ePRINTit™

SECURE CLOUD PRINTING

Intelligent by Design
Mobile and Remote
Printing/Scanning/Copying

ZERO Trust Printing

WHITE PAPER

By ePRINTit™ | Mar 2025

The term "Zero Trust" was coined by former Forrester Research analyst and thought-leader John Kindervag, He introduced the concept in 2009, emphasizing that trust is a vulnerability and advocating for the principle of "never trust, always verify"

ISO 27001 CERTIFIED by PRESCIENT SECURITY verify

Hidden Agents and Zero Trust Compliance

Many print management solutions and print manufacturers use hidden agents, which are small software components installed on users' computers and printers to enhance the functionality and control of their printing services. These agents can report on various metrics such as toner levels, connectivity status, errors, support needs, and usage for pay-for-click agreements. They can be managed through programs installed on print servers that control where, how much, color enforcing duplex, as well as support your current IDP solution. However, their presence can raise concerns regarding the Zero Trust security model. **It is crucial to avoid deploying print solutions that require direct IP connections** from servers or client devices, as this can introduce significant security vulnerabilities.

Hidden agents often operate with elevated privileges, which can create a security risk if they are compromised**. This implicit trust contradicts the Zero Trust principle of "never trust, always verify."** Users and administrators may not be fully aware of the presence and activities of these hidden agents. The software agents used to monitor your printer can have vulnerabilities that attackers might exploit. If these agents are compromised, they could provide unauthorized access to your printer and potentially your entire network. Therefore, it is essential to implement print solutions that do not rely on direct IP connections, ensuring a more secure and compliant printing environment.

According to a 2024 Verizon Data Breach Report - more than 80% of all attacks involve credentials use or misuse in the network. Printers are often targeted by cybercriminals because they handle sensitive data and have access to network resources. Printers store data from print jobs, which can include sensitive information such as financial records and confidential documents. Attackers can exploit vulnerabilities in printer software to gain access to credentials and other critical information, potentially compromising the entire network.

This lack of transparency can lead to blind spots in security monitoring and control. Hidden agents transmit data back to the manufacturer's servers. If this data is not encrypted or properly secured, it can be intercepted, leading to data breaches and exposure of sensitive information.

Printers with hidden agents are often connected to the internal network. If an attacker compromises the printer, they can use it as a foothold to move laterally within the network, accessing other devices and services.

Famously in 2020, CyberNews conducted an experiment where they hijacked and printed a PDF to 27,944 unsecured printers worldwide to raise awareness about printer security. They found over 800,000 printers with network printing enabled and internet accessibility, indicating a significant number of potentially vulnerable devices. Research indicates that printer-related security breaches are still a pervasive risk. For example, a study by General Prevalence found that 60% of businesses in the UK, US, France, and Germany experienced a print-related data breach in the past year, resulting in significant data losses.

This leads to the importance of always upgrading your printers and print management solutions critical to your business operations when a security patch notification is received. The leading print management solution PaperCut MF/NG had a significant security incident in April of 2023 after releasing a security patch in January for PaperCut servers, where over 2,000 organizations, who had failed to update, were at high risk. These unprotected systems, accessible through the internet, became prime targets for ransomware attacks globally.

To protect against these risks, it's essential to:

Secure Configuration: Immediately change default credentials and configure printers with strong security settings.

- **Regular Updates:** Keep printer firmware and software up to date with the latest security patches. Printers often run on firmware that may have security flaws. If the firmware is not regularly updated, it can be exploited by attackers to gain control over the printer and access stored data.
- **Network Segmentation:** Isolate printers from other critical network resources to limit potential damage from a breach. Secure your Wi-Fi network with strong encryption
- **Monitoring and Logging:** Implement robust monitoring and logging to detect and respond to suspicious activities involving printers.

By taking these steps, organizations can better protect their networks from printer-related security threats.

ZERO Trust Printing

Zero Trust printing is a security approach that ensures every connection and access request is verified, regardless of whether it originates from inside or outside the network. This model is particularly important for protecting sensitive data and preventing unauthorized access to printers and other network devices.

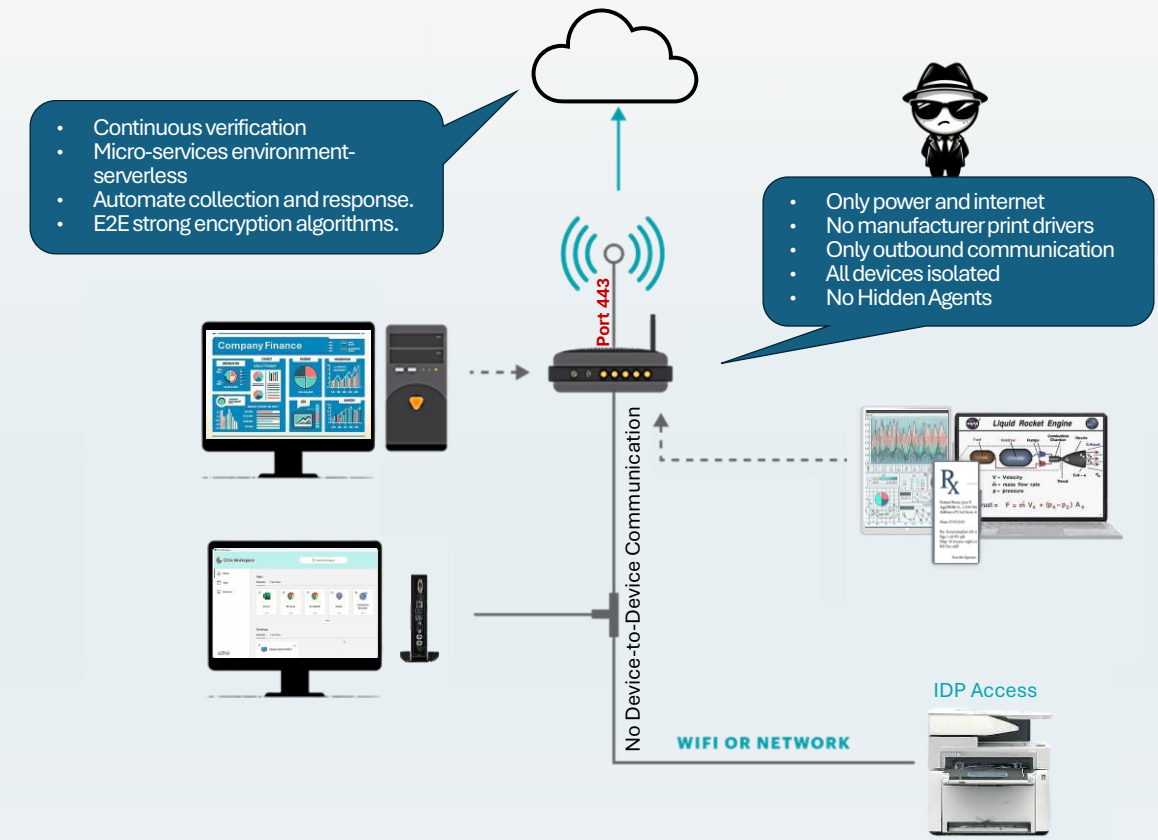
Key aspects of Zero Trust printing:

1. **Authentication and Access Control:** Every user and device must be authenticated before accessing the printer. This can be achieved through password protection, role-based access controls, and revalidation with inactivity timeouts and most important, NO HIDDEN AGENTS found in most trusted print management solutions.
2. **Monitoring and Detection:** Continuous monitoring helps detect potential security threats. Features like whitelisting, firmware verification, and tools such as reCAPTCHA can block brute-force entry attempts.
3. **Containment and Remediation:** In case of a security breach, measures are in place to contain the threat and remediate it swiftly. This includes restricting potential breaches and preventing them from spreading to other devices or the network.
4. **Data Protection:** Data encryption techniques and secure file formats protect stored data. Unnecessary data can be securely deleted using approved algorithms.
5. **Automation:** Automating security policies and updates simplifies management and ensures compliance. This allows security teams to focus on more critical issues.

Implementing Zero Trust Printing: Implementing Zero Trust printing helps organizations maintain a robust security posture while ensuring that only authorized users and devices can access printing resources. Protect confidential documents with secure release and pull printing through Port 443 without jeopardizing your in-house security. Cloud-based SSO and support for multiple authentication methods, such as OpenID Connect, OAuth 2.0, SAML, Google Authenticator, and Authorize.net, further enhance security by providing seamless and secure access to printing resource.

By leveraging cloud-based solutions like ePRINTit SaaS, businesses can overcome the challenges associated with on-premises print solutions and achieve a more efficient, secure, and sustainable print environment.

NO Device-to-Device Communication



March, 2025

Implementing Zero Trust with Microservices

Zero Trust is a security model that assumes no user or device, inside or outside the network, should be trusted by default. Every access request must be authenticated and authorized continuously. This model is particularly effective when combined with microservices architecture supporting a disparate network with several locations being served.

Microservices are a way of designing software applications as a collection of small, independent services that communicate with each other through independent API's. Each service is focused on a specific business function and can be developed, deployed, and scaled independently.

Different microservices can use different technologies best suited for their specific tasks, enhancing overall system performance and security. Microservices can be scaled independently based on demand, ensuring that the printing services remain efficient and responsive even during peak usage. Microservices architecture also allows for centralized logging and monitoring of all services. This provides a comprehensive view of system activities, aiding in quick detection and response to security incidents

Microservices align well with the Zero Trust model, where every access request is authenticated and authorized, regardless of its origin. By leveraging these features, microservices provide a robust framework for protecting printing services within a cloud environment, ensuring security, efficiency, and scalability

CORE Principles of Zero Trust

Isolation and Segmentation:

Each Microservice is an API that is developed, deployed and operated independently , aligning with Zero Trust micro-segmentation.

Compromise of one service doesn't affect others. Each service is responsible for a specific piece of functionality, such as user authentication, payment processing, or data storage.

Deploy microservices in isolated environments with additional isolation and granular control via security groups and network ACLs.

Continuous Verification:

Continuous verification is crucial in modern security, protecting hybrid environments of cloud and on-premise systems and helping to prevent lateral movement within the Network.

Requiring user authentication through Identity Providers (IDPs), Single Sign-On (SSO), or equivalent mechanisms to ensure only authorized access.

Configured to verify and authenticate each request, ensuring continuous identity verification.

Least Privilege Access:

Each microservice has Granular Access Control with only the permissions it needs, minimizing unauthorized access risk, supporting continuous verification.

By isolating services, Least Privilege Access ensures that even if one microservice is compromised, the impact is contained.

Implementing Least Privilege Access makes it easier to comply with regulatory requirements and conduct audits. Each service's access can be documented and reviewed, ensuring compliance with security policies.

Enhanced Monitoring & Analytics:

Centralized Logging utilizes tools to collect and analyze logs from all microservices, providing a comprehensive view of system activities. This centralized approach aids in quick detection and response to security incidents, ensuring anomalies are promptly addressed.

Integrates with real-time monitoring and alerting systems. This integration allows for automated responses to potential threats, enhancing the overall security posture by ensuring immediate action when necessary

Zero Trust Network Access (ZTNA) in a SaaS model:

Increased Adoption

Zero trust is rapidly becoming the standard security model for enterprises. By 2025, it's expected that 70% of new remote access deployments will rely on Zero Trust Network Access (ZTNA) rather than traditional VPNs1. This shift is driven by the need for more robust security measures in an era where remote work and cloud services are prevalent.

SASE Integration

Secure Access Service Edge (SASE) platforms are gaining traction as they offer a unified, cloud-native solution that integrates zero trust principles. SASE combines network security functions with wide area networking (WAN) capabilities, providing secure access regardless of location2. This integration helps organizations manage security more efficiently and effectively, especially with the increasing complexity of IT environments3.

Regulatory Pressures

Businesses face growing regulatory pressures to adopt zero trust architectures. Compliance with stringent privacy laws, such as GDPR and HIPAA, and the need to mitigate geopolitical risks are significant drivers4. Zero trust principles align well with these regulations by ensuring continuous verification and strict access controls, thereby protecting sensitive data and reducing the risk of breaches5.

Platformization

The trend towards platformization in cybersecurity involves consolidating multiple security tools and processes into a single, unified platform. This approach enhances visibility, streamlines operations, and improves efficiency by enabling seamless communication among security components. Organizations adopting this strategy report better integration across security, hybrid cloud, AI, and other technology platforms, which helps reduce complexity and operational costs7.

These trends underscore the growing importance of zero trust and SaaS models in modern cybersecurity, highlighting the need for continuous adaptation and integration of advanced security measures.

Enhancing Microservices Security with SASE

Secure Access Service Edge (SASE) significantly enhances security in a microservices environment. Microservices can significantly enhance the security and efficiency of printing services within a cloud environment. By isolating each service, microservices ensure that if one is compromised, it doesn't affect the others, thus minimizing the attack surface. This isolation also supports fault containment, enhancing system resilience.

Implementing granular access control and role-based access control (RBAC) ensures that each service operates with the minimum necessary permissions, reducing the risk of unauthorized access. Centralized logging and real-time monitoring provide comprehensive visibility into system activities, enabling quick detection and response to security incidents. Additionally, microservices allow for dynamic scaling based on demand, ensuring efficient and responsive printing services even during peak usage. The architecture supports continuous verification, with each service independently authenticating and authorizing access requests, aligning well with the Zero Trust model.

By leveraging these features, microservices provide a robust framework for protecting printing services within a cloud environment, ensuring security, efficiency, and scalability.

Network Dependency - Hacking your Printer

While printers might seem like unlikely targets for hackers, they can be a weak point in a network's security. Printers are typically connected directly within an organizations network as opposed to a SaaS model which would be a direct internet printing model with no network dependency, configurations and firewall rules. Here's how a determined hacker could potentially gain access to a printer, even with a firewall in place:

1. Printer Vulnerabilities:

- Outdated Firmware: Exploitable security holes in older printer software.
- Default Credentials: Easy-to-guess usernames/passwords grant access.
- Network Protocols (SMB/SNMP): Vulnerabilities in communication protocols.
- Direct IP Connections: Direct IP connections to printers can be exploited by attackers to gain unauthorized access, potentially compromising the entire network

2. Social Engineering:

- Phishing: Tricking employees with malicious links/attachments.
- Insider Threats: Compromised employees providing access.

3. Firewall Bypass:

- Port Forwarding: Exploiting open internet access to the printer.
- Protocol Tunneling: Hiding malicious traffic within legitimate traffic.
- Zero-Day Exploits: Exploiting unknown vulnerabilities before patches are available.
- Inbound Connections: Allowing inbound connections to printers can expose them to external threats, making it easier for attackers to exploit vulnerabilities and gain access to sensitive data

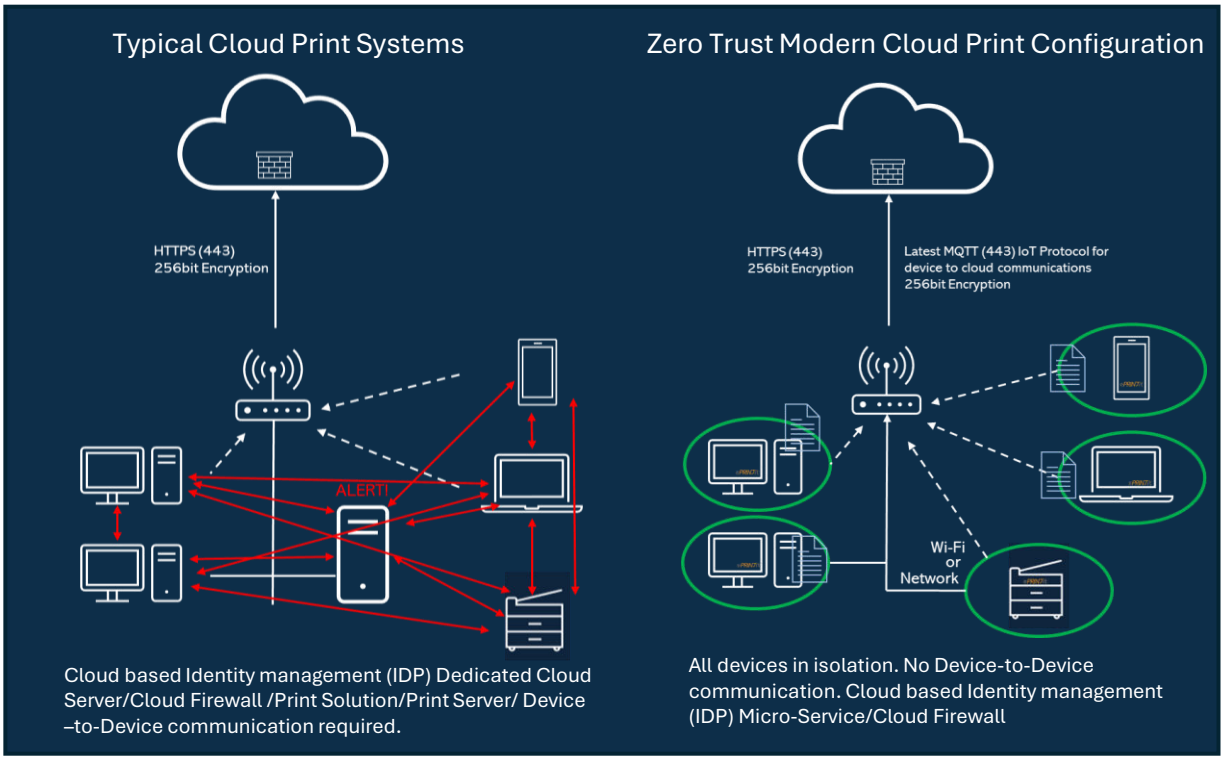
4. Using Printers as a Pivot:

- Install Malware: Monitoring network traffic, stealing data, launching further attacks.
- Gaining control of connected servers/workstations. Prime weakness for hidden agents.
- Denial-of-Service Attacks: Disrupting network services.

Mitigation:

- Don’t deploy print solutions that require client devices or servers to have direct IP connections
- No inbound traffic or port exceptions to printers
- Update Firmware: Patching vulnerabilities in both a print management solution as well as a printer.
- Change Default Passwords: Securing access.
- Network Segmentation: Isolating printers.
- Strong Passwords: For all devices.
- Monitor Traffic: Detecting suspicious activity.
- Printers would have a direct, secure internet connection.
- The SaaS platform communicates directly with the printers over encrypted channels (HTTPS, TLS).
- Printers would be configured to accept print jobs only from the authorized SaaS platform
- Employee Education: Preventing social engineering attacks.

Isolate Printers and Print Management



Conclusion

By leveraging microservices in AWS EC2 and Lambda, ePRINTit can effectively implement a Zero Trust architecture. This combination ensures isolation, continuous verification, least privilege access, and enhanced monitoring, all of which are core principles of Zero Trust.

Consider ePRINTit Hosted in your Environment

At ePRINTit, we take security seriously. Our cloud-based solution, hosted with 100% microservices architecture, prioritizes data protection, regulatory compliance, and robust identity and access management (IAM). We rigorously evaluate our authentication methods to prevent unauthorized access, implement fine-grained access controls, and use encryption in transit and at rest to safeguard sensitive information. Our mobile apps employ strong authentication mechanisms, and all data transmitted between the mobile app and our cloud services are encrypted. We manage app permissions carefully and follow best practices for data storage, including redundancy and automated backups. Additionally, we assess third-party integrations for security risks and ensure compliance with industry standards and data protection laws. Ensure to ask us for our detailed whitepaper on our solution's security.

- Robust authentication methods (IDP's)
- Role-based access limits user privileges.
- Encryption in transit (HTTPS) and at rest (256 RSA)
- Strong authentication mechanisms, SSO and MFA
- Secure protocols prevent eavesdropping TLS 1.2/3
- App Permissions: Microsoft Intune approved
- Data Storage: Redundancy, automated backups, automated destruction
- Strong cryptographic algorithms for sensitive data
- Third-Party Integration Security
- Compliance: Adherence to industry standards (ISO 27001-2022 Certified, NIST) and data protection laws (GDPR, CCPA)

Reference Material

What are Microservices? | AWS
Microservices Architecture: Meaning, Examples & Diagrams
Microservices Security: How to protect your architecture - Atlassian
CyberNews - 28000 printers hacked
LMG Security how criminals hack your printers
CISO MAG – 60% of firms suffer data loss due to printer security
PaperCut Security post-incident April 2023
US Cybersecurity & Infrastructure Agency Malicious Actors Exploit CVE-2023-27350 in PaperCut
Ogma Published 08-03-2024 CVE-2023-35833 identifies a significant security vulnerability in the YSoft SAFEQ 6 Server
CrowdStrike - Zero Trust Security
Harvard Business Review – The devastating impacts of a cyber breach May 4, 2023

Technology Partners and IdPs

Copyright Mar 2025_2026 "All trademarks and logos are the property of their respective owners. The inclusion of these trademarks and logos does not imply endorsement, sponsorship, or affiliation with ePRINTit. ePRINTit and its products are not affiliated with or endorsed by any of the trademark owners." For detailed information on sustainability factors please contact us for more information.

March, 2025

ePRINTit USA, LLC.
7820 S Quincy St,
Willowbrook, IL,
60527
Toll-free Number:
877-494-0443
General Email:
info@eprintit.com

ISO/IEC 27001:2022 CERTIFIED