tricerat | SCREWDRIVERS®

WHITE PAPER

ENDPOINT SECURITY & RESILIENCE

The Last Mile of Endpoint Security

Why print infrastructure is the overlooked risk, resilience, and experience gap in the regulated, branch-based VDI enterprise.

56%	**$15K**	**11%**
of organizations had a print-related data breach in the past year	average cost of IT downtime, per minute, across industries	of all security incidents trace back to print infrastructure

EXECUTIVE SUMMARY

The print path is the last endpoint left exposed

Financial institutions have secured the desktop, the network, and the data. In branch-heavy, virtualized environments, the print path remains the one endpoint rarely governed with the same rigor — and the one place where compliance, continuity, and digital-experience risk quietly converge.

56%
of organizations had a print-related data breach in the past year

$15K
avg. cost of IT downtime per minute, across industries

11%
of all security incidents trace back to print infrastructure

Across large, branch-based financial institutions, technology leaders have invested heavily in the endpoints that matter. They have moved thousands of employees onto virtual desktops for secure, consistent access from anywhere. They have adopted digital employee experience (DEX) platforms so issues are remediated before a help-desk ticket is ever opened. They have engineered redundancy and immutability into the systems that carry the business, because in a high-volume lending operation, hours of downtime translate directly into seven-figure revenue impact.

Yet one endpoint is still routinely treated as a commodity: the printer. In a virtualized, regulated, multi-branch environment, the print path is simultaneously a security surface carrying non-public customer information, a single point of failure absent from most disaster-recovery plans, and one of the most frequent sources of virtual-desktop friction. This paper argues that print infrastructure deserves the same secure-by-design, redundant-by-design, observable-by-design treatment as the rest of the endpoint stack — and outlines a practical framework for getting there.

> ***"Printing sits inside all of this — and is governed by almost none of it."***

1 · THE ENDPOINT THAT NEVER MAKES THE ROADMAP

The modern financial-services workplace has been deliberately re-architected around control. Virtual desktop infrastructure (VDI) gives security teams a hardened, centrally managed surface: policy follows the user, data stays in the data center, and access is governed dynamically by behavior and context. Zero Trust network transformation has eliminated hardware choke points and brought near-total traffic inspection. DEX platforms have shifted IT from reactive ticket-chasing to proactive remediation — resetting and cleaning up sessions before a team member even reports a problem.

Printing sits inside all of this — and is governed by almost none of it. It is one of the most common things to break in a virtual-desktop session and one of the most quietly dangerous things to get wrong. The result is a strategic blind spot: an endpoint that touches sensitive data, business continuity, and employee experience every day, managed as if it were a box of toner.

SECTION 02

Three risks hiding in the print path

2.1 Print is a security surface

In a regulated lending environment, documents printed at the branch carry non-public personal information (NPI) — loan applications, identity documents, statements. Protecting the privacy and integrity of that data is a stated top priority, validated through annual SOC 2 Type II audits. Yet print drivers, spoolers, and queues frequently sit outside the Zero Trust perimeter that governs every other endpoint. An ungoverned print path is an uninspected path — a gap in an otherwise airtight posture, and a category of access that regulators have explicitly flagged when controls are inconsistent.

2.2 Print is a resilience question

Leading institutions have consolidated disaster recovery and business continuity under a single framework, with immutable backups and tested, repeatable recovery as a regulatory expectation in financial services. Print servers, however, are classic single points of failure that rarely appear on the DR plan. When a branch print server fails, frontline staff cannot close loans, produce disclosures, or serve customers — and the cost of lost productive hours scales across every location at once. Designed redundancy should not stop at the application tier; it must extend to the path that puts documents in a customer's hands.

2.3 Print is a digital-experience issue

Nothing erodes trust in a virtual desktop faster than "I can't print." Organizations that have made DEX a strategic priority measure success by how often they resolve issues before users feel them. Proactive remediation that ends at the session boundary leaves the single most common VDI complaint unaddressed. Extending observability and self-healing to the print path closes the gap between "the desktop works" and "my work works."

WHERE THE PRINT PATH FALLS SHORT OF THE REST OF THE STACK

Endpoint dimension	Modern treatment	Typical print reality
Access & inspection	Zero Trust, full TLS inspection	Drivers/queues outside the perimeter
Resilience	Redundant, immutable, DR-tested	Single server, absent from DR plan
Observability	Proactive DEX, pre-ticket fixes	Reactive; surfaces only via tickets
Data governance	NPI encrypted, access reviewed	Released without release control

SECTION 03

A framework: secure, redundant, and observable by design

Treating print as a first-class endpoint does not require reinventing the workplace. It requires applying the same design principles already proven across the rest of the stack.

1 Govern the path, not just the device

Eliminate native print drivers and unmanaged queues. A driverless, server-side model removes a persistent attack and instability surface, and lets print policy follow the user in VDI exactly as application and data policy already do.

2 Build redundancy into the print tier

Remove the branch print server as a single point of failure. Designed failover and centralized management keep printing available during outages and bring print into the same DR posture as the applications it supports.

3 Extend observability to the last mile

Bring print health, queue status, and release events into the same single pane of glass used for DEX — so the most common VDI complaint becomes a proactively remediated signal rather than a recurring ticket.

4 Close the data-governance loop

Apply secure release, authentication at the device, and auditable tracking so NPI is never left unattended in an output tray — aligning the print path with SOC 2 controls and examiner expectations.

4 · THE LAST MILE IS WHERE THE RISK HIDES

The strongest technology organizations in financial services have already secured the desktop, the network, and the data. The print path is the last mile of that work — and in a regulated, branch-heavy, virtualized enterprise, the last mile is where the risk, the fragility, and the friction quietly accumulate. Bringing print under the same secure, redundant, and observable design discipline as the rest of the endpoint estate is not a back-office upgrade. It is the completion of an endpoint-security and resilience strategy that is, today, only mostly finished.

ABOUT THIS PAPER

Tricerat helps enterprises make print infrastructure secure, redundant, and optimized.

Helping regulated, branch-based, and virtualized environments bring the last endpoint into the same design discipline as the rest of the stack. To discuss print strategy in your VDI environment, start a conversation.

Start a conversation →