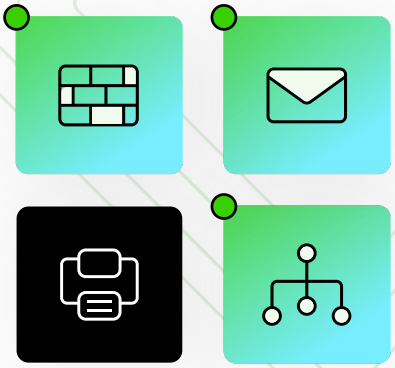
tricerat®

Kill Driver Hell

Virtualizing Print Infrastructure for Enterprise Performance and Security

The Anatomy of Driver Hell



While organizations invest heavily in modernizing their digital workspaces, legacy print driver management remains a persistent drain on IT resources. In environments utilizing Citrix, Omnissa, and Microsoft Azure Virtual Desktop, managing individual manufacturer drivers leads to session instability, slow logon times, and bloated master images. True operational efficiency requires abstracting the print process away from the endpoint. This paper explains how universal driver virtualization through solutions like Tricerat's ScrewDrivers eliminates driver conflicts, secures the endpoint, and optimizes bandwidth across the hybrid enterprise.

I'm sure we're preaching to the choir here, but the operational reality of managing thousands of unique, proprietary print drivers across a globally distributed workforce is a nightmare. Conflicting drivers inevitably cause print spooler crashes, which break critical workflows. Those disrupted workflows are annoying at best, but when it comes to mission-critical environments like healthcare or energy, those disruptions can put lives and critical infrastructure at risk. And print-related issues routinely account for up to 50 percent of helpdesk tickets, preventing IT teams from focusing on strategic digital transformation projects.

Tricerat ScrewDrivers© directly solves this issue by utilizing a single virtual driver to seamlessly handle every printer manufacturer and model across your entire environment. By removing the need to manage individual drivers and automating routine tasks like printer assignments, organizations utilizing Tricerat typically experience a 75 percent reduction in print-related help desk tickets.

The Performance Bottleneck in Virtual Environments

Traditional print infrastructure forces administrators into the constant cycle of rebuilding golden master images every time

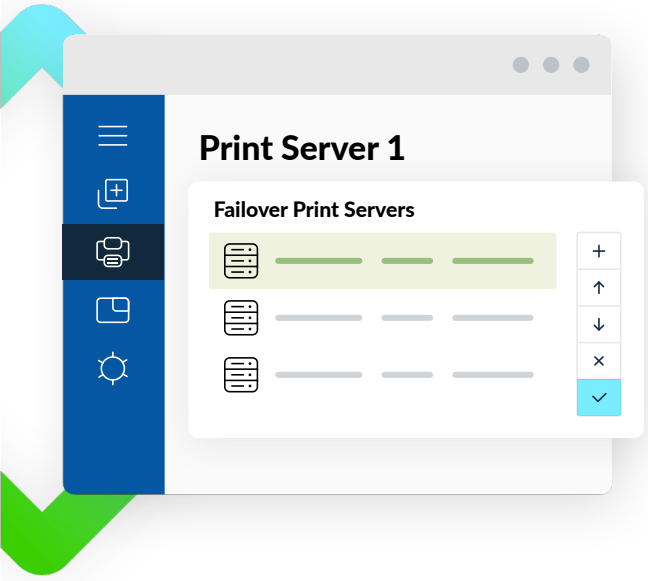
Traditional print infrastructure forces administrators into the constant cycle of rebuilding golden master images every time a new printer is added to the network, leading to severe virtual desktop image bloat. Furthermore, traditional printer mapping stalls login sequences, frustrating end users who expect seamless access to their virtual applications. Native print jobs also consume massive amounts of network bandwidth, which degrades the overall virtual desktop experience.

Tricerat addresses these performance bottlenecks through multithreaded processes that build printers rapidly in the background, ensuring that login sessions continue without interruption. ScrewDrivers© delivers mapping and spooling in under two seconds, and utilizes a proprietary TMF format with LZ4 compression to reduce print job bandwidth consumption by a factor of ten, ensuring pristine session performance across all VDI environments.

The Security Threat of Unmanaged Drivers

Beyond the manageability and performance issues of driver hell, constantly installing third-party executable files on enterprise endpoints significantly expands the attack surface. Recent industry security findings highlight that unvalidated driver upload mechanisms allow attackers to install malicious software without cryptographic signature verification. Additionally, insecure temporary file handling by traditional print clients has led to critical local privilege escalation vulnerabilities, allowing unprivileged users to overwrite protected system files.

Tricerat eliminates this security nightmare by removing third-party printer drivers from endpoints entirely. Because the ScrewDrivers© architecture does not rely on installing



Beyond the manageability and performance issues of driver hell, constantly installing third-party executable files on enterprise endpoints significantly expands the attack surface. Recent industry security findings highlight that unvalidated driver upload mechanisms allow attackers to install malicious software without cryptographic signature verification. Additionally, insecure temporary file handling by traditional print clients has led to

The Security Threat of Unmanaged Drivers

Beyond the manageability and performance issues of driver hell, constantly installing third-party executable files on enterprise endpoints significantly expands the attack surface. Recent industry security findings highlight that unvalidated driver upload mechanisms allow attackers to install malicious software without cryptographic signature verification. Additionally, insecure temporary file handling by traditional print clients has led to critical local privilege escalation vulnerabilities, allowing unprivileged users to overwrite protected system files.

Tricerat eliminates this security nightmare by removing third-party printer drivers from endpoints entirely. Because the ScrewDrivers© architecture does not rely on installing native manufacturer executable files on the client endpoint, organizations instantly close these dangerous vulnerability windows and protect their infrastructure from local privilege escalation and unvalidated upload attacks.

The Paradigm Shift into Universal Driver Virtualization

The good news is, there's a solution for the pain, performance issues, and security degradation of managing print drivers. Replacing hundreds of manufacturer-specific drivers with a single, secure virtual driver enables you to abstract the print layer away from the endpoint. This abstraction stabilizes the operating system and dramatically simplifies IT administration.

Historically, the concern with virtual drivers was the loss of advanced manufacturer hardware features. However, Tricerat ScrewDrivers© utilizes Advanced Print Features (APF) to enable native-driver functionality without the associated endpoint bloat. This means users retain full access to printer security features like PIN printing and secure print workflows, as well as advanced finishing options, directly through the native manufacturer implementation.

How Tricerat Transforms Print Management

Tricerat transforms print management by providing a platform-agnostic foundation for enterprise output, allowing IT teams to manage complex topologies from a single centralized console. Through Tricerat's unified control plane, administrators can automate routine tasks across the entire global print fleet.

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®