tricerat | SCREWDRIVERS®

WHITE PAPER

WHITE PAPER

The Enterprise Print Decision

Three paths, one defensible answer.

A strategic guide for IT and security leaders evaluating enterprise print management — the real trade-offs between doing nothing, removing your print infrastructure for a serverless model, or adopting a Hybrid Print Architecture.

OPTION A	OPTION B	OPTION C · RECOMMENDED
Do Nothing	**Go Serverless**	**Hybrid Print Architecture**
Scripts, GPOs, stacked drivers. The risk stays and grows.	Outsource print to the cloud. Trade known overhead for unknown risk.	Fortify what matters, unify the rest. Pays for itself in Year 1.

WHAT'S INSIDE

Contents

ABOUT THIS PAPER

Every enterprise running on-site or distributed printing faces the same decision — and it usually surfaces at a renewal, a security audit, or a cloud-migration project. This paper lays out the **only three credible paths**, the evidence behind each, and the math that makes one of them defensible.

EXECUTIVE SUMMARY

Three credible paths

Every enterprise running on-site or distributed printing faces the same decision, and it usually surfaces at a renewal, a security audit, or a cloud-migration project. There are only three credible paths and only one holds up on security, resilience, and ROI.

A Do Nothing

STATUS QUO

Treat printing as a minor utility: legacy scripts, GPOs, and stacked vendor drivers. No new license cost, but the operational drag and the open attack surface stay — and grow over time.

B Remove the Print Infrastructure

SERVERLESS / CLOUD-ONLY

Eliminate the print servers and outsource to a serverless / cloud-only platform. It promises lower hardware cost and a single cloud console — but it trades known overhead for an **unknown vendor security posture**, internet dependency, and data-sovereignty gaps.

C Consolidate, Secure, and Optimize

RECOMMENDED

Keep control of print where it matters, fortify the infrastructure, unify it under one console, and add Zero Trust security and a per-user audit trail with a Hybrid Print Architecture (HPA). You keep the convenience of central management while repatriating control of your data and uptime. This is the option that holds up on security, resilience, and ROI — and it pays for itself inside Year 1.

THE BOTTOM LINE Organizations don't have to choose between unmanaged legacy servers and a risky serverless black box. **A Hybrid Print Architecture fortifies what matters and unifies the rest** — and the value can be proven across an entire estate in a four-week trial.

WHY NOW

Why print became a security & resilience problem

Most organizations still treat print as a quiet IT utility. That assumption is exactly why it has become a primary attack vector and an operational liability. **Three forces converged in 2025** to change the conversation.

53
Print Spooler CVEs disclosed since PrintNightmare (2021)

83
vulnerabilities in one serverless print platform, April 2025

86%
of CIOs now plan to repatriate workloads on-premises

56%
of orgs suffered a print-related data loss in the past year

Print is now a named, repeatable attack surface

Print drivers and spoolers run with SYSTEM-level privileges. Microsoft has disclosed roughly **53 Print Spooler vulnerabilities since the 2021 PrintNightmare disclosure** — a continuous stream of privilege-escalation and RCE flaws. Every stacked vendor driver is another privileged loading path to track and patch.

"Serverless" print did not eliminate risk — it outsourced it

In April 2025 researcher Pierre Kim published **83 vulnerabilities in Vasion Print (formerly PrinterLogic)** — including a hardcoded SSH backdoor (CVE-2025-34217), cross-tenant data leaks (CVE-2025-27648), and unauthenticated RCE (CVE-2025-34215). At least four critical vulnerabilities remained unpatched as of December 2025. When print lives in a multi-tenant cloud, you inherit the vendor's security culture.

The market is already pulling control back on-premises

86% of CIOs now plan to move at least some workloads from public cloud back to private or on-prem infrastructure (Barclays) — the highest rate on record — and TechTarget reported **87%** plan to repatriate. Flexera found 21% of workloads already repatriated. The cloud-only era is correcting, and print should follow.

The cost of getting it wrong is measurable

Healthcare EHR downtime runs ~**$7,900 per minute** (over $25K for large hospitals); a seven-hour AWS outage in October 2025 disrupted operations nationwide. Quocirca found **56%** of organizations suffered a print-related data loss last year — multi-vendor fleets averaging £937K per breach. And print is roughly **23% of IT tickets**.

> ***WHY THIS MATTERS NOW - The 83-CVE vulnerabilities disclosure and the cloud-repatriation data reframe print from a commodity refresh into a security and resilience decision — one that carries executive sponsorship and budget.***

THE THREE OPTIONS · PART 1

The two paths that leave you exposed

Two of the three options feel safe for different reasons — one is free, the other is simple. Both leave the organization carrying risk it can't see or can't audit.

A Do Nothing — Stay on Scripts & GPOs

WHY IT FAILS

What it is: Keep mapping printers with PowerShell, VBScript, and per-site GPOs, with stacked vendor drivers on every workstation. It feels free, it "works today," and nobody owns the problem until something breaks or an auditor asks.

- ✕ **Open attack surface**
  Every stacked vendor driver is a privileged loading path against the PrintNightmare class of vulnerabilities.
- ✕ **Patch sprawl**
  A typical site runs 10–15 vendor drivers per workstation — dozens of independent CVE response paths.
- ✕ **No central audit trail**
  Who printed what, where, and when is scattered — no per-user attribution for HIPAA, SOX, or GDPR.
- ✕ **Brittle and slow**
  Logon scripts run synchronously, so users wait and the helpdesk takes the calls.

THE REALITY **Doing nothing isn't free — the cost is already being paid in helpdesk hours and unpatched risk. It's simply hidden until an audit or an incident makes it visible.**

B Remove the Print Infrastructure — Serverless / Cloud-Only

WHY IT'S A TRAP

What it is: Eliminate the print servers and replace them with Direct IP printing managed by a third-party cloud SaaS platform. The pitch is clean — reduce hardware, eliminate maintenance, manage everything from one cloud portal.

- ✕ **You outsource risk, not eliminate it**
  The 83-CVE Vasion disclosure proved multi-tenant SaaS print can fail at isolation and ship hardcoded backdoors.
- ✕ **Loss of data sovereignty**
  Print metadata — sometimes job data — traverses public cloud, breaking HIPAA/GDPR provability.
- ✕ **Operational fragility**
  If the management or auth plane lives in the cloud, an ISP or vendor outage can stop mission-critical printing.
- ✕ **Supply-chain opacity**
  Organizations lose visibility into the code running on their endpoints.

THE REALITY **Serverless doesn't delete risk — it ships it to a black box that can't be audited. The market has noticed: 86% of CIOs are pulling workloads back on-premises.**

OPTION C · RECOMMENDED

Adopt a Hybrid Print Architecture with ScrewDrivers®

HPA unifies centralized, direct-IP, and cloud printing under one control plane. It keeps print servers where they add value, fortifies them, and gives IT one console for drivers, printers, and policy across every site. The result: you consolidate the infrastructure, secure it end-to-end, and optimize how it runs.

THE HARDENED PRINT PATH

ENDPOINT WORKSTATION / VDI SESSION

ENCRYPTED PRINT STREAM
TMF® proprietary protocol

PRINT PATH HARDENED
Fortified print infrastructure

PILLAR 1

Fortified Print Servers

Hardened, high-availability instances for mission-critical sites. Active/active clustering delivers **sub-30-second failover and 99.9% uptime** — even if the internet goes dark.

PILLAR 2

Direct IP Zones

Serverless-style simplicity for distributed, low-risk branch offices — **without the cloud-only exposure**.

PILLAR 3

Unified Control Plane

One pane of glass for policy across the entire estate, replacing per-site GPOs with **drag-and-drop assignment** by user, group, device, or site.

CONSOLIDATE

100s → **driverless**
native drivers per endpoint — driverless

Dozens → **a few**
print servers, consolidated

SECURE

~90%

Smaller attack surface. Zero Trust, 100% on-prem, encrypted TMF, and an immutable audit trail.

OPTIMIZE

Sub-30s

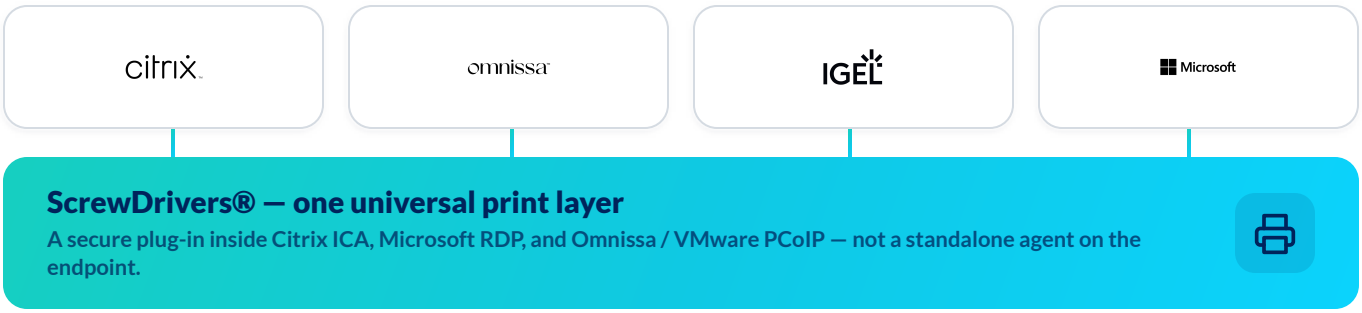
Failover with 99.9% uptime, the fastest time-to-first-print, and fewer print tickets.

THE POWER OF PARTNERS · BUILT FOR VDI

Solve printing in virtual desktops

Virtual desktops fixed almost everything about endpoint management — except print. Inside Citrix, Microsoft AVD, Omnissa, and IGEL sessions, stacked drivers, synchronous logon scripts, and a privileged spooler make print the **least stable, least secure** part of the stack. ScrewDrivers deploys as a secure plug-in inside each platform and turns print into a non-event.

VALIDATED ACROSS THE PLATFORMS YOU ALREADY RUN



THE VDI PRINT EXPERIENCE

WITHOUT SCREWDRIVERS

Print is the weak link in the session.

- ✗ 10–15 vendor drivers per gold image — conflicts crash sessions
- ✗ Synchronous logon scripts stall sign-in while printers map
- ✗ Printers duplicate, vanish, or mis-map between sessions
- ✗ A privileged spooler widens the attack surface inside the host
- ✗ Spooler crashes drop print jobs and take sessions down with them
- ✗ Per-site GPOs and manual scripts to assign every printer
- ✗ No failover — one server outage stops printing for the site

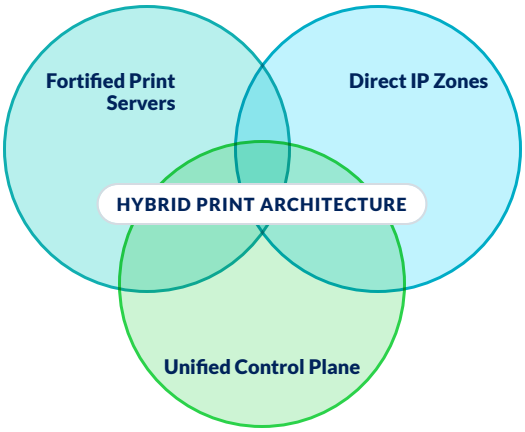
WITH SCREWDRIVERS

Print becomes a non-event.

- ✓ Driverless printing to remove print driver management and vulnerabilities
- ✓ No more management with GPOs and scripts
- ✓ The right printers, correct in every session and at every site
- ✓ Driverless endpoints shrink the print attack surface
- ✓ No more spooler crashes
- ✓ Drag-and-drop printer assignments
- ✓ Sub-30s failover with 99.9% uptime — even if the internet drops

OPTION C · WHY IT WINS

The future of print isn't serverless — it's fortified



THE ARCHITECTURE

Three pillars, one control plane

HPA keeps your print servers where they earn their place, adds **serverless-style direct-IP zones** for the edge, and binds both under a single unified control plane. **ScrewDrivers is the industry's defining HPA platform** — control is repatriated without losing convenience.

CONSOLIDATE · SECURE · OPTIMIZE

OUTCOME 01
Consolidate

- **Hundreds of drivers → driverless**
  Stacked vendor drivers vanish from the endpoint. Our driverless technology does the work of 10–15 per workstation — one CVE response path instead of dozens.
- **Dozens of print servers → a few**
  Collapse sprawling per-site servers into a handful of **fortified, clustered instances**, all run from a single console.

OUTCOME 02
Secure

- **Zero Trust by design**
  Native AD / Entra IDs (no hardcoded keys), least-privilege visibility, and hold-and-release PIN printing.
- **Sovereign & auditable**
  100% on-prem — jobs, metadata, and credentials never leave the firewall; immutable audit for HIPAA, SOX, GDPR & FedRAMP.

OUTCOME 03
Optimize

- **Fastest path to print**
  Mappings run in parallel and out-of-band of login — the **quickest time-to-first-print** of any method.
- **Fewer tickets, faster onboarding**
  New printer models onboard without per-model driver work, and print-related helpdesk volume drops.

Deploys as a secure plug-in within Citrix ICA, Microsoft RDP, and Omnissa PCoIP — reducing the attack surface versus standalone serverless agents.

THE STRATEGIC CASE

The future of enterprise print isn't serverless — it's fortified. A Hybrid Print Architecture lets an organization keep its print servers, add a faster and more secure workstation layer, unify everything under one console, and prove the value across all sites in a four-week trial. Control is repatriated without losing convenience.

SIDE-BY-SIDE COMPARISON

The three options, across what matters

Option A and Option B both leave the organization exposed; Option C closes the gaps without ripping out what works.

DIMENSION	A • Do Nothing Scripts & GPOs	B • Serverless Cloud-only SaaS	C • ScrewDrivers HPA Recommended
License cost	None	Subscription	Flexible concurrent user licensing
Driver attack surface	High (10–15 / workstation)	Vendor-dependent	~95% lower (driverless technology)
Data sovereignty	On-prem but unaudited	Private data leaves perimeter	100% in perimeter
Offline resilience	Local but fragile	Internet-dependent	Sub-30s failover, 99.9% uptime
Audit trail	Scattered / none	In vendor cloud	Per-user, immutable, local
Zero Trust / AD	GPO-based	Varies; backdoor risk	Native AD/Entra
Management	Per-site GPOs	Single cloud console	Unified control plane
Compliance posture	Hard to prove	BAA + cross-tenant risk	HIPAA/SOX/GDPR/FedRAMP

The pattern is clear: Option A and Option B both leave the organization exposed; **Option C closes the gaps without ripping out what works.**

MAKING THE DECISION

A buyer's framework

WHERE IT MATTERS MOST

- **Regulated industries** — healthcare, finance, government, legal — where sovereignty and uptime are non-negotiable.
- **Distributed enterprises** with many sites and a mix of HQ, clinical, and branch footprints.
- Organizations with existing Citrix, RDP, or Omnissa environments.
- **Inflection points** — a renewal, a compliance audit, a cloud-migration project, or a recent print outage.

QUESTIONS TO ASK

1. 1If your print-management vendor's cloud went down, what stops in your business?
2. Can you produce a per-user audit trail of who printed what, today, for a compliance request?
3. How many vendor print drivers are on a typical workstation — and who owns patching them?
4. What share of your helpdesk tickets are print-related?
5. Does any print metadata leave your secure perimeter today? Can you prove it doesn't?

COMMON CONCERNS, ADDRESSED

"Serverless is simpler and cheaper."

Simpler to deploy, riskier to own. 83 CVEs, hardcoded backdoors, cross-tenant leaks — and you can't prove HIPAA/GDPR when metadata leaves your perimeter. **Hybrid keeps the single-console simplicity and keeps the data home.**

"We'll just keep our scripts and GPOs."

That isn't free — it's ~23% of the helpdesk and an unpatched PrintNightmare surface. **A modern print layer pays for itself in reclaimed hours inside Year 1.**

"We're a cloud-first organization."

So is the market — and 86% of CIOs are now repatriating workloads. **Hybrid is the cloud-smart position**: cloud where it's safe, fortified local where it can't fail.

"We don't want to rip out our print servers."

You don't have to. Option C keeps them, fortifies them, and adds the workstation layer on top. **Existing rules and mappings carry over.**

GETTING STARTED — ASSESSMENT & TRIAL

1. **Setup & pilot**
   Week 1 · 2–3 sites online, baseline metrics captured.
2. **Validate**
   Week 2 · printer variance and WAN behavior confirmed.
3. **Scale out**
   Week 3 · full deployment in waves across the estate.
4. **Review & convert**
   Week 4 · results reviewed against success criteria.

THE DEFENSIBLE ANSWER

Prove it in your environment in four weeks.

A free architecture assessment, then a four-week trial. Existing rules carry over and a full rollout is typically a 2–4 week effort.

Request an assessment →

SOURCES

Sources & references

All figures are tied to 2025–2026 third-party research or named CVEs. Internal modeling figures are drawn from Tricerat ScrewDrivers product data and a representative customer scenario.

01 **Pierre Kim — 83 vulnerabilities in Vasion Print / PrinterLogic (April 8, 2025)**
pierrekim.github.io/blog/2025-04-08-vasion-printerlogic-83-vulnerabilities.html

02 **Full Disclosure mailing list — Vasion / PrinterLogic 83 vulnerabilities**
seclists.org/fulldisclosure/2025/Apr/18

03 **Tenable — CVE-2025-34217 (Vasion/PrinterLogic hardcoded SSH key)**
tenable.com/cve/CVE-2025-34217

04 **CISA — PrintNightmare, Critical Windows Print Spooler Vulnerability**
cisa.gov/news-events/alerts/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability

05 **Dark Reading — Windows Print Spooler security after PrintNightmare (~53 CVEs)**
darkreading.com/endpoint-security/windows-print-spooler-security-improves-in-wake-of-printnightmare-scare

06 **DataBank — Why 86% of CIOs Are Rethinking Their Cloud Strategy (Barclays CIO Survey)**
databank.com/resources/blogs/why-86-of-cios-are-rethinking-their-cloud-strategy

07 **TechTarget — Plan for Repatriation on Day One with a Hybrid Cloud Strategy (Dec 11, 2025)**
techtarget.com/searchcloudcomputing

08 **Flexera — 2025 State of the Cloud Report (cloud repatriation data)**
flexera.com/about-us/press-center/flexera-releases-2025-state-of-the-cloud-report

09 **Quocirca — Global Print Security Landscape 2025 (press release)**
quocirca.com/quocirca-print-security-landscape-2025-press-release

10 **Censinet — Healthcare downtime cost per minute study**
censinet.com/perspectives/healthcare-downtime-costs-hospitals-average-study

Tricerat source material — *The Print Security Paradox*, *The Serverless Print Trap*, *Resilience by Design*, *Eliminate the Print Security Nightmare*, *Kill Driver Hell*, and ScrewDrivers Workstation Printing product documentation.