

Attackers Continue to Exploit MFA Coverage Gaps in VPN and RDP Access



Recent ransomware incidents highlight how attackers exploit authentication gaps where MFA protects cloud applications but VPN, RDP and Windows logon remain password-only.

- Compromised credentials accounted for initial access in 21% of ransomware incidents investigated in 2025, typically through RDP or VPN
- RDP with compromised accounts was used for lateral movement in approximately 85% of ransomware investigations
- Organizations often enforce MFA for cloud applications while leaving VPN, RDP and Windows logon protected only by passwords
- Stolen credentials remain effective when authentication paths accept passwords without additional verification

- AI enables attackers to operate credential-based attacks at greater speed and scale

The Authentication Coverage Problem

A recent ransomware incident in August 2026 demonstrated a persistent vulnerability in enterprise authentication strategies. An attacker successfully accessed a corporate network through a SonicWall SSL VPN account that lacked **multi-factor authentication**, despite the organization enforcing MFA for cloud applications. Within approximately two hours of initial access, the attacker had reached the domain controller via RDP and begun Active Directory enumeration.

This pattern reflects a broader issue where organizations implement strong authentication for internet-facing SaaS platforms and Microsoft 365 while leaving critical access paths such as VPN, RDP and Windows logon protected only by passwords. The fragmented approach creates exploitable gaps that threat actors routinely target.

Credential Theft Remains Primary Attack Vector

Investigations into ransomware incidents reveal the continued effectiveness of compromised credentials as an initial access method. According to Mandiant research, legitimate compromised credentials accounted for the entry point in 21 percent of 2025 ransomware cases where initial access could be determined, predominantly through RDP or VPN channels.

The threat extends beyond initial access. RDP sessions using compromised or newly created accounts appeared in lateral movement activities in approximately 85 percent of investigated ransomware incidents. Artificial intelligence is amplifying this risk by enabling attackers to conduct credential-based operations at increased speed and scale, though the underlying identity compromise tactics remain largely unchanged.

Addressing the Gap

The Verizon Data Breach Investigation Report indicates stolen credentials are involved in 44.7 percent of breaches. For regulated institutions, the critical question is not whether MFA exists but where password-only authentication persists. Windows logon, RDP sessions, VPN access and legacy Active Directory-backed services represent common coverage gaps that warrant systematic review.

Extending MFA protection to these on-premises and hybrid access paths, alongside regular password auditing to identify weak or previously breached credentials, helps reduce the utility of stolen passwords before they can be exploited.

What to do now

1. Conduct an authentication coverage audit to identify all access paths (VPN, RDP, Windows logon, legacy services) that currently accept passwords without MFA

2. Extend MFA enforcement to VPN gateways, RDP sessions and Windows authentication, not only cloud applications and SaaS platforms
3. Implement regular Active Directory password auditing to identify weak, reused or previously breached credentials
4. Review RDP access controls and logging to detect lateral movement patterns using compromised accounts
5. Integrate authentication events from on-premises and hybrid access points into SIEM platforms for centralized monitoring
6. Establish a policy requiring MFA for all privileged accounts and remote access methods, documented in accordance with NCA ECC and SAMA CSF requirements