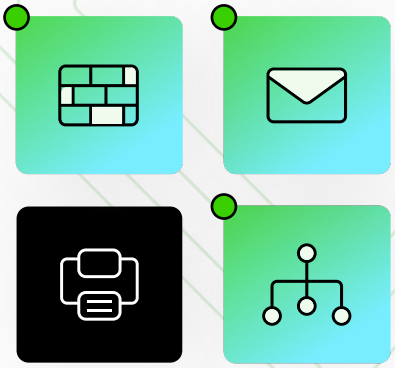
tricerat®

The Serverless Print Trap

Why Eliminating Print Servers Outsources Risk.

A Strategic Guide to Repatriating Control with a Hybrid Print Architecture

Critical Flaws of Serverless



For the last decade, the enterprise IT narrative has been dominated by a single, seductive promise: Delete your infrastructure. In the realm of print management, this manifested as the serverless movement – a push to eliminate your print servers and replace them with Direct IP printing managed by third-party cloud SaaS platforms. The value proposition was simple: reduce hardware costs, eliminate maintenance, and simplify the stack.

However, data from a decade of serverless adoption has revealed a critical flaw in this logic. By eliminating local infrastructure, organizations didn't eliminate risk; they simply outsourced it to a black box they could not control.

Recent security disclosures from 2021–2025 have laid bare the dangers of this model. Security researchers have identified 83 systemic vulnerabilities in leading serverless platforms, ranging from unauthenticated remote code execution to cross-tenant data breaches. Simultaneously, the rise of Cloud Repatriation – where 86% of CIOs are moving workloads back on-premises – signals a market correction (Barclays, 2024).

This white paper explores the reasons why the era of Serverless is ending, and what you need to know to be prepared for what's next. In an age of Zero Trust and operational resilience, the most secure enterprises are moving toward Hybrid Print Architecture (HPA) – a model that fortifies, rather than eliminates, the infrastructure that powers mission-critical workflows.

The Serverless Seduction

The Serverless trend was born from a desire for efficiency. Traditional print servers were viewed as costly, maintenance-heavy hardware that required constant patching. The promise of Direct IP printing managed by a cloud portal offered an alluring alternative: a single pane of glass to manage thousands of printers without a single local server.

However, this convenience came with a hidden trade-off: control.

When an enterprise moves to a serverless SaaS model, it trades the known management overhead of local servers for the unknown security posture of a vendor. As reliance on these platforms grew, so did the risks:

1. Loss of Data Sovereignty:
Print metadata and credentials began traversing public clouds.
2. Operational Fragility:
Printing became dependent on internet connectivity and vendor uptime.
3. Supply Chain Opacity: Organizations lost visibility into the code running on their endpoints.

Today, the tide is turning. According to recent research from OpenText cited in TechTarget, 87% of CIOs are planning to repatriate workloads from the public cloud back to private infrastructure.

The risk is not theoretical. The broader IT ecosystem has already seen how centralized cloud failures and supply chain weaknesses can paralyze entire industries for days or weeks, and print is no exception. When badge readers, follow-me queues, and clinical output all depend on a vendor's cloud and upstream identity path, print stops being a quiet utility and becomes a critical attack surface. The drivers are clear: unpredictable costs, data sovereignty requirements, and the need for operational resilience that cloud services cannot guarantee.

Anatomy of a Collapse – The Risks of No Print Servers

87%

of CIOs are planning to repatriate workloads from the public cloud back to private infrastructure.

"Plan for Repatriation on Day One with a Hybrid Cloud Strategy," TechTarget: SearchCloudComputing, December 11, 2025

When organizations dismantle their local print infrastructure in favor of cloud-dependent serverless agents, they introduce three catastrophic risk vectors.

The Cross-Tenant Nightmare

In a multi-tenant SaaS environment, your security is only as strong as the vendor's isolation logic. If a vendor's cloud architecture is breached, the attacker doesn't just gain access to one company;

they potentially gain access to every company on the platform.

The Consequence: A breach in a serverless management layer can allow attackers to pivot from the vendor's cloud directly into your internal network. As seen in the 2024 Change Healthcare breach3, centralized cloud failures can cripple entire industries for days or weeks.

The Offline Fallacy

The most immediate operational risk of serverless printing is the Internet Dependency Loop. While some solutions claim to keep printing offline, the management plane often resides in the cloud.

The Cost: In healthcare, downtime costs an estimated $7,900 per minute (Taylor,2025). If an ISP outage or a vendor cloud failure prevents a badge reader from authenticating a user, clinical workflows halt. Serverless agents often lack the robust, offline redundancy of a fortified local server.

Compliance & Sovereignty Gaps

For regulated industries (Healthcare, Government, Finance), Data Sovereignty is non-negotiable.

The Trap: Many serverless solutions route metadata – and occasionally print job data – through public cloud infrastructure. This creates a compliance nightmare for HIPAA and GDPR, as organizations cannot definitively prove that sensitive data remained within their secure perimeter at all times.

The Wake Up Call: 83 Points of Failure

The theoretical risks of serverless architecture became terrifyingly real between 2021 and 2025. Security researchers disclosed 83 critical vulnerabilities in a leading serverless print management platform (Vasion Print/PrinterLogic), exposing a pattern of systemic security negligence. These were not minor bugs. They were structural failures in the serverless model.

The Hardcoded Backdoor (CVE-2025-34217)

Researchers discovered a hardcoded SSH public key for a PrinterLogic user account embedded in the Virtual Appliance. This account had root privileges via a passwordless sudo rule.

The Risk: Any attacker with the matching private key could gain immediate, undetectable root access to the appliance. This is a textbook supply chain vulnerability – a master key left under the doormat of thousands of enterprise networks.

Cross-Tenant Data Leaks (CVE-2025-27648)

In the SaaS environment, researchers found that unauthenticated attackers could retrieve cleartext passwords belonging to customers in different tenants simply by querying an API.

The Risk: This shattered the illusion of tenant isolation. A malicious actor could harvest credentials from other companies sharing the platform, leading to massive downstream breaches.

Unauthenticated Remote Code Execution (CVE-2025-34215)

Attackers could upload malicious firmware to the appliance without authentication, achieving Remote Code Execution (RCE) with root privileges.

The Risk: This provided a roadmap for ransomware operators to turn print infrastructure into a beachhead for lateral movement across the corporate network.

The Takeaway

The vendor took over three years to patch some of these issues, with several critical vulnerabilities remaining unpatched as of late 2025. This proves the fundamental danger of the trap: When you use Serverless SaaS, you inherit the vendor's security culture. If they fail, you fail.

Why Hybrid Print Architecture Wins

The industry is moving beyond the binary choice of Unmanaged Legacy Servers vs. Risky Serverless SaaS. The new standard for enterprise resilience is Hybrid Print Architecture (HPA).

What is Hybrid Print Architecture?

HPA is a unified framework that combines the best of both worlds, providing a unified & fortified solution consisting of fortified print servers, direct IP zones, under a unified control plane.

1. Fortified Print Servers: Hardened, high-availability instances deployed on-premise for mission-critical sites (Hospitals, HQs).

2. Direct IP Zones: Serverless-style connections for distributed, low-risk branch offices.

3. Unified Control Plane: A single pane of glass for policy enforcement across your entire estate.

This approach provides a solution that is architected for your hybrid reality. You keep the convenience of central management, but you repatriate the control of your data and security back to your own perimeter.

How Tricerat De-Risks the Enterprise

Tricerat's ScrewDrivers® platform is the industry's defining Hybrid Print Architecture (HPA) solution. It is purposefully engineered to neutralize the risks inherent in serverless models while delivering the efficiency IT leaders demand.

The future of enterprise printing is not Serverless. It is Fortified. It's time to escape the serverless print trap. By adopting a Hybrid Print Architecture, organizations can regain control of their data, ensure 99.9% resilience, and turn their print infrastructure from a liability into a strategic asset.

Data Sovereignty: Audit all virtual appliances for hardcoded SSH keys or default credentials that could provide root access to your infrastructure. Unlike serverless competitors that require data to traverse their cloud, Tricerat allows for 100% on-premises data processing. Your print jobs, metadata, and Active Directory credentials never leave your firewall. This eliminates the risk of cross-tenant breaches and ensures intrinsic compliance with HIPAA, GDPR, and FedRAMP.

Fortified Print Servers: True Offline Resilience
For environments where downtime is measured in lives or revenue, reliance on an internet connection is unacceptable. Tricerat utilizes Fortified Print Servers – hardened, local instances that ensure printing continues even if the internet goes dark. This provides the redundancy required for healthcare and government sectors, ensuring that a cloud outage never becomes a clinical outage.

Identity-Centric Zero Trust
Tricerat integrates natively with your existing identity provider (Active Directory/Entra ID) using Kerberos ticket-based authentication. We do not use hardcoded backdoors or shared keys. Every print job is authenticated against your directory, ensuring that users only see and access the printers they are explicitly authorized to use. Hold-and-Release workflows further ensure that sensitive documents are never left unattended.

How Tricerat De-Risks the Enterprise

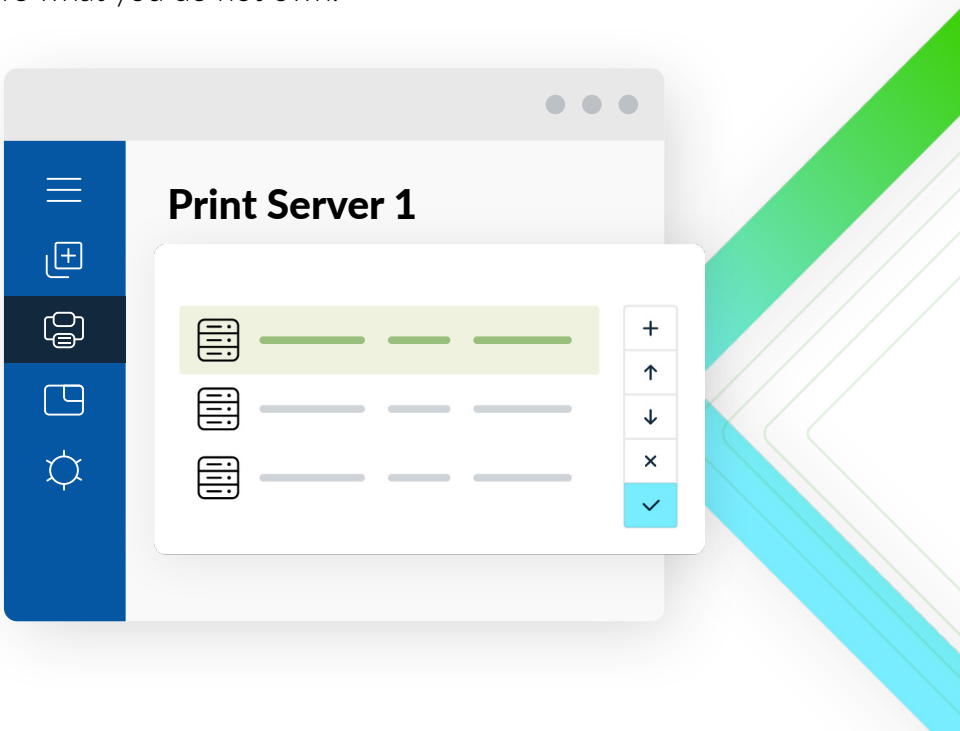
Identity-Centric Zero Trust
Tricerat integrates natively with your existing identity provider (Active Directory/Entra ID) using Kerberos ticket-based authentication. We do not use hardcoded backdoors or shared keys. Every print job is authenticated against your directory, ensuring that users only see and access the printers they are explicitly authorized to use. Hold-and-Release workflows further ensure that sensitive documents are never left unattended.

Supply Chain Transparency
ScrewDrivers operates as a plug-in within existing secure protocols (Citrix ICA, Microsoft RDP, Omnissa PCoIP) rather than acting as a standalone executable that opens new attack vectors. By interpreting data rather than executing code, and by blocking deprecated encryption protocols, Tricerat reduces the attack surface significantly compared to bloated serverless agents.

Stop Choosing, Start Architecting

The last decade taught us that convenience at the expense of control is a debt that eventually comes due. The disclosure of 83 systemic vulnerabilities in serverless platforms is the final warning: You cannot secure what you do not own.

The future of enterprise printing is not serverless. It is Fortified. It's time to escape the serverless print trap. By adopting a Hybrid Print Architecture, organizations can regain control of their data, ensure 99.9% resilience, and turn their print infrastructure from a liability into a strategic asset.



Ready to secure your infrastructure?

Request a Free Architecture Assessment. Stop guessing about your risk profile. Tricerat's architects will analyze your environment and design a Hybrid Print Architecture blueprint tailored to your specific security and compliance needs.

Book Your Free Assessment

tricerat®

End Notes

1. Barclays. Technology: 1H24 CIO Survey – 2024 Outlook Sustained. Barclays Equity Research, CIO Survey Program, October 7, 2024.
2. "Plan for Repatriation on Day One with a Hybrid Cloud Strategy," TechTarget: SearchCloudComputing, December 11, 2025
3. Nixon Peabody LLP, "The Change Healthcare Cybersecurity Breach: Impact on Health Care Providers," client alert, November 11, 2025, accessed February 13, 2026.
4. Taylor Corporation, "How To Manage EHR Downtime Costs," August 25, 2025