www.pharos.com

PHAROS CLOUD

Supporting Zero Trust Print Environments

PHAROS

Contents

1 Introduction

Changing work styles and behaviors, and the accelerated shift to remote work since 2020 has created new vulnerabilities for companies, individuals, and their data. A 2021 study conducted by HP[1] found a 238% increase in global cyberattack volume during the pandemic as remote employees were being increasingly targeted by hackers. Not surprisingly, this increase has occurred at the same time that organizations have a reduced ability to mitigate cyber threats.

"As the lines between work and home have blurred, security risks have soared and everyday actions such as opening an attachment can have serious consequences," said Joanna Burkey, Chief Information Security Officer (CISO), HP Inc. "Without all of the pre-pandemic sources of visibility of devices, and how they are being used and by who, IT and security teams are working with clouded vision."

> *"As the lines between work and home have blurred, security risks have soared and everyday actions such as opening an attachment can have serious consequences."*
>
> *Joanna Burkey, Chief Information Security Officer (CISO), HP Inc.*

The impact of a cyber-breach cannot be overstated. Beyond the damage to reputation, IBM's 2021 Cost of a Data Breach[2] study revealed that the average cost to a company from a single data breach rose nearly 10% year over year, from $3.86 million to $4.24 million. As the costs of security breaches continue to increase, so does the sophistication of cyberattacks—forcing companies to think differently about how to protect their data. In addition, at organizations where remote work was a factor in causing the breach, the average total cost of the breach was more than $1 million higher compared to breaches where remote working was not a factor ($4.96 million vs $3.89 million). The increased risk of cyberthreats from a distributed workforce has made it harder for companies to secure their data and infrastructure as critical data is being hosted outside the enterprise firewall.

1 HP Wolf Security. Blurred Lines and Blindspots, 2021.
2 IBM. Cost of a Data Breach Report 2021, Jul. 2021.

2 The Rise of Zero Trust

When it comes to network security, the conventional wisdom was that a secure perimeter—like a moat around a castle—was enough to defend against attackers. But keeping up with sophisticated and evolving threats has become an unending battle. The fundamental problem with the castle and moat approach is that it assumes everyone (and every device) inside the network is a trusted entity. This makes every endpoint on the network—every workstation, every server, every printer, every database—a prime target for attackers. Once an attacker compromises a single endpoint, they are essentially inside the network—inside the moat—and every other node on that network becomes easy prey.

In the traditional network model where the entire network is protected by one verification point (user login credentials or a perimeter firewall), an attacker can leverage the inherent trust of the compromised endpoint to move laterally across the network to access sensitive data.

An important trend was already underway prior to the pandemic to address this changing environment— the increased adoption of a zero trust security framework as the standard for securing corporate networks. Zero trust is more than a singular technology or network topology; it's a comprehensive information security paradigm that initially distrusts all users and all devices.

The premise of zero trust is that no user, device, or application is inherently trusted, even inside the firewall. No user or device can gain access to other network resources without first proving the required level of identification and authentication. This controls lateral movement across the network and reduces the risk of an endpoint being compromised and providing a path to propagate a malicious payload to other endpoints. Zero trust involves the principle of least privilege and several technologies, including policy engines, encryption, endpoint security, and more.

Bad actors are assumed to be inside the network already. But the network remains secure, thanks to an array of technologies and best practices that make it more difficult for hackers to do the kind of damage they have done in the past to data centers and corporate networks.

3 The 7 Tenets of Zero Trust Architecture

Zero trust architecture incorporates the tenets of zero trust into the planning, execution, and maintenance of enterprise infrastructure and related workflows. The National Institute of Standards and Technology (NIST) publishes a set of guidelines to help IT professionals secure their organization's networks and maintain a secure environment using the principles of zero trust. In NIST Special Publication 800-207, Zero Trust Architecture, the 7 tenets of zero trust are outlined.[3]

3 Rose, Scott, et al. (2020) Zero Trust Architecture (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207, August 2020. https://doi.org/10.6028/NIST.SP.800-207

Replacing the conventional network with a zero trust network has helped shift the advantage to the organization rather than the determined hacker, preventing attacks and reducing the impacts of attacks that do occur. According to IBM Security's Cost of a Data Breach Report 2021, the difference in the average total cost of a data breach was $1.76 million lower for mature zero trust organizations ($3.28 million) compared to organizations without zero trust ($5.04 million).

Zero trust doesn't create the network latency issues VPN can cause. It also provides greater flexibility and scalability at much lower cost, especially for remote workforces, which can oftentimes be secured more cost effectively with the less resource-intensive zero trust network architecture than the traditional VPN and firewall. This is a key reason why zero trust principles are being adopted at such an aggressive pace: the zero trust segment alone is expected to be a $51.6 billion market by 2026, growing 17% annually.[4]

4 Research and Markets. *Global Zero Trust Security Market 2021*, Feb. 2021.

4 Securing Print

Print security is a small component of an effective network security strategy—but it's a critical one that's often overlooked despite the fact that hackers view office printers as Internet of Things (IoT) devices connected to a corporate network, and have used them as an attack vector for corporate breaches. Printer-related events have hit the news, including an MIT Technology Review report that Russian hackers are infiltrating companies via the office printer[5], and the 2020 hack of 28,000 printers – fortunately by a team of ethical hackers raising awareness.[6]

How should printing work in this new zero trust world?

To the end-user, the printing experience should remain the same. Behind the scenes, however, it's a different story.

Printing in a zero trust environment means that every device permitted access to the system is managed by the organization with a combination of policy and technology. Print jobs are still submitted as they normally are, from whatever application the employee is using, however, endpoint certificates are validated via two-way authentication before any print traffic is initiated. In addition, all print traffic and network communications occur over secure, encrypted channels.

The zero trust secure print workflow means that any employee who is properly configured in the system can submit print jobs from their workstation or mobile device, from any network location—be it a coffee shop or their home office—and then securely release their documents when it's convenient by going into the office to authenticate, release, and collect the documents, or by enabling an authorized user at the office to print and deliver the documents to a desired location.

In addition to the network architecture, there are many other technologies and policy-based aspects of zero trust that are directly relevant to printing. For example, it's important to disable unsecured protocols like RAW and LPR

5 "Russian Hackers are Infiltratng Companies Via the Office Printer." MIT Technology Review, 5 Aug. 2019, https://www.technologyreview.com/2019/08/05/133880/russian-hackers-fancy-bear-strontium-infiltrate-iot-networks-microsoft-report/.

6 Mathews, Lee. "Nearly A Million Printers At Risk Of Attack, Thousands Hacked To Prove It." Forbes, 31

which have long been the veins through which print data flows. For a print solution to support zero trust, it will need to work without these outdated protocols to keep the data encrypted across the network.

Shifting to zero trust and incorporating secure cloud printing into your print environment enhances security, reduces costs, drives IT productivity, and increases scalability. All the benefits of zero trust security extend to the printing context:

Benefits of Zero Trust Security Architecture

5 Supporting Zero Trust Print Environments

Pharos Cloud is a secure print management platform with a proven track record of supporting the scalability and high-availability requirements of the largest global organizations. The native cloud-based print management solution eliminates costly print servers and ongoing maintenance of vendor-specific print drivers and print queues, and provides control over the day-to-day print operations across the enterprise through intuitive, web-based administration.

Not all cloud-based print management platforms are created equal and able to support zero trust security principles. In fact, only a small number of solutions would permit employee printing to operate in a mature zero trust environment.

Pharos Cloud eliminates the risk of print server vulnerabilities and secures workstation to printer print paths with end-to-end encryption. Its secure-release workflows enhance document security by requiring authentication at the device by the document owner to release the prints—reducing the likelihood sensitive information is left unattended at the printer. In addition, Pharos Cloud delivers a robust and highly-secure cloud service, with an architecture that can address each of NIST's zero trust security principles:

1. **All communication is secured regardless of network location.** Pharos Cloud encrypts data in transit using Transport Layer Security (TLS) between the workstation, printer, and Pharos Cloud. In a secure print workflow, users can submit documents from mobile devices, securely submit a document for print from their home network, and safely release and collect it in the office from any secured device after authenticating. The delivery of print jobs occurs over IPPS to ensure end-to-end encryption of the print stream.
2. **All data sources and computing services are considered resources.** The focus is protecting individual resources rather than network segments. Pharos Cloud acts as the trust broker to securely deliver a printed document from the user's workstation to the network printer.

3. **Access to individual enterprise resources is granted on a per-session basis.**
   Pharos Cloud verifies the user's identity before allowing the user to print. It checks for an identity token and prompts for authentication if one is not valid.
4. **Access to resources is determined by dynamic policy and may include other behavioral attributes.**
   Pharos Cloud reduces the liability of a misplaced employee card by allowing the removal of the ID badge registration. User identities (card numbers, passcodes) are securely stored in the cloud as non-reversable hash values. Encrypted values can be decrypted but hash values cannot.
5. **The enterprise ensures all owned and associated devices are in the most secure state possible and monitors assets to ensure they remain in the most secure state possible.**
   Pharos Cloud does not rely on unsecured protocols such as RAW and LPR printing, and Pharos encourages every customer to disable them and continually verify that they are not in use.
6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.**
   Pharos Cloud verifies that the network printer is the expected endpoint using Simple Network Management Protocol (SNMP) before sending the user's document from the workstation or cloud service to the network printer.
7. **The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture.**
   User workstations check in with Pharos Cloud on startup and at least once per day for a health check. Updates and new settings are automatically applied in a manner similar to endpoint (antivirus) protection software.

Secure cloud printing plays a critical role in this security paradigm—incorporating these principles with Pharos Cloud will help enhance the security of your networks and information. Not all cloud-based print management platforms are created equal and able to support zero trust security principles. In fact, only a small number of solutions would permit employee printing to operate in a mature zero trust environment. For most organizations that rely on the traditional print workflows with print servers and print queues, have not to implemented client authentication for job submission, or still use the unsecure LPR or RAW protocols for job delivery, print would need to be an exception to their zero trust policies. Pharos Cloud is the comprehensive cloud-based print management platform that supports your multi-vendor fleet and enables you to implement a zero trust model without having to disrupt your organization's printing workflows.

6 Next Steps

If your office printers and employee printing workflows are not part of your security strategy, don't wait to change that. According to NextGov, "COVID-19 should prompt enterprises to move quickly to zero trust."[7] This is not about singular technology you can deploy to transform your organization, but a new paradigm for security and the corporate network.

Organizations implement zero trust in a variety of ways, but here are a few must-haves for your zero trust print security checklist:

- Identity and access management, including the separation of the print user identity from the workstation login
- Validation of all communication endpoints (printers, workstations, mobile devices, cloud) before communication is initiated
- Industry best practices for encryption such as zero knowledge encryption (for print jobs stored locally and in the cloud)
- End-to-end encryption of print paths (from workstations to printers)

The security strategy of zero trust has grown in popularity in recent years, as more corporate enterprises abandon traditional organizational strategies that rely on perimeter security. In today's world of lockdowns, health anxiety, remote workers, increasing cybercrime, and too many unknowns to count, zero trust is emerging as the new standard for corporate security and infrastructure.

Pharos Cloud can be configured to complement different implementations of zero trust. Pharos has worked with Fortune 500 companies to provide guidance and solutions expertise to help them enhance the security of their printing operations within their unique frameworks. Pharos continues to lead and innovate in the area of security and encourage IT professionals to prepare for the unknowns of tomorrow.

If you're interested in learning more about Pharos Cloud, visit our website at pharos.com or contact our team at info@pharos.com.

7 Sundra, Ellen. "COVID-19 Should Prompt enterprises to Move Quickly to Zero Trust." Nextgov, 2 April 2020, https://www.nextgov.com/ideas/2020/04/covid-19-should-prompt-enterprises-move-quickly-zero-trust/164309/.

PHAROS

Pharos Systems International, Inc.
4545 East River Road Suite 210, West Henrietta, NY 14586, USA
888-864-7768 (Toll free US/Canada) | info@pharos.com | www.pharos.com