SENSAKA

sensaka.com

RDP Essentials & Hardening

Remote Desktop Protocol in four facts — and the lane that works when RDP won't

RDP in four facts

Full desktop

Screen, keyboard, mouse, clipboard, and drive redirection over the network

Port 3389

TCP/UDP 3389 — the port scanners probe first, and firewalls should hide

Harden it

Never internet-exposed: VPN or gateway, NLA, MFA, lockout policies

In-band limit

Needs a live OS and network — useless during boot failures and crashes

Hardening checklist

- Never expose RDP directly to the internet — it is one of the most attacked services (brute force, BlueKeep-class exploits, ransomware entry)
- Put it behind a VPN or gateway
- Require Network Level Authentication (NLA)
- Enforce MFA and account lockout policies

When RDP is the thing that's broken

In-band: RDP / VNC

- Full desktop day to day
- Needs a running, reachable OS
- Part of the outage during boot loops, blue screens, dead NICs

Out-of-band: the BMC lane

- vKVM console that works from power-on
- Independent of Windows entirely
- Remote power cycle and virtual media
- Isolated management network, sessions audited

RDP vs VNC: RDP is Microsoft's protocol, Windows-native and generally faster; VNC is a cross-platform framebuffer protocol. Both need a running, network-reachable operating system.

Public knowledge from Sensaka · free to share with attribution
Source: sensaka.com/resources/what-is-rdp