PrinterLogic
a VASION solution

Adopting Zero Trust Printing

Your Guide to a More Secure Future

PrinterLogic
a VASION solution

Table of Contents

SECTION 1

Your Current Network Security Is Failing 03

SECTION 2

What Is Zero Trust? Why Should You Adopt It? 04

SECTION 3

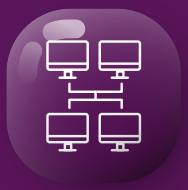
Yes, Print Security Matters 06

SECTION 4

PrinterLogic Checks All the Boxes 08

SECTION 1

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 no longer works in light of the remote work movement. We're in the age of empowering end users out of necessity, but this creates new security vulnerabilities. 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 to 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. Many 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 the year 2026. This would make up roughly a quarter of the U.S. workforce. 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:

- Providing off-network access to end users without opening up holes for vulnerabilities.
- Providing in-person office functions to remote employees, like printing.
- Create new ways for employees to be able to do their jobs on the go with their mobile devices.
- Troubleshooting issues for remote workers.

The increase in cyberattacks due to a distributed workforce has made it difficult for companies to secure their 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.

Remote Work Causes Security Headaches

42%

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

67%

of organizations say BYOD practices weakened their security posture

47%

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

Source: Ponemon Institute

SECTION 2

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.

Zero Trust uses the Principle of Least Privilege (PoLP) which is one of the key tenets of the Zero Trust security model. This process reduces an organization's attack surface since users are only

Full Steam Ahead

78%

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

$38.6 B

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

40%

of all remote access usage will be served predominantly by ZTNA, up from less than 5% at the end of 2020. Source: Gartner

authorized to access necessary applications. Limiting access is perhaps 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 cyberattackers. 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 symbolize that 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

- Endpoints
- Domain Controllers
- Servers
- Business Critical Assets
- Critical Applications
- 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 that 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 amplified these issues and caused companies to seek better ways to secure endpoints and data as employees accessed them through their personal devices in off-site locations. In an Okta survey taken by over 600 global security leaders, 90% said they are

Despite recognizing the importance of Zero Trust and the financial implications of not modernizing network security, companies still struggle to get the ball rolling.

Common Barriers To Adopting Zero Trust

- Budgets are Limited - Initial costs may be a barrier and not everyone has allocated funds just for cybersecurity.
- Change is Difficult - Everyone has to be onboard and ready to make a change from their legacy systems and processes.
- Each Step is Critical - It's important to know your organization's workflows from top to bottom in order to take the proper steps.
- Not Knowing Where to Start - It takes research, resources, and an initial plan to begin executing.

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. It's a continuous effort to keep cyberthreats 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.

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

SECTION 3

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 the conversation of security or Zero Trust comes up. Print security is a small, but critical, component that, if not taken seriously, can wreak serious 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 are left unsecured (Cybernews, 2020). Another instance involved the breach of 150,000 printers by Stackoverflowin, a professional cyberattacker 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 checklist.

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 cyberattackers to come in and steal data.

According to a print security report by Quocirca, over two-thirds (68%) of organizations have experienced data losses due to unsecure 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 a lot of the real security issues lie in using print servers. The increased complexity of print environments make them difficult to maintain and manage. 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 malicious 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 Concerns Are REAL

70%

of organizations expect to increase their print security spend 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% who are concerned about office print security

Source: Quocirca

The Rise of Remote Printing

You may think that remote work would decrease the need to print. 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 recognisable 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 unsecure home printer provides a gateway past any VPN or security. Once a hacker moves from the printer to the company drive, they can browse computer files, or worse, gain access to the company's primary network.

Information stored on the printer's hard drive: Printer hard drives store previously queued print jobs for a varying degree of time. Criminals can use 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. It's where sensitive data flows. And it's one of the easiest endpoints to penetrate. They're also the most costly when a breach does happen ($8.94 million average cost). It's best to leverage a solution that will help you eliminate unnecessary hardware (like print servers), allow you to print securely from anywhere and from 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:

- Bridging the security gap between remote work and organizations
- Simplifying IT print management
- Reducing attack surfaces
- Increasing threat detection and prevention
- Complete visibility into print activity across an organization

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

PrinterLogic
a VASION solution

SECTION 4

PrinterLogic Checks All the Boxes

We get it. Moving from a legacy infrastructure is a daunting task. It takes time, money, and knowledge to begin putting the pieces together. Getting Zero Trust Printing right will reduce your legacy infrastructure and minimize your attack surface, saving you time and money in the long run. With PrinterLogic, you don't have to worry about how we fit into your Zero Trust environment because we inherently have what you need for a Zero Trust Printing solution.

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:

- Your hybrid workforce can print from anywhere with simple verification based on whichever SSO application you use.
- Manage access to applications for employees, contractors and an increasingly remote workforce.
- Our integrations are based on SCIM and JIT provisioning. This allows automatic user creation, saving your team time and money.

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 management makes it easy to ensure that users have the right permissions and connected devices are authorized to access the data they share.

Zero Trust Benefits:

- You eliminate data being stored in the cloud or sitting at rest in a single, centralized location.
- Confidential documents are kept secure at all times while printing.
- Security remains the same for every device and endpoint since our solution is device agnostic.

Your Zero Trust Printing Checklist:

- ☐ Access and identity management
- ☐ Authentication for all connections and endpoints
- ☐ Segmentation of data to limit harm from individual breaches
- ☐ Simple, secure management features

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

Segmentation of Data to Limit Harm From Individual Breaches

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 need for Zero Trust Architecture. Thankfully, device segmentation is a core feature of the PrinterLogic platform. This is possible because PrinterLogic is a cloud solution that offers direct IP printing and is built on the security of AWS.

Simple, Secure Management Features

Beyond security, there are additional considerations for finding the right print management to fit 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 other features that make it a good fit for every organization moving toward Zero Trust.

Additional Benefits:

- Make changes to user permissions as well as deploy device and driver updates to all devices—all from a single pane of glass.
- Enjoy native integrations with other necessary business applications, including EMR solutions, VDI environments, and more.
- Keep your printed documents safe with multiple Secure Release Printing and Pull Printing options.
- Bolster your Zero Trust environment with our Off-Network Printing feature, allowing guests to print without using VPNs or web portals.

Get more from your print management solution. Don't settle for just any Zero Trust Printing platform. PrinterLogic offers everything you need to secure your network while reducing your IT costs and help desk tickets.

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