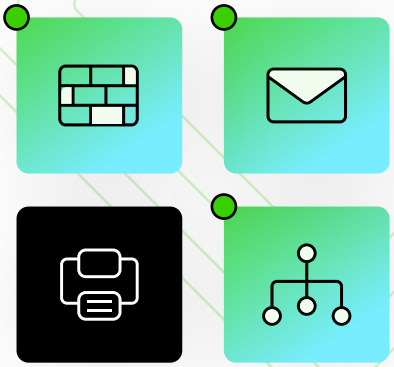
tricerat®

The Print Security Paradox

83 Vulnerabilities and the Collapse of Convenience-First Print Architecture

A guide for leadership on transforming a legacy utility into a fortified security pillar.

The Invisible Attack Surface



When it comes to protecting your systems and data, it's common practice to harden the network perimeter, secure email, and deploy sophisticated endpoint protection. Yet, a massive strategic blind spot remains: your print infrastructure. Long treated as a mere IT utility, print management has quietly evolved into a primary attack vector for lateral movement and data exfiltration.

Recent disclosures have shattered the myth that serverless or cloud-hosted print is inherently safer. The discovery of 83 critical vulnerabilities in a leading print management provider reveals a systemic failure of convenience-first print solutions. For organizations in regulated sectors like healthcare, finance, and government, these flaws are not just bugs - they are structural risks that can lead to cross-tenant data breaches and unauthenticated remote code execution (RCE).

This paper outlines the strategic mandate for moving beyond tactical admin tools toward a fortified Hybrid Print Architecture (HPA) that prioritizes data sovereignty and identity-centric controls.

Background: The Pierre Kim Disclosure

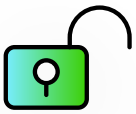
The alarm was sounded by renowned security researcher Pierre Kim, who disclosed one of the most extensive collections of security flaws ever found in an enterprise print solution. His research, spanning four years (2021-2024), targeted the Vasion Print (formerly PrinterLogic) product.

The findings were staggering. Kim identified 83 vulnerabilities affecting every component of the ecosystem, including Windows, MacOS, and Linux clients, as well as Virtual Appliance and SaaS deployments. Perhaps most concerning was the timeline for remediation: the vendor took over three years to provide even incomplete patches, and as of December 2025, at least four critical vulnerabilities remained unpatched.

Anatomy of a Systemic Failure

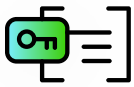
The vulnerabilities found by Kim represent fundamental architectural weaknesses throughout Vasion Print's serverless offering.

Unauthenticated Remote Takeover: Attackers could gain root access to entire infrastructures without a single credential, allowing them to intercept print jobs or move laterally into the corporate network.



The "Secret" Backdoor (CVE-2025-34217): A hardcoded SSH key was discovered that provides immediate root access to Virtual Appliances with passwordless sudo privileges.

Cross-Tenant Data Breaches: In SaaS environments, unauthenticated attackers could retrieve cleartext passwords and sensitive data belonging to other customers (tenants) due to a lack of server-side validation.



Hardcoded Secrets: Developers left AWS secret access keys, Mailgun credentials, and OKTA private keys embedded in plaintext within the application code, creating a massive supply-chain risk.

The Structural Flaw: Why "Serverless" Often Means "Unsecured"

Many organizations moved to serverless print management to reduce IT overhead. However, this shift often inadvertently outsourced risk rather than eliminating it.

When print management is purely cloud-based, sensitive document metadata - and sometimes the data itself - leaves the secure corporate perimeter. The Vasion disclosure proves that multi-tenant SaaS models can fail to maintain strict isolation, allowing one compromised tenant to impact others. Furthermore, total reliance on a vendor's cloud creates a single point of failure; if the ISP or the vendor's infrastructure goes down, mission-critical printing stops.

A Strategic Framework for Zero Trust Print Security

To defend against these threats, organizations must apply Zero Trust principles to their print infrastructure:

Data Sovereignty

Print data and spool files must remain within the organization's secure network or on-premises whenever possible to eliminate cross-tenant risks.

Identity-Centric Access

No user or device should be trusted by default. Every print job must be authenticated, utilizing Hold and Release and PIN Printing to ensure physical output only occurs in the presence of an authorized user.

Immutable Accountability

Comprehensive audit trails must capture every print event - who, what, when, and where - to satisfy regulatory mandates like HIPAA, SOX, and GDPR.

The Tricerat Advantage: A Fortified Architecture, From the Ground Up

Tricerat's approach to print management is built on the philosophy that security is a product of intentional architecture. Unlike convenience-first tools, Tricerat's ScrewDrivers platform utilizes a fortified Hybrid Print Architecture (HPA) to protect organizations from the types of vulnerabilities discovered in the Vasion disclosure.

Fortified Print Servers & Data Isolation

While legacy servers are vulnerable, Tricerat deploys Fortified Print Servers - hardened, high-availability environments designed for mission-critical workloads. By keeping print data within your secure perimeter, Tricerat eliminates the risk of cross-tenant leaks inherent in SaaS-only models.

Proprietary TMF Format vs. Malicious Code

Tricerat does not send raw, executable files across the network. Instead, it uses a proprietary TMF format that interprets data rather than executing code. This effectively neutralizes many common network attack vectors used for Remote Code Execution (RCE).

The Universal Driver: Eliminating “Driver Hell”

One of the most common entry points for vulnerabilities is the constant uploading of unvalidated third-party drivers. Tricerat virtualizes the print process through a patented universal driver, eliminating the need for unmanaged drivers on every endpoint and reducing the attack surface significantly.

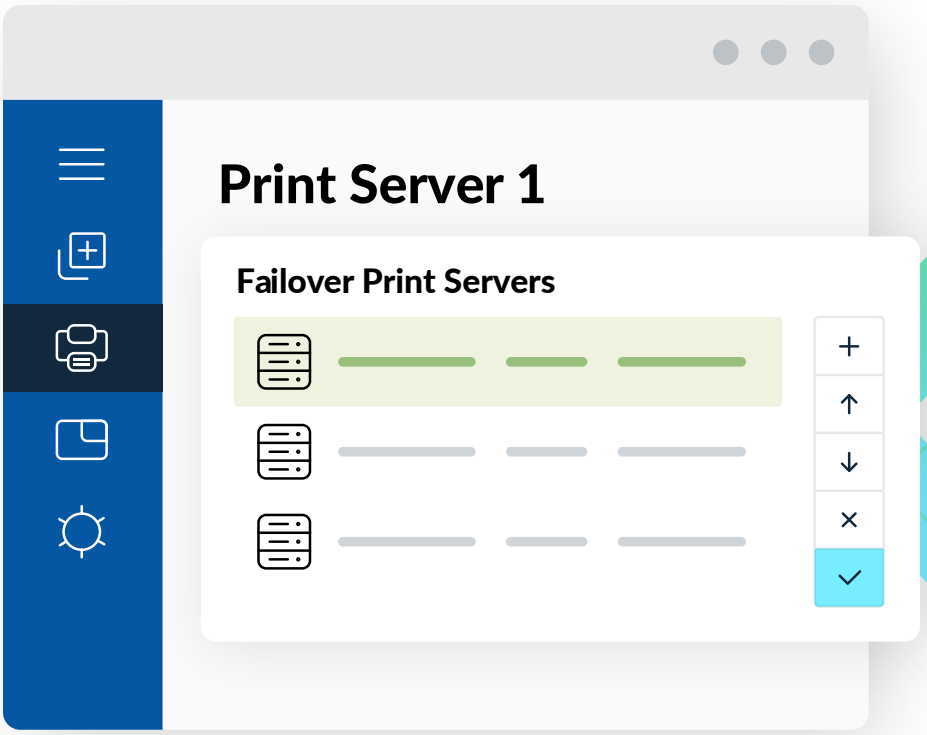
True Zero Trust Enforcement

ScrewDrivers integrates directly with your existing Active Directory to enforce the principle of least privilege. Users only see the printers they are authorized to use, and every job requires explicit verification through secure hold-and-release mechanisms.

Moving from Utility to Strategic Asset

The discovery of 83 vulnerabilities in Vasion Print’s serverless print management product is a wake-up call for the enterprise. Print infrastructure can no longer be ignored as a minor utility. Instead, it must be architected for resilience, compliance, and security.

By transitioning to a Hybrid Print Architecture (HPA), organizations can reclaim their data sovereignty, eliminate backdoors, and ensure that their most sensitive documents and data remain exactly where they belong: under their own control.



The Print Architecture Security Checklist

C-level leaders and IT directors can use this checklist to evaluate their current print security posture and ensure their architecture meets modern security standards.

- [ ] **Eliminate Hardcoded Backdoors:** Audit all virtual appliances for hardcoded SSH keys or default credentials that could provide root access to your infrastructure.
- [ ] **Enforce Data Sovereignty:** Ensure that print spool files and sensitive document metadata never leave your secure perimeter or enter multi-tenant cloud environments.
- [ ] **Implement Secure Output Orchestration:** Deploy Hold and Release or PIN-based printing to ensure documents are only printed when the authorized user is physically present at the device.
- [ ] **Adopt Universal Driver Virtualization:** Reduce the attack surface by removing third-party printer drivers from endpoints and replacing them with a single, secure universal driver.
- [ ] **Apply Zero Trust Access Control:** Integrate print management with Active Directory to ensure users only see and use printers they are explicitly authorized to access.
- [ ] **Harden Data in Transit:** Verify that all print-related communications use TLS 1.2+ encryption and that outdated, vulnerable protocols like SSL 3.0 are blocked.
- [ ] **Establish Immutable Audit Trails:** Log comprehensive metadata for every print event - including user identity, document name, and timestamps - to meet regulatory compliance requirements like HIPAA, SOX, and GDPR.
- [ ] **De-Risk SaaS Dependencies:** Ensure your architecture can continue to function during ISP or vendor outages by using local, fortified print servers for mission-critical sites.
- [ ] **Validate Administrative Permissions:** Use tiered, Role-Based Access Control (RBAC) to ensure IT staff only have the specific permissions needed for their role.

Book a free review of your print security posture

Tricerat's Hybrid Print Architecture experts provide a free, vendor-neutral consultation and review of your existing print environment.

Schedule a Free Review

tricerat®