaper, you'll get a crash course on what Zero Trust is (and what it is not), along with a roadmap for simplifying security management and implementing Zero Trust for your clients so you can unlock the freedom to focus on growth.

CRASH COURSE

# What is Zero Trust?

01

# You've probably heard the term "Zero Trust" thrown around lately. It's gained popularity as a buzzword, even though it's often misunderstood.


As an MSP, the most important thing to understand is that Zero Trust isn't a product; it's a method of approaching security – a framework. The concept centers around the idea that employees should have the lowest level of security and identity clearances necessary to do their jobs – and no more.

In this section, we'll explore the details of the Zero Trust model, and why it's not only beneficial but vital for you and your clients to implement.

## What is and isn't Zero Trust?

Due to its buzzword status, the term Zero Trust gets thrown around a lot, but it's not always used correctly. Here's a quick guide based on the National Institute of Standards and Technology (NIST)'s [Zero Trust Architecture](#) publication that clarifies the main principles.

## Zero Trust is

- ✓ Sometimes also called Zero Trust architecture, ZT, or ZTA
  - ✓ Based on the principle of “trust nothing; verify everything”: devices are trusted only after they meet all credentialing and security requirements, but never trusted by default, and all users must be regularly authenticated and validated
  - ✓ A framework with three main parts:
    -  the principle of least privilege
    - Secure authentication using methods like multi-factor authentication (MFA) and passwordless authentication
    - Authentication at every login attempt or access transaction, not just at the beginning of the session
- 

## Zero Trust is *not*

- ✗ A way to make your employees' and clients' lives more difficult
- ✗ The idea that you “don't trust your employees and lock them out of necessary applications”
- ✗ A product, service, or tangible platform
- ✗ A new concept. While it has gained popularity recently because of how well it works in hybrid environments, the methodology has been around for over 10 years.

**While this list is a great starting point for understanding Zero Trust, there's a lot more to the framework and the way it benefits your business and your clients.**

## Benefits of Implementing Zero Trust (For Clients)

# Before you can sell your clients on the Zero Trust model, you need to understand the benefits for yourself.

These benefits will form the roadmap of your conversations with your small to medium-sized businesses (SMBs). Long story short? They have a lot to gain when they implement Zero Trust architecture - and a lot more to lose if they don't.

### Increased Security

The most obvious benefit to adopting a Zero Trust framework is greatly improved security, which SMBs cannot afford to take lightly in our increasingly cloud-based work environments.

A recent study by Check Point Research found that **cyberattacks are increasing worldwide**, with a 30% increase in weekly attacks on corporate networks in Q2 2024 compared to Q2 2023. Meanwhile, **IBM reports** that the most prevalent attack vector is stolen or compromised credentials.

Today, cybercriminals are smarter and more sophisticated than ever. To protect themselves and their business assets, your clients need a security strategy that's just as smart. **While Zero Trust principles can be used for both legacy on-prem and remote systems, the framework really thrives in remote environments, making it the perfect protection against security breaches that target remote assets, data, and workers through credentialed attacks.**

## Better User Experience

Many SMBs have evolved to support remote and hybrid work, but some were left with disjointed, ill-adapted solutions due to quick adoption. These setups put strain on their IT departments and make for a clunky or unsecured **end user** experience for employees.

No matter if your clients are utilizing on-prem or cloud security systems, a Zero Trust framework will offer increased convenience and a better user experience through elements like passwordless authentication, password vaults, and zero-touch onboarding and offboarding. A streamlined, intuitive user experience means better security with less friction, less frustration for employees, and fewer help desk tickets for your support teams to contend with.

## Cloud Compatibility

If your clients aren't currently using cloud-based software, they may not immediately see why Zero Trust's cloud compatibility matters. But whether they make the transition now or in a few years, cloud-native software is here to stay.

While the Zero Trust framework wasn't created for the cloud, it is a natural fit for cloud-native platforms and applications. Zero Trust makes use of many popular cloud-based applications, like single sign-on (SSO) and multi-factor authentication (MFA), because these solutions inherently protect the user and the way they access critical assets.

Simply put, choosing a security model that will integrate seamlessly with future IT advancements – whether they're ready to upgrade their systems today or not – is an investment in the future of cybersecurity, and your clients' success.

## Benefits of Implementing Zero Trust (For Clients)

# As an MSP, what's good for your clients is good for you, too.

Zero Trust not only positions you as a valued and experienced partner and streamlines your management process; it also offers additional monetization opportunities.

### Lead By Example

With 39% of technical leaders at small- to medium-sized enterprises feeling concerned about MSPs' security management, it's critical to prove to clients that you prioritize security both in your offerings and your internal practices. Ensuring you're secure internally benefits you just as much as it benefits your clients.

### Trust Building

One of the biggest impacts Zero Trust can have is how it can strengthen your clients' confidence in you as a trusted advisor. Offering a service that improves and grows their business – and being the person who brought it to them – builds your relationship, thus securing your clients' loyalty.

In fact, trust-building could even earn you more revenue in the long run.

A recent PwC study found that 46% of consumers spend more money when they trust the brand. You achieve and grow trust by investing in your partnership with your clients and bringing them not just products, but also frameworks specifically tailored to drive their success. Zero Trust is a powerful model that all SMBs can benefit from implementing.

### Easier for You to Manage as an MSP

With more businesses adopting remote work, your accounts likely look much different today than they did in early 2020. If you don't employ a Zero Trust model that allows you to better support the many security functions your clients need, you're working harder than you have to.

This is especially true if you are your clients' IT department. Converting to a Zero Trust model makes device and user management an easier process internally. When paired with cloud platforms, Zero Trust offers increased efficiency, convenience, single-pane oversight, customization, and automation options.

Having better, more streamlined oversight of your IT accounts also helps you manage another big issue for MSPs: [Shadow IT](#). Shadow IT costs companies money in the form of lost income from security breaches, non-compliant apps, poor password management, and lack of MFA controls. Instead of employees managing their own apps, devices and security strategies, Zero Trust's least privilege and authentication practices bring all elements of a company's security under one umbrella: yours. The better visibility you have into what individual users are doing, the more you can secure your (or your client's) organization.

## Opportunities to Monetize

While Zero Trust itself isn't a product or service, the framework does allow for opportunities to monetize.

Having Zero Trust as a starting point gives you a reason to introduce new platforms or applications to your MSP tech stack. For example, say you have a client who recently switched to a remote-first business model and is now struggling with instances of shadow IT. Using income loss as the conversation starter, you may bring up to them that upgrading to a Zero Trust-compatible, cloud-native security management system will help keep closer oversight on user provisioning and activities.

Since Zero Trust is perfect for remote environments but is still functional with on-prem systems, no matter where your clients are at in their tech journey, you can find a way to make Zero Trust work for them, while increasing your market share.

### Recommended Reading

Read an even more in-depth explanation of Zero Trust—and why it's important for your SME clients—in our [Zero Trust Demystified](#) whitepaper. The guide describes what Zero Trust looks like in practice, why more businesses haven't adopted the principles, and how to kickstart your implementation.

# How to Get Zero Trust Buy-In from **your clients**



02

# As an MSP, you're more than a software partner or an IT expert; you also have a business to grow.

---

To successfully bring your clients on board with Zero Trust, you need to appreciate their past experiences, their understanding of the concept, and any objections they might have — beyond just focusing on selling your product suite or services.

## Demonstrate Benefits Beyond Cost-Savings

While over one-third (37%) of IT teams reported saving money for their organizations by using MSPs, this is just one of the benefits. Security and improved IT effectiveness are also significant factors. Over half of IT teams noted that MSPs enhanced their security (56%) and increased their effectiveness at managing IT (57%), which are key benefits to demonstrate when selling Zero Trust to your clients.

## Take your Client's Security Pulse

To begin, you need to understand how your clients currently view security and how open they are to changing their thinking or biases. It's crucial to gauge their security mindset and identify any roadblocks that may prevent Zero Trust from being positioned as the logical approach.

A great first step is to simply start a conversation. Talk to your clients about their current security posture, and identify areas where there's room for improvement in their strategy. Hint: there is always more to be done from a security perspective—especially if a business has yet to implement Zero Trust.

 **Here are a few questions you may ask to get the conversation rolling:**

**“What is your organization currently doing well? What are you struggling with, or where do you see the greatest opportunity for improvement?”**

These questions help you take the temperature of a client’s overall happiness with the way their business is going, and reveal both what they value and what they perceive as their pain points.

**“What are your organization’s most valuable assets? How are they currently being protected, and how could you protect them better?”**

Zero Trust’s biggest benefit is increased security. Identifying the things your client is most committed to protecting can help build an emotional case around those assets.

**“How happy are you with your current level of security?”**

This question drills down into the frontlines of Zero Trust. If they report pain points around security, Zero Trust is an obvious solution.

**Note:** They may not know enough about their current security strategy to answer this, and that’s okay! Lack of knowledge is just an opportunity for you to educate them.

**“Are you familiar with the Zero Trust security model? If so, what have you heard about it?”**

This question helps you gauge your clients’ mood on Zero Trust. Is it a new concept for them, or do they understand its value but not how to implement it?

# These questions help you understand your customers' starting point and create a pathway to framing **your future Zero Trust conversations.**

Say you're interviewing a current customer who reports that they're very happy with their current security strategy, and have no interest in changing it. They may be a tough sell for a Zero Trust overhaul. In these instances, identify activities they may already be doing (or are interested in doing) that align with Zero Trust principles.

For example, implementing multi-factor authentication (MFA) has become an essential component of any Zero Trust model, but it's beneficial even outside of this framework. Instances like these can open the conversation back up to Zero Trust principles, which allows you to further your position and build more trust as an advisor and expert.

On the flip side, if the customer reports they've been struggling with maintaining security in their new remote workplace environment, or they've heard of Zero Trust but don't entirely understand it... you're in.

## Note

Regardless of where they land after this conversation, if they aren't currently using Zero Trust, find a way to frame it as the ultimate solution.

## Address any Objections

If your SMBs have heard of Zero Trust but haven't yet implemented it, you need to find out why. Here are a few common objections to Zero Trust implementation.

### Inconvenience of Changing Legacy Systems

**Objection: "It will take too long or cost too much to completely change our existing security approach."**

Because your clients may not have highly technical employees or an IT department, they likely know how to use their current systems, and little else. Or, they may have so much on their plate that the thought of also taking on a major migration seems impossible. Transferring what they know into a whole different platform can feel overwhelming.

#### How to Counteract It:

##### Acknowledge their feelings

Yes – if you're currently running an on-prem system, switching to cloud-based does represent a hefty initial investment.

##### Bring your clients up-to-speed with the Benefits of Zero Trust Security

Because the future is in the cloud, this is a sound financial decision that will make future growth and scalability as easy as pushing a button. On-prem security is costly year-over-year, so the sooner you make the switch, the better.

### Cost Constraints

**Objection: "Our (legacy) system is already fully paid for. I don't want to spend money on something new."**

Changing to a cloud-based platform that's more Zero-Trust compatible with its corresponding subscription fees may cost more money initially. Without understanding the benefits, this can feel like an unnecessary investment to make.

#### How to Counteract It:

Acknowledge their feelings. Yes – switching to a cloud-based platform that's more Zero Trust-compatible may cost more initially, but because the future is in the cloud, this is a sound financial decision that will make future growth and scalability as easy as pushing a button. On-prem security is costly year-over-year, so the sooner you make the switch, the better.

**\$4.88M USD**

Average cost of a security breach to a business. Can they afford the risk of leaving their systems vulnerable?

**60%**

of SMBs go out of business within 6 months of a security breach

## “Security Through Obscurity”

**Objection: “All this stuff is for bigger companies. No one is trying to hack my small business.”**

Many SMBs don’t think cybercriminals will bother to target a smaller company, so they think they aren’t at risk.

### How to Counteract It:

Security through obscurity is not security at all. Small businesses are often prime targets for cybercriminals because they may have a weaker security posture than larger enterprises.

## Misunderstanding Zero-Trust Benefits

**Objection: “Oh, I’ve heard of that. It’s probably just the latest trend that’ll blow over.”**

Due to a knowledge gap or misunderstanding, your clients may have a negative connotation toward Zero Trust, or think it’s too much of a hassle for not enough results. Or they think it’s “just another buzzword”.

### How to Counteract It:

This kind of objection just needs better education. If you have case studies or client success stories from moving to a Zero Trust model, share them. If not, check out a few of our Zero Trust resources to give your clients a more thorough understanding.



---

**While these are just a few examples of common arguments against Zero Trust, the pattern of listening to your client's objections and figuring out how the framework fits into their business can be applied to many different situations.**

## Share the Benefits

Once you've listened to any objections, rebut by sharing the benefits of Zero Trust, which are highlighted earlier in this whitepaper.

**Remember:** the goal in discussing the benefits should be to make your clients see that it is in their best interest to make the change, despite any upfront work that may be required. Helping them envision a secure future will not only set them up for a more streamlined, compliant approach to security but will position you as the ideal long-term partner on this journey.

## Develop a Marketing Plan

**While explaining Zero Trust and getting buy-in from your current customers is a critical component of implementing the framework, existing customers aren't the only opportunity you have.**

---

**It's just as important — in fact, perhaps more so — to get the word out about Zero Trust beyond your existing client base to future potential clients.**

The key to expanding your reach successfully lies in thought leadership. Presenting yourself as a Zero Trust expert gives your business additional credibility and helps build trust with potential clients, even before your very first conversation. Here are a few ways to corner the market on Zero Trust knowledge:

- **Make an appearance on industry podcasts** Such as **Make Work Happen**, **the SaaS Podcast**, or **Unsupervised Learning**. Podcasts reach a broad range of audiences, show that your organization keeps up with the latest trends, and give you a platform to evangelize Zero Trust from your perspective. It's also a great way to reach new customer segments and network with other industry professionals.
- Consider **hosting a webinar or lunch and learn** that educates viewers on the benefits of implementing Zero Trust. This type of "freemium" content is a great way to suss out potential warm leads, and sign-ups give you access to email addresses for continued visibility and conversations.




**Tip:** Make sure you think carefully through who you invite to these events to ensure the content is relevant to their business. It's far better to have a smaller audience who feels the content is tailored to them than a larger turnout with information that doesn't resonate. Be targeted with these activities, and consider hosting multiple events for different audiences.

- To expand your reach, **build out your social diagram**. This means being involved in Zero Trust-specific conversations on social media, joining groups, and connecting with other Zero Trust practitioners on platforms like LinkedIn. Look at your connections and strategically share content relevant to them, so they will further share it with their networks. It's the basic concept of "going viral," and it can be just as effective in business as it is with cat memes on Instagram. Strategically growing your social and business networks can also help you break into new customer segments and influence additional connections.

## Marketing Plan Additional Resources

**Marketing Plan Worksheet:** This PDF walks you through how to develop your company's marketing plan, and helps you organize your strategy for implementing Zero Trust with present and future clients.

**SMART Goal Setting Worksheet:** Use this worksheet to create tangible goals and actionable steps to achieving them.

 **Strategic Business Plan Worksheet:** You can use this worksheet yourself, or use it to facilitate a planning discussion with your clients. We also provide a facilitator's guide to help you lead your clients through the process.

## A Few Top-Ranking Industry Podcasts

### **Down the Security Rabbithole**

This podcast has gained popularity for discussing issues like cybersecurity law, what makes SMBs particularly vulnerable to attack, and new perspectives on current cybersecurity challenges.

---

### **SaaStr**

One of the most popular SaaS podcasts interviews top industry experts and executive leaders for all their tips and tricks.

---

### **The SaaS Podcast**

Host Omer Khan interviews startup founders and entrepreneurs on the latest trends in the SaaS industry.

---

### **The Social-Engineer Podcast**

This fascinating podcast delves into human psychology to explain how cybercriminals use social engineering to compromise private and company credentials. Host Chris (loganWHD) Hadnagy interviews an eclectic mix of reformed hackers, cryptocurrency experts, and academic researchers.

---

### **Unsupervised Learning**

Host Daniel Miessler talks about all things cybersecurity in this podcast, from tips and tricks to the latest breaking stories.

---

### **Make Work Happen**

How do IT leaders make work happen? Join us to hear how companies of all sizes are transforming their workplaces with stories of innovation, resilience, and success straight from the leaders making it happen.

# How to Implement Zero Trust with Your Clients

---

**03**

# Once you have client buy-in on adopting a Zero Trust framework, **the real fun begins:** helping them convert their legacy systems into an optimized Zero Trust model.

## Initial Strategy and Development

Start your Zero Trust implementation by taking stock of your current security system. For MSPs, this means performing a security assessment for your clients and formalizing their Zero Trust rollout strategy based on your findings.

### STEP 1

#### Gather Client Feedback And Conduct An Assessment

Questions to ask during the assessment:

- **Where do you feel the greatest weakness in your current security strategy is?**
  - Some options: Identities (lack of authentication), endpoints (lack of device visibility), Apps (lack of control and monitoring), Infrastructure (lack of access control, not using least privilege), Data (lack of cloud-based protection), Network (lack of threat detection or weak encryption)
- **To implement Zero Trust at your organization, what has to change?**
  - EX: Is there legacy software that needs to be upgraded? Do they have the capabilities to implement MFA, passwordless authentication, etc.?
- **Will these necessary changes require a time investment, a training investment, a cost investment, or all three?**
  - Help them prioritize and plan these changes in a phased manner.

### STEP 2

#### Develop A Feasible Rollout Strategy

- Look at the organization as a whole and try to align the Zero Trust adoption timeline with other large company-wide initiatives. For example, if the whole company is looking to move to cloud-based software, that's the perfect opportunity to piggyback with Zero Trust, too.
- Depending on resources, a typical adoption timeline typically takes 1-3 years.
- Create the deadline for full adoption, then work backward to decide on smaller milestones and deadlines.

### STEP 3

#### Continue your Role as a Trusted Advisor

Throughout Zero Trust implementation, ensure you have a clear, easy way for your clients to communicate issues with you. Make sure your customer support team is trained on common Zero Trust tickets to help further build trust and authority. Remember: You're likely dealing with a nontechnical audience, so communication should be clear and accessible.

## Implementation Stages

Once you've formalized the Zero Trust rollout strategy with your clients, it's time to begin implementation. Though each organization's timeline will look slightly different, all rollouts should take place in three main stages.



### STAGE 1

## Start with Users

The first phase focuses on identities and people. There are a few main reasons for this. First, it gives your clients a chance to focus on employee security buy-in. It is harder to form compliant, secure networks and devices if your users aren't on board with Zero Trust, making it a logical place to begin.

Users are also the most likely to be compromised by cyberattacks (via stolen credentials or data breaches) and the easiest to protect (with additional authentication and a robust Zero Trust campaign).

**Here are 3 main things to ensure you include in the user section of your client's Zero Trust rollout plan:**

- **Invest in IAM solutions like MFA and SSO.** MFA is one of the very best security measures you can take to protect your client's identities, and its implementation represents a short-term win to build confidence right out of the gate. These security measures are quick to implement without adding significant inconvenience to users.

Note: equipping your clients to run IAM services may be as easy as turning on options in their current cloud-native security software, or may mean selling them an add-on product or extension to their existing system. Make sure you've accounted for these changes in your rollout strategy.

- **Apply least privilege principles as soon as possible.** Implementing least privilege will likely include a current access audit to ensure existing users have the appropriate level of access... and no more. It's easier to do this through user groups rather than per individual user, but in a smaller company, this distinction may not matter so much.

For example, you could create a batch of least privilege permissions for all interns that expire after 3 months and only provide "viewer" privileges. Or maybe you make an executive leadership group where all execs receive the same least-privilege access to major applications and data. If you start with batch creation as an established baseline, you can always go back and increase privileges on a case-by-case basis later.

Keep in mind that this will very likely reduce or even remove privileges that some end users currently have... and may feel entitled to maintain. Communication is paramount to ensure a successful rollout of least privilege principles, which means a steady pulse of emails, reminders, and training. Work with your champion to identify who across the organization may struggle with this transition the most, so you can spend additional time with them. That extra hand-holding at this phase will pay dividends over the years to come.

- **Get rid of passwords altogether (if you can).** Many enterprises are moving toward a truly passwordless system of identity management. The reasoning is clear: “Passwords are snoopable, crackable, and stuffable, representing a significant weakness”. Converting to passwordless authentication methods greatly increases security while providing a seamless user experience.

### Go Passwordless in 3 Easy Steps:

1. **Ban easy-to-guess login credentials.** Start with a list of banned passwords users aren’t able to set as login credentials, such as 1234, Password1, etc. This is a great starting step to increase security while you work on a larger passwordless strategy.
2. **Upgrade your stack.** Going passwordless is, admittedly, a lot easier if your clients are already running cloud-based software. These modern products easily lend themselves to extensions with passwordless authentication options like biometric scanners and MFA.
3. **Weed out all old-school authentication methods.** If your clients are still using any products or applications with legacy login (simple username and password) that cannot support MFA, they need to go for a truly passwordless environment. For clients running many on-prem systems, this step may take a while and represent a significant cost. For those clients already working from the cloud, this should be a quicker fix.

Note: Going entirely passwordless won’t work for all clients. Due to government regulations and compliance laws, users in certain positions or certain industries are required to maintain a username/password login interface. However, moving toward passwordless authentication for other employees will still significantly increase your client’s security posture.

## STAGE 2

### Apply User Principles to Devices

Once your client has adopted their Zero Trust user policies, move on to the next biggest vulnerability: devices.

Remote-first work happened so suddenly that many organizations weren’t properly prepared. Today, they may still have weak bring-your-own-device (BYOD) policies, or may still be relying on outdated machine and device rules. For Zero Trust to be successful on the device level, your clients have to be able to track, secure, control, and decommission seamlessly. Here are a couple of steps for rolling out Zero Trust to devices.

- Revise the current, or develop a formalized, BYOD policy. If your client has a BYOD policy, take a closer look at it. If they don’t have one but allow it, help them formalize it. There are both pros and cons to allowing BYOD and many companies are turning to BYOD as the default in the new hybrid environment. Should your client choose to allow BYOD, you’ll need to help them create a clear policy that protects both users and company assets. For example, personal devices often have less stringent security requirements, anti-malware, and patches, leaving them more vulnerable to being compromised than the average managed device.

One solution is to utilize software that conducts “device health checks” before allowing an employee-owned device to connect to company networks or applications. You can then apply software-defined network (SDN) solutions to these devices to ensure continual security. Another option is to secure company access and data by using a security solution that offers containerization of company assets. Containerization keeps company assets from intermingling with personal information and makes offboarding secure and swift if a user leaves the organization.

- Ensure least privilege and Zero Trust principles are active for devices. This means creating safeguards and policies that require constant verification of devices— not just during login activity.

Suggest a cloud-native security solution like JumpCloud. The ease of managing devices in a single pane is one of the biggest selling points of upgrading to cloud native security software. For your MSP, the [multi-tenant portal](#) is indispensable for simplifying your customer care.

It can be challenging for teams to keep track of all their devices at once—especially if they are juggling both managed and personal devices. Cloud native software can streamline this approach by giving IT admins (or you, as the MSP) a single platform where you can view all devices, commission and decommission remotely, manage patches, and change privileges and permissions. If your client isn't currently using cloud software, this is a great opportunity to show them the benefits.

Once stage 2 is complete, your client should be fully entrenched in a Zero Trust culture. Applying these principles to users and devices already provides a much more robust security strategy you—and your clients—can be proud of.

## STAGE 3

### Apply User and Device Principles to Networks

The final stage of Zero Trust implementation is taking the principles used in user and device management and applying them to your clients' broader networks.

**“The perimeter did not disappear: our perception of the network perimeter has just evolved”**

Says Forrester.

Network perimeters used to be physical, like a building or a geographic location. Now, that location still exists, but it lives in the cloud.

In some ways, digital perimeters are more secure; cybercriminals can no longer walk into a building and wreak havoc on a company's networks. But they have grown in sophistication, and the cloud network still must be protected. Help your customers understand the importance of controlling their network perimeters, and offer software solutions to help make the process as painless as possible.

One way to secure this digital network with Zero Trust is by using a segmentation policy to “redraw” your clients' security perimeter. For example, segmenting standard vs. admin users offers admins the access they need to perform their daily tasks without giving standard users the same privileges. A more barrier-focused solution for in-office networks may be something like virtual local area networks (VLAN) separation, where certain protocols are limited to specific enterprise network segments.

#### **Another argument for the cloud:**

Cloud security platforms allow IT admins to manage network permissions all from one place, making network Zero Trust a much easier process.

Become a Stronger MSP with Zero Trust

# Hopefully, one thing is now clear about Zero Trust: implementing it isn't optional

And it's your job as the MSP partner to guide your clients through adoption. Encouraging them to implement this framework sets them up for success while positioning your organization as an educated, experienced, and trusted partner for security solutions. It's a win-win.

JumpCloud for MSPs™ provides MSPs with the Freedom to Simplify IT management through an Open Directory Platform that is identity-centric, cloud-native, and vendor-agnostic. Using JumpCloud, MSPs can centralize identity, access, and device management capabilities under a single Multi-Tenant Portal.

To learn more, please visit [jumpcloud.com/msp](https://jumpcloud.com/msp).

© 2024 JumpCloud Inc. All rights reserved.



Get **Started**