Devolutions

Secure, compliant, productive

remote connection management

A Devolutions playbook

OCTOBER 2025

Table of contents

ABSTRACT

Damaging cybersecurity incidents don't typically begin with malware: they begin with a stolen credential that enables malware or lateral movement (Verizon 2025, 6; CrowdStrike 2025, 3).

Since credentials have become increasingly used over remote connections, both by IT professionals and end users alike, **remote connection management** poses either a practical control point — or a pain point.

This playbook examines the top three remote connectivity challenges — **security**, **compliance**, and **productivity** — and outlines best practices to address them.

INTRODUCTION:
The new remote access landscape

Remote connectivity now underpins nearly every business sector, from tech startups and enterprises to nonprofits, hospitals, and even faith-based organizations.

Hybrid and remote work have surged globally, a trend expected to continue: nearly 65% of surveyed organizations predict significant growth in remote work over the next five years (We Work Remotely 2025). Virtually all companies have enabled remote access in some form; one security survey found that 94% of organizations allowed remote access to corporate applications and assets from both managed and unmanaged devices (Check Point Software Technologies Ltd 2022, 4).

Remote connection management, which governs how IT staff and end-users securely connect to servers, PCs, cloud instances, and network devices from afar, is now a mission-critical IT function across the board.

However, this new landscape brings formidable challenges...

KEY CHALLENGES

Security

The primary security concerns for IT professionals revolve around securely managing and monitoring remote connections to internal networks, servers, and critical infrastructure.

The Check Point Software Technologies security report (2022, 5) found that among those who reported allowing remote access to corporate applications, an alarming 11% weren't using any security precautions — no VPNs, no multi-factor authentication (MFA), no Zero Trust Network Access (ZTNA).

Such statistics underscore remote connection management as a **security imperative** for protecting organizational integrity.

Several security pain points demand attention:

Credential theft and privileged access abuse

Stolen or weak credentials are a leading cause of breaches. In fact, credential abuse accounted for 22% of initial access vectors — making it the leading cause among nearly 10,000 confirmed breaches in 2025 (Verizon 2025, 6).

Unfortunately, many IT departments still struggle with basic password hygiene. A 2022 survey (Hitachi ID Systems and Pulse Q&A) of IT and cybersecurity leaders revealed that 46% were storing passwords in shared spreadsheets or documents (and an additional 8% were writing them on paper notes).

Such practices are highly risky — a single stolen spreadsheet can hand an attacker the "keys to the kingdom" — privileged accounts; Forrester Research Inc. estimated that at least 80% of data breaches were the consequence of compromised privileged credentials (Cser 2018, as cited in Gurucul 2021). These statistics underscore the critical need for strong password management and privileged access controls in any setup — remote, hybrid, or on-site.

Organizations ought to deploy a secure password vault (Hitachi ID Systems and Pulse Q&A 2022) or privileged access management (PAM) system. Modern password managers and PAM tools can, among other things:

- Store credentials in encrypted form;
- Auto-fill (or broker) them for remote sessions (removing the need for staff to memorize or manually retrieve passwords);
- Enforce password policies (length, complexity, rotation).

Only 30% of companies reported using a business password manager solution in a 2022 survey (Hitachi ID Systems and Pulse Q&A), so adopting one is low-hanging fruit for many.

Lack of multi-factor authentication (MFA)

VPNs, RDP gateways, and admin portals protected only by single-factor logins (just a password) are easy prey for attackers leveraging stolen credentials or guessing weak passwords. Yet, less than half of organizations (only 46%) use multi-factor authentication for remote access to company resources (Check Point Software Technologies Ltd 2022, 5).

Requiring more than one factor for authentication (one-time code, biometric, geolocation, etc.) can thwart the vast majority of credential-based attacks by ensuring that a leaked password alone isn't enough for entry. Implementing MFA for all remote admin support tools is therefore a top best practice (OWG 2024, para 1). Coupled with encrypted connections, this drastically hardens the security of remote access.

Expanded attack surface and endpoint security

With staff connecting from myriad locations and networks, opportunities for attackers multiply. Home or public Wi-Fi networks may be poorly secured, making it easier for attackers to intercept remote sessions or plant malware. Personal devices used for work (in BYOD scenarios) might lack up-to-date security software. This dispersion led 54% of IT professionals to view remote workers as a greater security risk than on-site workers (OpenVPN 2024). Moreover, home workers became prime targets: one analysis noted cyber attacks rose 238% since the start of the pandemic, largely aimed at employees working from home (Blandford 2022).

Organizations should establish clear remote endpoint security policies, such as:

- Require approved anti-malware and firewall software on any device used;
- Enforce regular patching;
- Consider endpoint management tools, which let IT remotely update and secure home-user machines (OWG 2024, para 4).

In high-security environments, issuing company-managed laptops for remote work (and disallowing access from unvetted personal devices) can greatly reduce risk.

Unmonitored or "shadow" remote access

Another security challenge is visibility — knowing who is accessing what, when, and from where. In the rush to go remote, many firms stood up ad-hoc solutions (like opening remote desktop ports or using quick fixes such as unofficial remote control apps) without integrating them into central logging or identity management. Unmonitored remote access channels are a compliance nightmare and an open door for abuse. Lack of oversight is why 20% of organizations reported that remote workers caused a security breach in the past year — not necessarily through malice, but often through unsupervised actions or misconfigurations (Malwarebytes Labs 2020, 5).

IT teams should consolidate remote access through sanctioned platforms that support:

- Session logging and activity monitoring (especially for privileged sessions), which create searchable audit trails, allowing suspicious activity to be traced and addressed in real time, and making forensic analysis possible if an incident occurs (ironcore 2019);
- Granular access controls (each user gets access only to the resources they absolutely need) to limit the damage any single account compromise can do (ironcore 2019);
- Just-in-time (JIT) access provisioning and revocation after use for vendors or temporary workers (ironcore 2019).

Every remote session should leave an audit trail.

By addressing these security challenges with the measures above — secure credential management, MFA everywhere, endpoint security enforcement, and comprehensive monitoring — organizations can dramatically reduce their risk. Notably, these improvements also set the stage for better compliance and efficiency, as we explore next.

Compliance

Organizations also have to navigate complex **compliance regimes** in a remote context, which present their own challenges:

Data privacy regulations

Laws and regulations worldwide require organizations to protect sensitive data from unauthorized access — whether access occurs on-site or off.

Remote work makes this harder.

Employees may inadvertently use insecure networks or personal devices, creating vulnerabilities (Cooper 2025). Regulations like the European GDPR and industry-specific rules like HIPAA (for health data) or PCI DSS (for payment data) explicitly demand controls that are pertinent to remote access, for example:

- PCI DSS requires multi-factor authentication for administrative access to cardholder data environments (including remote admin access);
- HIPAA mandates encryption of PHI and access controls (Cooper 2025).

Failure to comply has severe repercussions: GDPR fines can reach €20 million or 4% of annual turnover, and even a single data breach can trigger investigations and penalties under various laws (Cooper 2025). Beyond fines, non-compliance means exposing clients' data to breaches, which can irreparably damage trust.

Ensuring secure remote access is a compliance necessity — not just an IT best practice.

Auditability and logging

Many frameworks for IT compliance require that organizations maintain logs of user activities, especially for privileged or remote access sessions (Cooper 2025). In practice, this means that when an administrator RDPs into a server or a helpdesk technician remotes into a user's PC, there should be a record of that session.

Companies relying on disparate tools might struggle here — logs might not be centralized or even enabled, delaying monitoring (and reporting). Consequently, IT teams can miss signs of misuse and face reactive firefighting.

From a compliance standpoint, inability to produce access logs during an audit is a red flag.

Adopting a remote access solution that automatically logs all sessions and changes is crucial. Detailed audit logs should capture who connected, when, for how long, and what actions were taken (e.g., commands run or files accessed).

Ideally, solutions will also allow exporting or integrating logs into a SIEM (security information and event management) system for analysis. By having these audit trails, organizations can demonstrate to auditors that every access is traceable.

Maintaining policy enforcement at scale

In-office, it's easier to enforce IT policies (you can physically restrict devices, require login via the corporate network, etc.). Remotely, IT must ensure policies "travel" with users.

One compliance challenge is simply policy adherence. A survey found that nearly half of IT leaders (49%) felt that remote employees only somewhat adhere to established IT security policies (OpenVPN 2024). This gap can be due to lack of oversight or clarity.

For compliance, organizations should:

- Update their policies to explicitly cover remote work scenarios (acceptable use of personal devices, requirements for VPN, etc.) and get user acknowledgment;
- Back these policies with technical controls: for instance, enforce that only company-approved remote access methods are usable (blocking less secure remote desktop apps), and use configuration management to check that encryption and patch levels on remote endpoints meet standards;

- Regularly audit their remote access infrastructure for compliance (Rathnam 2024).

Many companies now conduct internal audits or use external assessors to probe their remote access for weaknesses — e.g., scanning that all open remote ports are secured, and that terminated employees or contractors have had their access revoked promptly (a point often overlooked, risking "ghost" access).

Notably, in the earlier-mentioned survey of IT leaders, only a low 5% were extremely confident that ex-employees could no longer access company passwords or systems once they left, highlighting the need for diligent offboarding processes as part of compliance (Anderson, 2022).

Third-party access and vendor compliance

Because of the risk that vendors, contractors, or managed service providers pose to security, industry regulations often extend to third parties (for example, regulators expect that if you outsource IT functions, you still ensure the vendor follows security best practices). Yet, many organizations lack insight into these connections.

The Target retail breach of 2013 (caused by a HVAC vendor's remote credentials being stolen) remains a cautionary tale (Krebs 2014).

In a 2024 survey report, CyberArk reveals that 94% of respondents were using more than 10 vendors for identity-related cybersecurity initiatives, decentralizing security (4).

This creates a visibility problem: in the same survey, "26% of respondents chose lack of visibility across multiple identity-related point tools, products and services as the top two truest statements for their organizations" (CyberArk Software 2024, 17).

It's no wonder that 91% of organizations are concerned about third-party risks, and 82% are concerned about fourth-party risk (CyberArk Software 2024, 5).

Organizations should incorporate third-party access into their remote connection management strategy. Some best practices include:

- Using tools that can provide time-limited, audited access for vendors and contractors (Cooper 2025);
- Implementing just-in-time (JIT) access (this best practice was especially emphasized by IT professionals within the broader context of threat mitigation and vendor risk management) (CyberArk Software 2024, 27);
- Evaluating and consolidating third-party stacks for better visibility and manageability (CyberArk Software 2024, 18);
- Implementing MFA and adhering to least-privileged access principles can also help tighten vendor remote access, and help close a common compliance loophole.

In summary, **remote access compliance** boils down to extending robust security controls and oversight to wherever your users and data are.

The complexity has increased with increasingly distributed environments, but the solutions are within reach: with the right tools that keep data secure without overburdening the team, companies can remain both agile and compliant.

Productivity

Finally, the **productivity challenges** of remote connection management cannot be ignored. A secure, compliant system still needs to be usable and efficient, or IT teams and end-users will find workarounds that undermine policies.

Key productivity-related challenges include:

Tool fragmentation and workflow inefficiencies

IT teams often juggle disconnected tools for remote access — RDP for Windows, SSH for Linux, a VPN, cloud portals, credential vaults, and a ticketing system. This context switching is costing IT professionals dearly: ~8 hours per week — nearly a full workday (Integrated Research 2023).

By adopting a platform that aggregates remote connection types (RDP, SSH, VNC, VPN, etc.) into one interface, IT professionals can drastically reduce friction — and the mental load on IT staff.

Complexity of managing diverse environments

Modern IT environments are diverse and distributed, sometimes even across multiple geographic sites. Managing on-premises servers, cloud VMs, virtual desktops, employee laptops, operating systems, and protocols is complex — and that complexity grows as organizations scale.

Small businesses might get away with ad-hoc methods, but when dozens of endpoints become thousands, a lack of centralized remote management leads to chaos — missing access details, inconsistent configurations, and difficulty onboarding new IT staff (who have to learn a convoluted system).

Solution: a scalable remote-management framework that can:

- Add endpoints easily;
- Support diverse technologies;
- Maintain a single, up-to-date inventory of all remote-accessible systems and their connection details;
- Enable one-click lookup and session launching, eliminating manual IP/URL recall;
- Automate routine tasks (scripting, one-to-many actions), such as applying a change across 10 servers at once.

Balancing security with usability

Often, productivity issues arise when security measures are implemented in a user-unfriendly way. A classic example is burdensome password rules leading users to circumvent them, as mentioned earlier (Hitachi ID Systems and Pulse Q&A 2022).

Another is overly restrictive access processes — if, say, a helpdesk technician has to go through 10 steps to remote into a user's PC to resolve a simple issue, that's consuming more time than necessary. Striking the right balance is itself a challenge.

The goal should be to simplify the user experience of secure remote access. In practice, this might mean:

- Implementing SSO to eliminate repeated credential entry;
- Integrating VPN launch with the connection (so users don't separately connect VPN then RDP — the tool does it seamlessly);
- Injecting credentials to avoid exposing passwords;

- Enforcing role-based access to reduce clutter and risk;
- Surfacing frequent tasks in a straightforward UI.

By reducing the friction in doing things the secure way, organizations can prevent the dangerous workarounds that users otherwise adopt in the name of speed.

A well-designed remote connection management system will hide the complexity of security from the end-user, allowing them to be both safe and efficient.

Supporting collaboration and knowledge sharing

In many IT teams, knowledge about remote connections resides in personal silos — one senior admin "just knows" all the important server addresses and logins, for instance. This is not only a risk (if that admin leaves or is unavailable, productivity can grind to a halt) but also inefficient for team collaboration.

The challenge is ensuring that institutional knowledge of remote access is captured and shareable in a secure manner. Without a centralized system, new team members have to be onboarded by trading spreadsheets or notes about how to access various systems, which is slow and insecure.

A remote connection management platform should:

- Centralize all connection info, system notes, troubleshooting steps, and access rights in a single source of truth;
- Provision role-appropriate access so team members immediately see the resources they need;

- Standardize methods and workflows so everyone uses the same, up-to-date procedures;
- Enable session sharing and handoff to invite peers into live sessions or transfer control during complex incidents.

By making remote support a collaborative, well-documented process, IT teams can resolve issues faster and avoid duplicated effort.

In tackling these productivity challenges, the overarching theme is consolidation and simplification. The fewer moving parts IT professionals have to manage to do their jobs, the better their focus and output.

It's important to emphasize that productivity gains do not have to come at the expense of security or compliance — in fact, a unified remote connection management system tends to enhance all three areas.

In the next section, we'll see how combining all of the above best practices can lead to a holistic solution.

CONCLUSION: Resolving these challenges

Remote connection management sits at the intersection of productivity, security, and compliance — and this white paper has illustrated how challenges in each of these areas are deeply interrelated: weaknesses in one propagate to the others.

The remedy is a comprehensive strategy anchored by a centralized platform: one that ideally includes a credential vault with MFA, granular access controls, full auditability, wide protocol support with automation, an efficient interface, and accommodations for third-party and privileged access.

A shining example of this all-in-one approach is Devolutions' **Remote connection management solution** (spearheaded by **Remote Desktop Manager**) which epitomizes the features and benefits outlined above by centralizing connections, credentials, and access control; enabling one-click, vaulted session launch; and preserving complete audit trails across RDP, SSH, VNC, cloud consoles, and VPNs. For elevated accounts, **Devolutions' Privileged access management solution** adds privileged vaulting and workflows.

Approaching remote connection management as a unified discipline — integrating both policy and platform — enables organizations to mitigate risk, meet compliance obligations, and increase the efficiency of IT operations.

The final takeaway is one of empowerment: by addressing security, compliance, and productivity in tandem, IT leaders can transform remote connection management from a pain point into a competitive strength for their organizations.

WORKS CITED

1. Blandford, Andrea. 2022. "Working from Home Increases Cyberattack Frequency by 238%." ***Alliance Virtual Offices Blog***. March 14, 2022. https://www.alliancevirtualoffices.com/virtual-office-blog/remote-work-statistics-costs/.

2. Check Point Software Technologies Ltd. 2022. ***The 2022 Workforce Security Report***. Accessed September 5, 2025. https://pages.checkpoint.com/remote-workforce-report.html.

3. Cooper, Verena. 2025. "Compliance in Remote Access: Key Standards and Features." Splashtop Inc. Last updated August 30, 2025. https://www.splashtop.com/blog/compliance-in-remote-access.

4. CrowdStrike, Inc. 2025. 2025 ***Global Threat Report Executive Summary***. Accessed September 22, 2025. https://4datasolutions.com/wp-content/uploads/2025/03/CRWD-2025-Global-Threat-Report-Exec-Summary.pdf?

5. CyberArk Software. 2024. ***Identity Security Threat Landscape Report 2024***. Accessed September 9, 2025. https://www.cyberark.com/resources/ebooks

6. Gurucul. 2021. "Stop Misuse of Privileged Accounts: Identity Analytics with UEBA." July 19, 2021. https://gurucul.com/blog/a-one-two-punch-to-stop-misuse-of-privileged-accounts/.

7. Hitachi ID Systems, and Pulse Q&A. 2022. "Enterprises Lack Confidence in Their Secret and Password Management" [Infographic]. ***Bravura Security***, May 5, 2022. https://www.bravurasecurity.com/hubfs/Images/Infographics/Hitachi%20ID_2022-05-05_Enterprises%20lack%20confidence%20in%20their%20secret%20and%20password%20management_full.png

8. Integrated Research Ltd. 2023. ***The IT Time Crunch***. Accessed September 5, 2025. https://www.ir.com/hubfs/Guides/The%20IT%20Time%20Crunch%20-%20Final.pdf.

9. ironcore. 2019. "74% of Data Breaches Start With Privileged Credential Abuse." Securis. April 13th, 2019. https://securis.com/news/privileged-access-management/.

10. Krebs, Brian. 2014. “Target Hackers Broke in Via HVAC Company.” ***Krebs on Security***. February 5, 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

11. Malwarebytes Labs. 2020. ***Enduring from Home: COVID-19’s Impact on Business Security***. Accessed September 8, 2025. https://www.threatdown.com/wp-content/uploads/2024/04/enduringfromhome_report_final-1-1.pdf.

12. OpenVPN. 2024. “OpenVPN Quick Poll Remote Workforce Cybersecurity.” ***OpenVPN Blog***. September 24, 2024. https://blog.openvpn.net/remote-workforce-cybersecurity-quick-poll/

13. OWG. 2024. «Top 6 Challenges of Remote Access and How Your Business Can Overcome Them.» ***LinkedIn***. October 16, 2024. https://www.linkedin.com/pulse/top-6-challenges-remote-access-how-your-business-can-overcome-dazic/.

14. Rathnam, Lavanya. 2024. “7 Ways To Ensure Your Remote Access Strategy Is Compliant.” Planet Compliance. Last updated April 2, 2024. https://www.planetcompliance.com/it-compliance/7-ways-to-ensure-remote-access-strategy-is-compliant/

15. Verizon. 2025. ***2025 Data Breach Investigations Report: Executive Summary***. Accessed September 8, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf.

16. We Work Remotely. 2025. “Welcome To We Work Remotely’s State of Remote Work Report 2025!” June 19, 2025. https://weworkremotely.com/welcome-to-we-work-remotely-s-state-of-remote-work-report-2025.