Silverfort

Solving key identity security challenges in retail with Silverfort

As retailers compete in an increasingly competitive marketplace, they invest a great deal of resources in becoming household names. But brand recognition is a double-edged sword when it comes to cybersecurity. The bigger your name, the bigger the cyber target on your back. In Q1 2025, the retail sector saw almost 75% increase in ransomware extortion incidents, with the average cost of a breach rising to $4.5 million. Additionally, 65% of breaches involved compromised employee credentials, and 55% were linked to third-party vendors, reflecting the complex and evolving threat landscape.

The nature of retail organizations differs from most industries in that they are multi-site and multi-channel, resulting in many more entry points for ransomware attacks. The threat of ransomware is one of the greatest concerns for retailers. Typical retail operations include item-level RFID-based packages and pallets, vehicle-mounted computers, handheld scan-based computers, smart shelves and more, resulting in a massive attack surface to protect.

What makes retail institutions a key target for identity threats?

Lack of visibility across complex environments

Retailers deploy a multitude of devices and applications that operate independently, making it difficult for security teams to monitor and manage the entire identity lifecycle. As a result, unauthorized access and potential breaches are more likely to occur.

Inability to stop real-time lateral movement attacks

Lateral movement attacks use valid but compromised user credentials, making attacker activity identical to legitimate user access. These attacks exploit the existing authentication infrastructure for malicious purposes.

Lack of visibility into non-human identities

Despite the critical role NHIs play in every environment, they suffer from extremely low visibility, exposing them to compromise and lateral movement.

How Silverfort solves identity security challenges in the retail sector

Full context across environments

Silverfort automatically discovers and provides centralized visibility into every authentication and access request across the entire hybrid environment. As a result of its native integrations with all identity providers, it can log every authentication request.

Lateral movement protection

Silverfort is the first solution that can extend MFA verification to all access interfaces and authentication protocols in the AD environment, including command-line access tools like PsExec and PowerShell, lateral movement tools of choice.

Full NHI visibility and security

Silverfort automatically identities all NHI within the environment and offers the identity and security teams the tools to secure them based on each account's behavior.

Learn more about how Silverfort helps retail institutions solve their key identity security challenges.

Download the full eBook