# Remote access: which ways into your network should still exist?

This quarter, close every RDP, SSH and admin port on the internet, require phishing-resistant MFA on every way in and a compliant device for staff, and allow one licensed remote support tool. Then give supplier sessions an approval, an end date and a recording, and plan per-app access for the VPN's next renewal.

| Reviewed | Next review | Version | Written for |
|---|---|---|---|
| **5 Nov 2026** | **5 Dec 2026** | **1.0** | **IT and security teams in small and mid-size organizations, including those on Microsoft 365 and Azure** |

Latest version
**sheets.einblick.dev/remote-access/**

## If you only do five things

1. **Close RDP, SSH and admin ports on the internet.** Put them behind a gateway. In the access broker offers Verizon analyzed, remote desktop access such as RDP and VNC came a close second to VPNs[11].
2. **Require phishing-resistant MFA and a compliant device.** Sign users in through your identity provider so Conditional Access applies, with a method from the passkeys and MFA sheet. The NPS extension can't: it offers only calls, texts, push and codes[2].
3. **License one remote support tool and block the rest.** Free versions don't cover work use: TeamViewer counts home office use and supporting colleagues as commercial[3]; AnyDesk needs a license on any client that starts a commercial session[4].
4. **Open supplier access per job.** NIS2 rules for cloud providers and MSPs allow supplier connections only on request and for a set time[5]. BSI adds that your staff watch and record them[6].
5. **Alert on remote tools nobody approved.** Microsoft found an unsanctioned RMM agent to be one of the most reliable signs of a hands-on intruder, usually installed within minutes of the foothold[1].

## Decide whether to replace the VPN

1. **What do people reach through it?** A compromised account on a VPN can reach every service on the network; ZTNA admits users only to the apps they're authorized for[7]. List those apps from the VPN's logs.
2. **Is a replacement due anyway?** It pays off when the appliance nears end of support, keeps needing emergency patches or serves suppliers who need two apps. Entra Private Access needs Entra ID P1 plus the Entra Suite or its own license[8].
3. **Can you switch the VPN off safely?** The NCSC lists what must come first, such as encrypted internal traffic, devices that block inbound connections, protected legacy systems and DNS monitored another way[9].
4. **Move broad first, then narrow.** Entra's Quick Access copies the VPN's access to whole subnets and reports who reaches what. Then move each app into its own segment and policy[10].
5. **Close the old path.** Once apps have moved, delete the VPN accounts, routes and firewall rules they used, so no forgotten way in stays open.

## How attackers use legitimate remote access

- **Remote tools replace malware.** Legitimate RMM software in Verizon's system intrusion breaches rose 240% in a year[11]. Google found one in 24% of Mandiant's 2025 ransomware cases, down from 28%; AnyDesk led, in 10%[12].
- **Brokers sell the way in.** Of the access offers Intel 471 tracked in the year to June 2026, 37% came through compromised remote access portals such as VPNs[1].
- **The fake help desk asks to share the screen.** After a spam flood, attackers offer help in an external Teams chat, then usually connect with a built-in tool such as Quick Assist[11]. Teams accepts all external domains by default; allow only those you work with[13].

## Admin access without open ports

- **Azure: Bastion.** VMs need no public IP, and Bastion carries RDP and SSH over TLS on port 443. Premium adds session recording; the free Developer SKU serves one test VM at a time[14].
- **On premises: RD Gateway behind an app proxy.** Publishing RD Web and RD Gateway through Entra application proxy adds Conditional Access and needs only outbound connections[15].
- **Only from admin workstations.** BSI expects jump servers that only trusted systems can reach[6]. PAWs and zones are in the privileged access and network segmentation sheets, OT access in the OT security sheet.

## Contractors and vendors

- **Named accounts that expire.** Give contractors guest accounts through Entra access packages with approval, an end date and automatic removal. This needs Entra ID Governance or the Entra Suite[16].
- **Hours, not standing access.** Limit VPN access to the times it's needed and disable unused accounts promptly, as BSI requires[17].
- **Recording in Germany.** The works council co-determines any system able to monitor staff conduct or performance, whatever you intend[18,19]. Agree recordings and support-tool reports with it. Contracts are in the third-party risk sheet.

## Remote support and RMM tools

- **Use what you own.** Intune Remote Help works only inside your tenant and logs each session. Helpers and the users they help each need a license[20]: $3.50 per user per month as an add-on[21].
- **Block the rest centrally.** Defender for Endpoint blocks other tools by certificate, but not Microsoft's[22]. So uninstall unused Quick Assist, as Microsoft advises; blocking its endpoint breaks Remote Help too[23].

## Logs and alerts for remote sessions

- **Collect every way in:** VPN, gateway, ZTNA, Bastion and support-tool logs and Windows remote desktop logons, kept as the logging sheet advises.
- **Alert on unapproved remote tools,** including portable and in-memory copies, and keep log deletion out of any RMM tool's reach[24].

- **Block their traffic.** CISA advises blocking common RMM ports at the perimeter in both directions, except for the approved tool[24].

## Split tunneling

- **Tunnel by default.** The NCSC advises an automatic, full-device VPN without split tunneling, to keep data from leaking outside it[25].
- **Exempt Microsoft 365 by IP.** Let only its Optimize endpoints bypass the tunnel: about 20 subnets with 70 to 80% of its traffic. Don't use FQDN rules[26].
- **Route other web traffic through a cloud web gateway** if it leaves the tunnel[26].

## What you can skip

- **Recording every employee's VPN session.** Record admin and supplier sessions; logs are enough for the rest.
- **A ZTNA suite for a few web apps.** Entra application proxy publishes them with Conditional Access on Entra ID P1[29].
- **Moving RDP or SSH to another port.** Scanners find it. Close it.

- **Hunt for the vishing pattern:** a Teams call followed within 30 minutes by a remote management process starting[1].

## What changed in 2026

- **Remote support servers were exploited all year.** From February to October, CISA added ten exploited flaws in BeyondTrust, ScreenConnect, N-central and SimpleHelp to KEV[27]. Treat them as edge devices.
- **Remote Help came to Microsoft 365 E3 and E5.** Microsoft began adding it in July 2026[21]. Retire support tools it replaces.
- **RDP files now trigger a warning.** Since April 2026, Windows turns their redirections off by default and flags unsigned files, so sign yours[28].

## Mistakes that cost the most

- **Excluding RMM install paths from EDR.** CISA notes it's common[24].
- **Sharing Bastion links.** Holders need only the VM's password or key[30].
- **One vendor VPN nobody watches.** Google saw ransomware actors reach an OT system through a vendor's VPN[12].

## What this looks like at your size

**Small team, no security staff**

- Ask your IT provider to list every way in, including its own remote tool, and close the rest.
- Check that the support tool is licensed to your company or provider and requires MFA.
- Reach Azure VMs through Bastion instead of public IPs.

**Growing, with IT or security staff**

- Move VPN sign-in to Entra ID with phishing-resistant MFA and compliant devices.
- Start per-app access with contractors, through access packages that expire.
- Allowlist one support tool and alert on any other.

**Enterprise or regulated**

- Replace the VPN at its next refresh with per-app ZTNA.
- Record supplier and admin sessions at a gateway, agreed with the works council in Germany.
- Map controls to NIS2 implementing rules point 6.7.2 and BSI OPS.1.2.5 and NET.3.3.

**Version history**

**5 Nov 2026, version 1.0** Published after a copy edit and a source-by-source fact check, which scoped the Verizon and Google remote tool figures, narrowed the free license claims to each vendor's terms, added Teams external access limits and corrected the works council and Bastion statements.

**Sources**


1. Microsoft Digital Defense Report 2026. Microsoft, Oct 2026. cdn-dynmedia-1.microsoft.com
2. Integrate NPS with Microsoft Entra MFA. Microsoft Learn, 4 Mar 2025. learn.microsoft.com
3. Commercial use suspected. TeamViewer, 11 May 2026. teamviewer.com
4. AnyDesk licenses. AnyDesk, 30 Oct 2025. support.anydesk.com
5. Implementing Regulation (EU) 2024/2690, Annex point 6.7.2. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu
6. IT-Grundschutz OPS.1.2.5 Fernwartung. BSI, Edition 2023. bsi.bund.de
7. Modern Approaches to Network Access Security. CISA and partners, 18 Jun 2024. ic3.gov
8. What is Global Secure Access?. Microsoft Learn, 15 Apr 2026. learn.microsoft.com
9. Zero trust migration: How will I know if I can remove my VPN?. NCSC (UK), reviewed 16 Jan 2026. ncsc.gov.uk
10. Tutorial: VPN replacement with Quick Access. Microsoft Learn, 2 Apr 2026. learn.microsoft.com
11. 2026 DBIR. Verizon, 19 May 2026. verizon.com
12. Ransomware Under Pressure. Google, 16 Mar 2026. cloud.google.com
13. Manage external meetings and chat. Microsoft Learn, 19 Nov 2025. learn.microsoft.com
14. What is Azure Bastion?. Microsoft Learn, 4 Feb 2026. learn.microsoft.com
15. Publish Remote Desktop with application proxy. Microsoft Learn, 25 Mar 2026. learn.microsoft.com
16. What is entitlement management?. Microsoft Learn, 24 Jun 2026. learn.microsoft.com
17. IT-Grundschutz NET.3.3 VPN. BSI, Edition 2023. bsi.bund.de
18. Betriebsverfassungsgesetz § 87(1) no. 6. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
19. Decision 1 ABR 7/15. Federal Labor Court (Germany), 13 Dec 2016. bundesarbeitsgericht.de
20. Planning for Remote Help with Microsoft Intune. Microsoft Learn, 8 Sep 2026. learn.microsoft.com
21. Microsoft Intune plans and pricing. Microsoft, checked 5 Nov 2026. microsoft.com
22. Create indicators based on certificates. Microsoft Learn, 3 Jul 2026. learn.microsoft.com
23. Use Quick Assist to help users. Microsoft Learn, 30 Sep 2025. learn.microsoft.com
24. Guide to Securing Remote Access Software. CISA, NSA, FBI, MS-ISAC and INCD, 6 Jun 2023. cisa.gov
25. Virtual private networks. NCSC (UK), reviewed 13 May 2025. ncsc.gov.uk
26. Overview: VPN split tunneling for Microsoft 365. Microsoft Learn, 26 Jun 2026. learn.microsoft.com
27. Known Exploited Vulnerabilities Catalog. CISA, version 2026.11.04. cisa.gov
28. Security warnings when opening RDP files. Microsoft Learn, 14 Apr 2026. learn.microsoft.com
29. Add an on-premises app to application proxy. Microsoft Learn, 10 Jul 2026. learn.microsoft.com
30. Create a shareable link for Bastion. Microsoft Learn, 11 Aug 2026. learn.microsoft.com