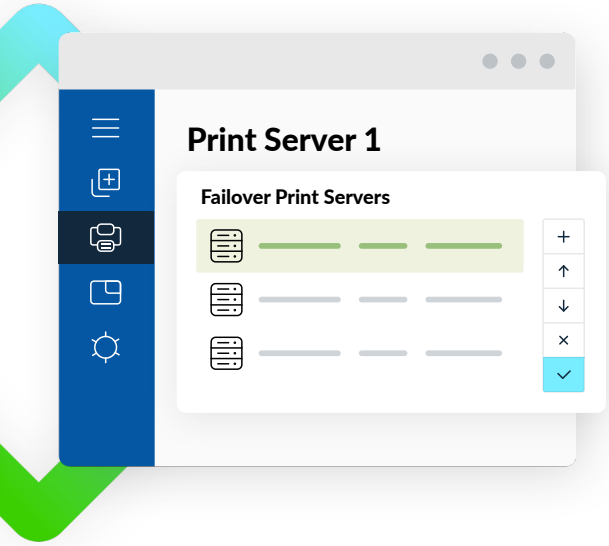
tricerat

Eliminate the Print Security Nightmare

Why Print Infrastructure Must Evolve to a Zero Trust, Data-Sovereign Model



When it comes to protecting systems and data, it is common practice to harden the network perimeter, secure email, and deploy sophisticated endpoint protection. Yet, a massive strategic blind spot remains: the enterprise print infrastructure. In the rush to eliminate local hardware, many organizations adopted serverless or cloud-only print tools. This pivot inadvertently outsourced their security posture to third-party vendors and significantly expanded their attack surface.

True enterprise protection requires printing solutions that follow Zero Trust security principles and ensure strict data sovereignty. This level of security is achievable only through an architecture purposefully designed to keep sensitive data within the corporate perimeter.

Defining Zero Trust for Enterprise Printing

To eliminate these vulnerabilities, Zero Trust must apply to the physical release of a document. This means utilizing hold and release workflows alongside native PIN code authentication. This ensures that a user is physically present before a document materializes, eliminating the vulnerability window where documents sit unattended. Enforcing least privilege requires identity-centric access control. Integrating directly with existing directory services, such as Active Directory, ensures that users only see and access the specific devices they are authorized to use.

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.

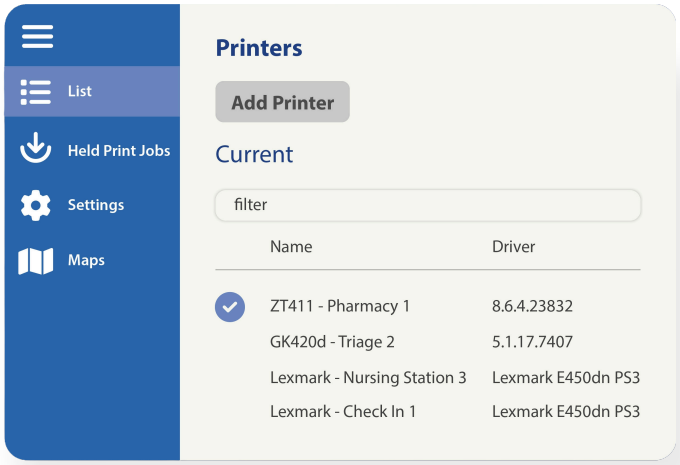
Immutable Accountability

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

The Mandate for Data Sovereignty and Compliance

For highly regulated industries such as healthcare, finance, and government, data sovereignty is non-negotiable. Print jobs containing protected health information or classified data must never traverse external vendor networks. Keeping data strictly on-premises is the only way to eliminate cross-tenant risks and avoid complex business associate agreements.

Furthermore, organizations require immutable accountability. Comprehensive audit trails must capture user identity, timestamps, and document metadata to satisfy strict HIPAA, SOX, and GDPR compliance mandates. Cloud-based logging systems can fail during vendor outages, leading to direct compliance violations, making local accountability critical.

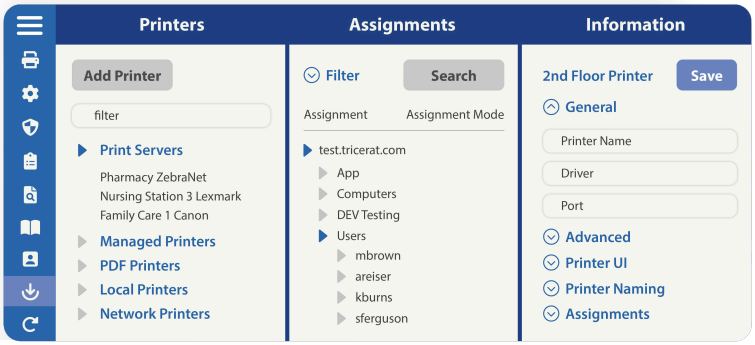


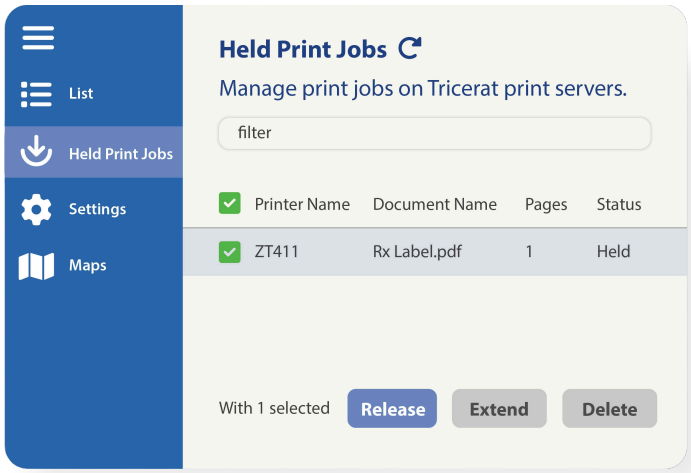
The Universal Driver: Eliminating "Driver Hell"

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.





Secure Print Release

Secure hold-and-release printing is one of the best ways to prevent data exposure in the print path. In a secure printing environment jobs are only printed when the user confirms their identity at the printer. This ensures other users will not gain access to the wrong document.

The Strategic Pivot to Hybrid Print Architecture

Security-conscious organizations must transition their framework away from unmanaged legacy servers and risky cloud-only models. Hybrid Print Architecture (HPA) provides a secure alternative by unifying centralized, direct IP, and cloud printing into a single cohesive architecture.

HPA utilizes the concept of Fortified Instances, which replaces vulnerable, unmanaged legacy print servers with these hardened, local instances designed specifically for critical workloads. This approach keeps data processing strictly on-premises, eliminating third-party data transit and guaranteeing total data sovereignty.

How Tricerat's Hybrid Print Architecture Fortifies the Enterprise

Tricerat delivers secure output orchestration through encrypted hold and release workflows, preventing unattended documents and data exfiltration. By utilizing Advanced Print Features, Tricerat enables native manufacturer PIN printing, leveraging the built-in hardware security of existing printer fleets without requiring proprietary workarounds.

The Tricerat unified control plane provides true Zero Trust enforcement by integrating natively with Active Directory for role-based access control. This eliminates the need for secondary, vulnerable identity databases. It enforces the principle of least privilege by ensuring users only see the printers they are explicitly authorized to access.

Additionally, the ScrewDrivers client is designed for maximum security. It operates as a plug-in within existing secure virtual channel protocols like Citrix ICA, Microsoft RDP, and VMware PCoIP. This architecture interprets data rather than executing code, effectively neutralizing many common network attack vectors and supply chain risks associated with standalone executables.

Moving from Utility to Strategic Asset

Print infrastructure can no longer be ignored as a minor IT utility. It must be treated as a fortified security pillar.

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