SILVERFORT

Facing and Overcoming Retail Identity Protection Challenges

Silverfort enables retailers to overcome common identity protection challenges by mitigating ransomware risk, gaining visibility across all users and service account activity, and extending MFA protection to all resources.

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. **Data breaches in the retail sector cost an average of $3.28 million in 2023**, with 50% of cyberattack victims experiencing extortion and 25% experiencing credential harvesting.

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 Retailers a Key Target for Identity Threats

Lack of Visibility Across Complex Environments	Inability to Stop Lateral Movement Attacks in Real Time	Lack of Visibility into Service Accounts
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.	Lateral movement attacks involve the use of valid but compromised user credentials. Authentications performed by an attacker are essentially identical to those performed by a legitimate user. As such, a lateral movement attack is a series of authentications that utilize the legitimate authentication infrastructure for malicious purposes.	Despite the critical role service accounts play in processes, programs, and applications, most organizations have extremely limited visibility of their behavior and roles, leaving them open to compromise and lateral movement.

How Silverfort Solves Retail Identity Protection Challenges

Full Context Across Environments	Lateral Movement Protection	Securing Service Accounts
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.	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.	Silverfort automatically identifies all service accounts within the environment and enables the identity and security teams to secure them with pre-made policies, tailored to each account's behavior.

Learn more about how Silverfort helps retailers solve their key identity protection challenges.

Download our Full eBook