External Remote Services Mitigation, Mitigation T1133 - Enterprise

Archived: 2026-04-05 16:42:26 UTC

Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems. Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls. Disable or block remotely available services such as Windows Remote Management. Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of Multi-Factor Authentication Interception techniques for some two-factor authentication implementations.

Source: https://attack.mitre.org/mitigations/T1133