PrinterLogic
by VASION

Adopting Zero Trust Printing

Your Guide to a More Secure Future

Table of Contents

01 Your Current Network Security Is Failing

The workforce has changed rapidly over the last three years–where they work, the tools they use, and the sophistication of modern collaborative technologies. The back-end infrastructure previously used to support and protect business processes will no longer suffice in light of the remote work movement. We're now in the age of empowering end users out of necessity, but this poses new security vulnerabilities to address. Transitioning to Zero Trust Architecture is necessary if you intend to scale and secure remote work.

According to Deloitte, nearly 40% of organizations adopting Zero Trust accelerated their efforts because of the pandemic. Their primary reasons have been to reduce the risk of remote work and insider threats, mitigate third-party risk, and manage cloud risk.

Driven in great part by the rise of digital transformation, trends such as bring-your-own-device (BYOD) practices, surges in ransomware attacks, and the growth of cloud-delivered applications have allowed bad actors to exploit security holes that weren't present in years past. As network perimeters become nonexistent, assets are harder to protect, and cyberattacks have multiplied. These frequent attacks damage company reputations and expose customers' private information.

Why The Time Has Come

Remote work is a staple in today's work environment, and it's poised for continual growth. A report by Upwork found that remote work projections are strong, with nearly 40.7 million people expecting to work remotely by 2026. This would make up roughly a quarter of the U.S. workforce.

Remote Work Causes Security Headaches

42%

of respondents say their organizations have no understanding of how to protect against cyberattacks due to remote working

67%

of organizations say employees using their own personal devices for work weakened their security posture

47%

of organizations are concerned about the inability to control security risks of remote employees' home networks and personal devices

Source: Ponemon Institute

With companies becoming increasingly concerned about the security vulnerabilities of a perimeter-less network, another significant issue has come to the forefront: How can companies secure their network, assets, and data without limiting employee productivity?

Paired with the uncertainty of how to do so, organizations also encounter the following challenges:

- Offering off-network access to end users without risking vulnerabilities.
- Providing in-person office functions to remote employees, like printing.
- Enabling employees to do their jobs on the go with their mobile devices.
- Troubleshooting issues for employees, regardless of their location.

The increase in cyberattacks due to a distributed workforce has made it difficult for companies to secure critical data, particularly those who still follow traditional security approaches. Companies recognize that now is the time to throw away old security habits and embrace a new security philosophy designed to minimize risk in the ever-changing workplace.

Contact our team today for a demo to see how easy Zero Trust Printing can be.

Schedule A Demo

02 What Is Zero Trust? Why Should You Adopt It?

Zero Trust Network Architecture (ZTNA) is a completely new approach to traditional network models. Traditional networks trust anyone inside their network's perimeter and are protected through a single verification point (usually a simple password). Also deemed the "castle and moat" approach, a traditional network acts as the organization's moat, and everything inside the moat–endpoints, users, data, servers, etc.–is inherently trusted. The downfall of traditional networks is that once any endpoint inside the network is compromised, attackers can move laterally and gain access to anything else on that network. Sadly, the old premise of keeping the bad guys out and letting the good guys in just doesn't work in today's workplace.

The Zero Trust Philosophy

Let's start by discussing what Zero Trust isn't: A single product, a quick fix, or an all-in-one solution. These misconceptions were created because the term has been thrown around like you can find it on the shelf at your local supermarket. It's not a physical object. Zero Trust is a complete shift in the way organizations think about security.

> **"Zero Trust is not a product, although Zero Trust-based security infrastructures can be implemented by using many different products. Nor does Zero Trust require organizations to rip and replace existing security infrastructure–rather, it leverages existing technology to support the Zero Trust mindset, with new tools added as needed."**
>
> **— John Kindervag, the father of Zero Trust and a Forrester researcher**

Zero Trust is a security model based on the principle, "Never trust, always verify." In Zero Trust networks, no device is trusted by default. Users must be continually authenticated, authorized, and validated before being allowed access to applications and data, whether they are inside or outside the organization's network.

Full Steam Ahead

78%

of companies around the world report that Zero Trust has increased in priority.
Source: Okta

$38.6B

is the expected market value of Zero Trust in 2024 (20% increase from 2019).
Source: Deloitte

40%

of all remote access usage will be predominantly served by Zero Trust Network Access.
Source: Gartner

Zero Trust uses the Principle of Least Privilege (PoLP), a key tenet of the Zero Trust security model. This process reduces an organization's attack surface since users are only authorized to access necessary applications. Limiting access is one of the most critical pieces of an effective Zero Trust strategy since most cyberattacks are internal and, more often than not, accidental.

According to a study by **Ponemon Institute**, 54% of insider threats are due to negligence. This is the result of a variety of factors like not following company security policies, having no multi-factor authentication, and forgetting to patch and update hardware.

Zero Trust Networks also utilize microsegmentation, the practice of breaking up security perimeters into small zones, to prevent lateral movement by cyber attackers. Once a threat is detected, the compromised device or user account can be cut off from further access. By adding security policy enforcement in front of each workload, the ability of malware and other attacks to spread within the organization is greatly reduced.

According to **Guardicore's 2021 Segmentation study**, 96% of organizations are currently implementing some form of segmentation into their network. However, only 2% of the respondents have successfully segmented all six mission-critical areas. These numbers reflect how companies are aware of segmentation and its benefits, but may not have all of the resources or know-how to secure all critical assets.

Mission-Critical Areas

1. Endpoints
2. Domain Controllers
3. Servers
4. Business-Critical Assets
5. Critical Applications
6. Public-Facing Applications

Zero Trust's Rise to Prominence

So why has a concept that originated in 1994 finally become a priority for companies across the globe? Events transpired over the past three years have significantly increased the adoption of remote and hybrid work models. New workplace trends that were fueled by a rise in mobile computing, IoT (Internet of Things) devices, and cloud-based services had employees working outside the company network.

The pandemic exacerbated these issues, forcing workplaces to better secure endpoints and data as employees accessed company networks through their personal devices at off-site locations. In an Okta survey taken by over 600 global security leaders, 90% said they are pursuing Zero Trust initiatives due to the security challenges of hybrid work, a 41% increase from the year before (Okta, 2021).

Companies are already witnessing the financial perks of adopting a Zero Trust framework. According to a report by IBM Security, companies with a mature Zero Trust approach saved an average of $1.76 million compared to those with no Zero Trust initiatives. This is also true for companies that implemented critical digital transformation changes while adopting remote and hybrid work, which saved them close to $750,000 per breach.

You'll notice that experts use the word "mature" to describe a highly compliant Zero Trust framework. That's because achieving a 100% compliant Zero Trust Architecture is a myth. It's not a destination; it's a journey. A continuous effort is necessary to keep cyber threats out as technology and best practices evolve. Zero Trust intends to help businesses keep up with the leaps and bounds that cyberattackers have made in adapting to developing technology and work trends.

Common Barriers To Adopting Zero Trust

Budgets are Limited

Not every organization has allocated funds just for cybersecurity.

Change is Difficult

Everyone must be on board to deviate from legacy systems and processes.

Each Step is Critical

You need a clear understanding of company workflows to take proper steps.

Not Knowing Where to Start

Research, resources, and an initial plan are required to begin executing.

Contact our team today for a demo to see how easy Zero Trust Printing can be.

Schedule A Demo

03 Yes, Print Security Matters

Printers connected to your corporate network are a huge attack vector for hackers. But they continue to be one of the most overlooked pieces of machinery when discussing security and Zero Trust. Print security is a small, but critical, component that, if not taken seriously, can wreak havoc on a business. This is evident based on the number of print-related cyberattacks that have hit the news.

Cybernews reiterated the importance of securing printers when they hacked 27,944 printers to show how easy it was to gain access when printers were left unsecured (Cybernews, 2020). Another instance involved the breach of 150,000 printers by Stackoverflowin, a professional cyber attacker who infiltrated printers to flaunt his hacking prowess (Cybersecurity Insiders). The fact that printers are prone to large-scale attacks like these should put print security at the top of every company's priorities

Printers Are Your Weakest Link

They outlive almost every piece of office equipment despite having a lifespan of 3-5 years and were one of the first machines to be used in corporate offices around the globe. They're run into the ground before being replaced despite heavy use in corporate offices. When sitting around for a long time, they become forgotten, unpatched, and not updated to their latest firmware, leaving the gates open for cyber attackers to steal data.

According to a print security report by Quocirca, over two-thirds (68%) of organizations have experienced data losses due to unsecured printing practices in the past 12 months, leading to an average of $770,000 per data breach (Quocirca, 2022). Along with being an entryway into your business's network, hackers can also attack other applications or launch ransomware through a compromised printer.

Securing your printers is one thing, but the real security issues lie in using print servers. The increased complexity of print environments makes them difficult to maintain and manage.

The Concerns Are Real

70%

of organizations expect to increase their print security spending over the next 12 months

64%

of organizations state that printing will be critical to them over the next 12 months

67%

of respondents are concerned about the security risks of home printing, compared to 57% whoare concerned about office print security

Source: Quocirca

The information they output becomes vulnerable to security breaches and potential non-compliance if they aren't constantly monitored and updated.

An attacker can partake in various malicious actions against your system through your print server, such as: Installing a printer driver, using the spooler to drop files remotely, or using the spooler files to gain remote code execution privileges. Print spooler vulnerabilities like PrintNightmare, which suffered 65,000 attacks in nine months, have caused companies to reconsider their print infrastructure (Tech Republic, 2022).

The Rise of Remote Printing

You may think remote work would decrease the need to print, but the opposite is actually true. A study on remote printing following the pandemic found that 59% of employees printed more or the same amount at home as they did in the office. A separate study found that 67% of organizations are concerned about the security of home printing. Now, more than ever, employees work from remote and sometimes unexpected locations, accessing networks via a mixture of corporate and personal devices. More employees working from home and potentially using their devices to print corporate documents have created new print security concerns.

> **"Printers are often one of the first devices mentioned when discussing the security risks attached to connected devices. There are legitimate reasons for this: the printer is a highly recognizable piece of office equipment and something that many workers have at home too. As such, it is easy to consider a connected printer as a likely route through which hackers could try to gain access to sensitive data."**
>
> **— Aaron Anderson, head of Marketing at Kyocera Document Solutions UK**

The growing number of home printers used for company printing has created two situations at odds with each other–remote and hybrid employees need to print, but companies want airtight security for their devices. Unfortunately for companies, home printing creates two potential points of attack:

An unsecured machine connected to a company computer. Connecting a company computer to an unsecured home printer provides a gateway past any VPN or security. Once a hacker moves from the printer to the company drive, they can gain access to the company's primary network.

Information is stored on the printer's hard drive. Printer hard drives store previously queued print jobs for a varying degree of time. Hackers are able to break into these hard drives using a back door to view sensitive company information by accessing the employee's home Wi-Fi.

Providing secure remote printing solutions is one area you can expect significant development and innovation as remote working becomes the international standard for employment.

Your Printers Will Thank You Later

As you develop your Zero Trust strategy, it's a good idea to prioritize secure printing solutions. Why? Well, printing is as essential as it has ever been. Printers are where sensitive data flows and they're one of the easiest endpoints to penetrate. They're also the most costly when a breach does happen with an average cost of $8.94 million (Ponemon Institute, 2020). It's best to leverage a solution that will help you eliminate unnecessary hardware (like print servers), allow you to print securely from anywhere on any device, and doesn't require you to upgrade from your legacy printers.

Shifting to a Zero Trust way of thinking and incorporating serverless printing into your print environment enhances security, reduces costs, and increases scalability.

Additional benefits of Zero Trust print security include:

- Strengthening security for remote workers
- Simplifying print management for IT
- Reducing attack surfaces company-wide
- Increasing threat detection and prevention
- Enhancing visibility into all print activity

Contact our team today for a demo to see how easy Zero Trust Printing can be.

Schedule A Demo

04 PrinterLogic Checks All the Boxes

We get it. Moving from a legacy infrastructure is a daunting task. It takes time, money, and knowledge to start the transition. Leveraging PrinterLogic's Output Management solution allows you to connect processes from legacy applications to manage all aspects of document distribution, printing, and routing from a centralized platform. With the inherently necessary tools for your Zero Trust Printing environment, you can finally address your organization's needs with a scalable solution that unlocks the true potential of your document and print management processes.

Access and Identity Management

PrinterLogic offers native IdP integrations with leading solutions, including Okta, Azure AD, Ping Identity, OneLogin, and more. Take advantage of the identity protection and access management benefits of single sign-on (SSO) and multi-factor authentication (MFA).
You can even utilize concurrent IdPs with our Advanced Security Bundle.

Zero Trust Benefits:

- Verify hybrid workers' printing from anywhere with your preferred SSO application.
- Manage access to applications for on-prem and hybrid employees, and contractors.
- Allow automatic user creation with our SCIM and JIT provisioning-based integrations.

PrinterLogic makes it easy to verify and authorize every single connection without time-consuming manual updates from your team.

Authentication for All Connections and Endpoints

PrinterLogic is built around direct IP printing. Data for print jobs is held on the initial device until it is sent directly to the printer. Your data is not exposed or at rest in a server or spooler during printing. Our centralized control with Output Management makes it easy to ensure users have the right permissions and that their connected devices are authorized to access the data they share.

Zero Trust Benefits:

- Eliminate data being stored in the cloud or sitting at rest in a centralized location.
- Secure confidential documents at all times while printing with user permissions.
- Uphold security for all devices and endpoints with our device-agnostic solution.

Don't leave your data vulnerable with outdated print spoolers. Keep your data secure with PrinterLogic's direct IP printing architecture.

VAS-4803 | Apr 2024

Segmentation of Data to Limit Harm From Individual 4vBreaches

Hackers are getting more sophisticated and breaches are getting more costly. Print servers are a major focus because they connect to your whole network. By eliminating print servers, your attack surface is reduced, making your network a less desirable target. With PrinterLogic, each device connects directly to the printers. Even if one device is compromised, data on other devices are not at risk of being exposed.

Zero Trust Benefits:

- Remove the single point of failure that can be exploited in data breaches.
- Eliminate the need to have trusted devices; all users and connections get verified.
- Contain any potential breaches that do occur by keeping endpoints segmented.

Microsegmentation is a fundamental player in a Zero Trust Architecture and a core feature of the PrinterLogic cloud solution with device segmentation.

Simple, Secure Management Features

Beyond security, there are additional considerations when selecting the right print management solution to incorporate into your Zero Trust strategy. These include everything from centralized management to save your team time and money, to robust features making it easy to secure your printed documents. PrinterLogic has a number of additional features, making it the right choice for every organization moving toward Zero Trust.

PrinterLogic's Output Management solution provides a single point of management and automation that reduces interruptions, improves productivity and efficiency, and protects your data.

Your Zero Trust Printing Checklist:

☑ Access and identity management

☑ Authentication for all connections and endpoints

☑ Segmentation of data to limit harm from breaches

☑ Simple, secure management features

Key Benefits

- Control user permissions, assign drivers, and deploy updates to all devices from a single pane of glass.
- Leverage direct connectors for your Epic, Oracle Health, and SAP systems from the Admin Console.
- Protect printed documents using multiple Secure Release Printing and Pull Printing options.
- Allow users to print without using VPNs or web portals using our Off-Network Printing feature.

Contact our team today for a demo to see how easy Zero Trust Printing can be.

Schedule A Demo