THE REMOTE ACCESS PARADOX:

RealVNC's Remote Access Trends Report 2026

Data from RealVNC's survey of 190 IT leaders reveals why "free" is expensive, more tools mean less security, and your team is blind to the risks.

REALVNC®

TABLE OF CONTENTS

A NOTE FROM REALVNC ON THE 2026 REMOTE ACCESS TRENDS

At RealVNC, we know secure remote access is an essential tool in a world in which everything cyber security related changes at lightning speed. Our 2026 Remote Access Trends report highlights the growing risks and evolving demands facing today's organizations. We found that the way security incidents are seen by technology leaders and their employees differs, and this is impacting on the measures taken. We also revealed that open-source solutions often come with hidden costs when enterprise security and support are considered, and that the use of RDP, despite its security risks, remains high.

The most secure organizations are investing in layered, proactive defenses. However, the most secure of organizations might not be in the fields you would normally think of.

We remain dedicated to delivering trusted remote access solutions, that do not compromise security for the sake of sheer simplicity. Thank you for partnering with us on this journey.

The RealVNC Team

WHAT THIS REPORT INCLUDES

This report is built on the findings from a survey of 190 IT professionals, offering a balanced and insightful look at remote access in 2026. Participants represent a wide range of organizations: many work at mid-sized companies, with strong representation from both smaller businesses and larger enterprises, including the very largest organizations.

We surveyed a robust cross-section of roles, including IT Directors and Managers, CIOs and CTOs, Systems Administrators, Developers and Engineers, Security and Compliance leaders, and Operations professionals. This diversity ensures our analysis reflects both strategic leadership and hands-on technical perspectives, highlighting today's remote access challenges and emerging opportunities.

NOTE: This is a snapshot of 2026's remote access landscape, highlighting rising security risks, gaps in how incidents are perceived, the hidden costs of open-source tools, and the ongoing reliance on RDP. Built from insights shared by 190 IT professionals across diverse roles and organizations, it reveals where proactive security is thriving, and where vulnerabilities remain.

EXECUTIVE SUMMARY: THE HOUSE IS ON FIRE (AND YOUR SYSADMIN DOESN'T KNOW)

Let's imagine this scenario. We have a building where the fire alarm is ringing on the top floor, but the ground floor is completely silent. The executives in the penthouse are smelling smoke, scrambling for the exits, and calling the fire department. Meanwhile, the security guards in the lobby are sipping coffee, convinced it's just a quiet Tuesday.

This isn't a hypothetical scenario. According to our latest survey of 190 IT and security professionals, this is the current state of Remote Access at the start of 2026.

We uncovered a strange statistic: **81% of CIOs and CTOs report suffering a remote access security incident in the last two years.** Yet, when we asked Systems Administrators (these are the people whose hands are on the keyboards), **only 21% reported the same.**

How is it possible that leadership sees four times as many fires as the people managing the infrastructure?

This "Visibility Gap" is just one of several paradoxes defining the IT landscape as we enter 2026. Our research reveals a world where "free" software costs more, overall, than paid solutions, where adding security tools lowers your defense, and where the technology companies that should be building our future are running the most archaic, vulnerable infrastructure of all.

"This isn't a hypothetical scenario. According to our latest survey of 190 IT and security professionals, this is the current state of Remote Access at the start of 2026."

The purpose of this report is a double one. Apart from being informational, it is meant as a warning that the old ways of using remote access are not a risk worth taking with the threats lurking around the corner today.

EXECUTIVE SUMMARY: THE HOUSE IS ON FIRE (AND YOUR SYSADMIN DOESN'T KNOW)

Relying on legacy RDP or cobbling together open-source tools of questionable security is a risky practice. Confusing “activity” and “security” is dangerous, not inefficient. And, if you do so, it’s not a matter of whether a cybersecurity issue will affect you. It’s a question of when.

So, without further ado, here are the paradoxes that will determine whether your organization thrives or becomes a statistic in 2026.

With that said, the purpose of this report is a double one. Apart from being informational, it is meant as a warning that the old ways of using remote access are not a risk worth taking with the threats lurking around the corner today.

CHAPTER 1: THE "FREE" TOOL TRAP

The High Cost of Zero Cost

For decades, the open-source ethos has been the backbone of IT innovation. The promise is seductive: total control, infinite customizability, and, most importantly, zero licensing fees. "Why pay a vendor," the logic goes, "when we can spin up a free VNC server and manage it ourselves?"

Our data suggests that, when it comes to enterprise remote access, this logic is a trap.

The Open-Source Penalty

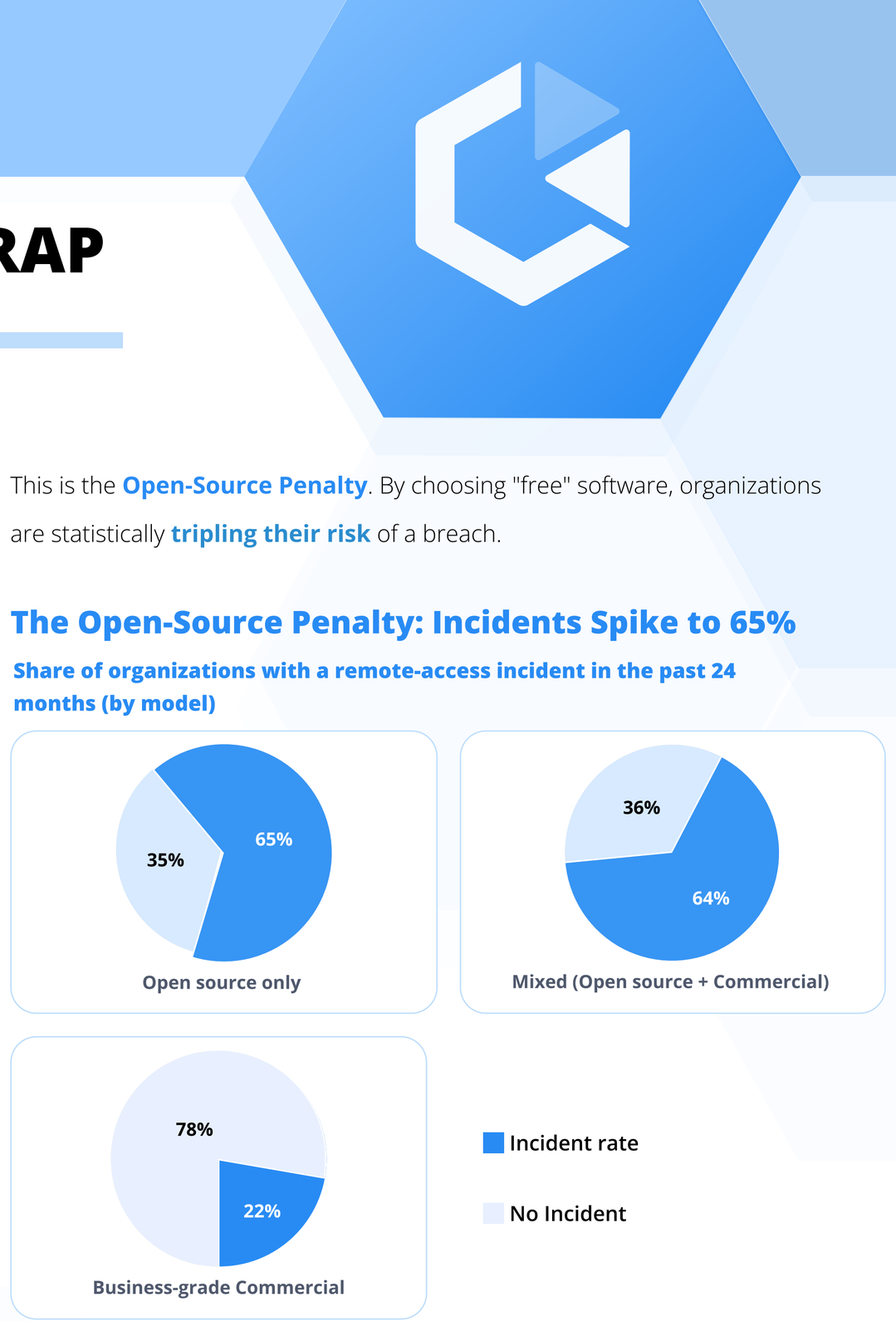
We investigated incident rates across three primary deployment models: purely commercial, purely open-source, and "mixed" environments. The results were rather grim.

Organizations relying on open-source or mixed models reported a security incident rate of **64–65%** in the last 24 months. By comparison, those using fully business-grade commercial solutions reported an incident rate of just **22%.**

This is the **Open-Source Penalty**. By choosing "free" software, organizations are statistically **tripling their risk** of a breach.

The Open-Source Penalty: Incidents Spike to 65%

Share of organizations with a remote-access incident in the past 24 months (by model)



CHAPTER 1: THE "FREE" TOOL TRAP

Think of Your Customers!

The Risks of Integrating Open-Source Remote Access Software into Your Products

Are you happy to take on the responsibility that a commercial dev team has to take by default?

Open-source remote access software may appear to be a flexible and cost-effective option, but it introduces critical security and operational risks. Without the safeguards and support of a secure remote access solution, organizations face vulnerabilities that can compromise their systems and compliance. Below are some risks to consider:

Supply Chain Vulnerabilities:

Open-source software relies on complex dependency stacks, which can introduce unintentional vulnerabilities or malicious code injected by bad actors.

AI-Generated Code Risks:

The rise of AI-generated patches in open-source projects increases the likelihood of vulnerabilities slipping through due to limited review resources.

Compliance Challenges:

Many open-source projects do not meet compliance standards (e.g., ISO27001), creating potential regulatory and operational risks.

Delayed Vulnerability Response:

Open-source projects often lack SLAs for resolving critical vulnerabilities, leaving organizations exposed for longer periods.

Resource Burden on Organizations:

Managing, updating, and securing open-source remote access software often falls on the customer, requiring significant time and expertise.

Guaranteed Performance

In RealVNC's experience, organizations are often disappointed with the performance that open-source solutions offer. This includes very high latency, laggy mouse, clipboard issues, or non-functional shortcuts among other things.

The lack of accountability, in the form of guaranteed support, from qualified technicians, turns this into another thing that ends up on the internal IT department's desk. An enterprise remote access solution ensures the necessary performance, as well as the ability to request features or know what's on its roadmap well in advance.

Bottom Line:

Integrating open-source remote access software can expose your organization to unnecessary risks. A secure remote access solution provides the support, compliance, and protection needed to safeguard your systems.

CHAPTER 1: THE "FREE" TOOL TRAP

Our Star Player: The Exhausted Admin

Why does free software lead to more breaches? It's not that the code is bad; open-source projects often have brilliant security foundations. The failure point happens when it comes to implementation.

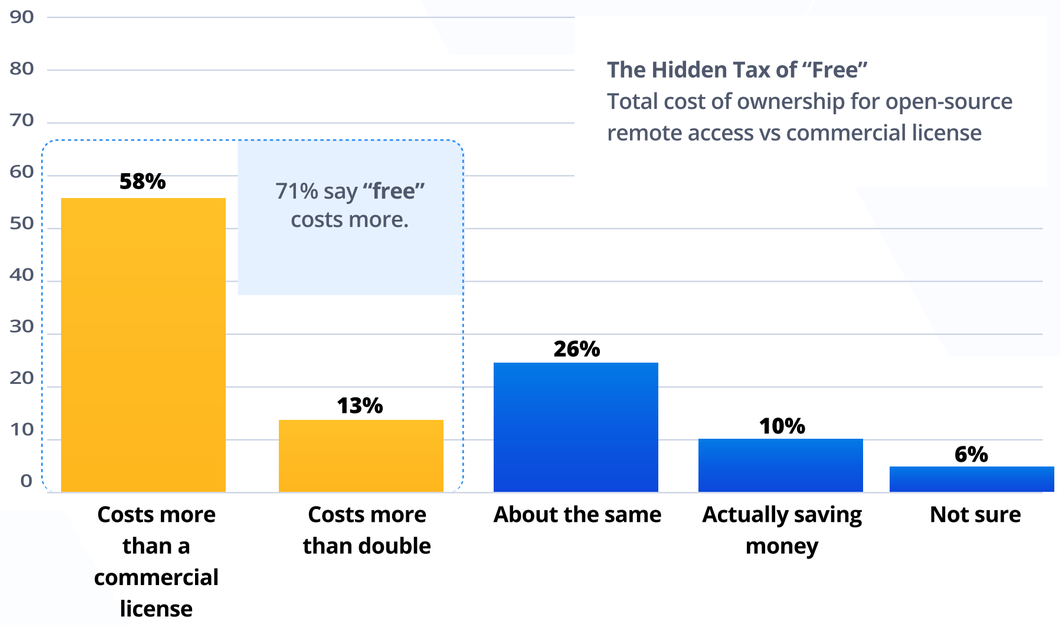
Meet "The Exhausted Admin." In a commercial environment, security patches are pushed automatically by the vendor. Vulnerabilities are patched before the admin even wakes up. But in an open-source shop, Exhausted Admin is responsible for everything. They must manually track CVEs, write scripts to deploy patches across hundreds of endpoints, troubleshoot compatibility issues with the latest Windows update, and manage encryption keys.

Eventually, they get tired. A patch gets missed. A configuration script fails on 10% of devices. And that is where the attackers get in.

The Hidden Tax of "Free"

The financial argument for open-source remote access collapses under scrutiny. We asked respondents to calculate the total cost of ownership (TCO) of their free solution, factoring in the man-hours required for maintenance, scripting, and troubleshooting.

- **58%** of open-source users admitted their "free" solution costs more than a commercial license would.
- **13%** said it costs more than double.
- Only **10%** believe they are actually saving money.
- **6%** are not sure.



CHAPTER 1: THE "FREE" TOOL TRAP

This is the hidden tax of free software. You are effectively paying premium rates for your own staff to act the way a software vendor would, distracting them from strategic initiatives to perform commodity maintenance and daily tasks.

The TCO Reality Check

1. **The Patching Hour:** How many hours per month does your team spend manually patching or updating remote access agents? (Multiply this by your hourly IT rate).
2. **The "Script Tax"**: How much time is spent writing, testing, and fixing deployment scripts that a commercial tool would handle natively?
3. **The Downtime Cost**: Our data shows open-source users face more "moderate to severe" downtime. What is the cost of one hour of lost productivity for your workforce?

The Main Takeaway:

If you are paying your smartest engineers to reinvent the wheel, "free" is the most expensive software you can buy. You're spending more time and money than it would cost you to pay for an enterprise solution that guarantees you what's better security anyway. Not to mention that those resources would be much better spent on making your customers happy.

CHAPTER 2: RDP AND THE "UNCANNY VALLEY" OF DEFENSE

Why "Good Enough" Security is Getting You Hacked

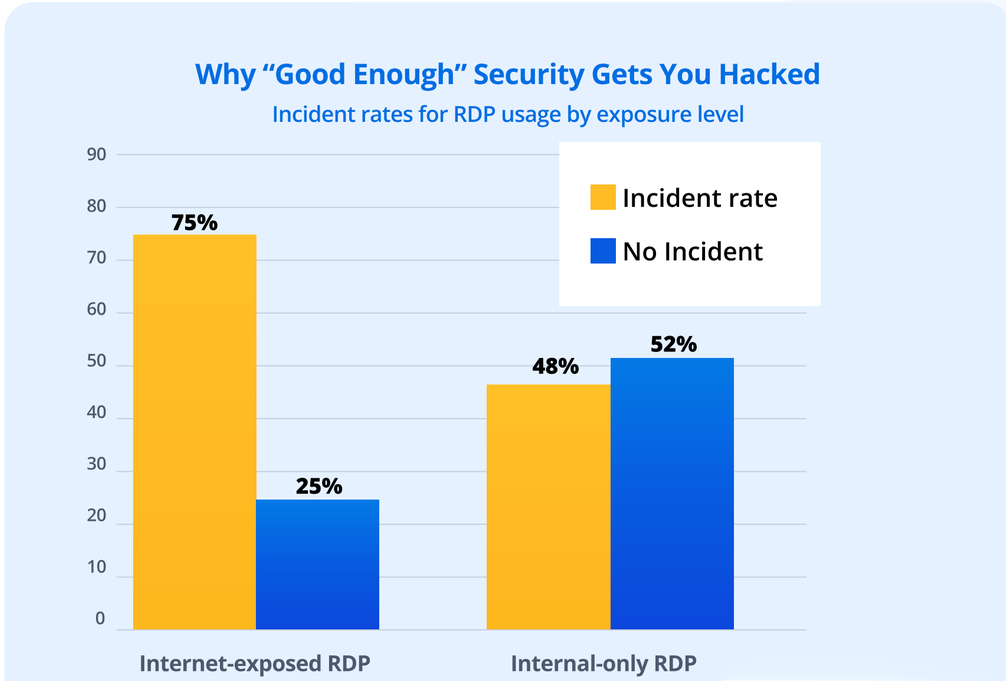
Remote Desktop Protocol (RDP) is the cockroach of the IT world; it survives everything. It's built into Windows, it's familiar, and it works. But it is also the favorite entrance for ransomware gangs.

Our survey found that while 35% of companies plan to stop using RDP, nearly **30% have no plans to change**. For those staying the course, the data reveals a terrifying truth about how we secure (or fail to secure), this protocol.

Security by Obscurity: A Death Wish

We found that **75%** of organizations with internet-exposed RDP suffered a security incident. This isn't surprising. What is surprising is the data regarding "internal-only" RDP usage. Even when not exposed to the internet, organizations using RDP reported a **48% incident rate**.

"For those staying the course, the data reveals a terrifying truth about how we secure (or fail to secure), this protocol. "



Why? Because RDP is often the vehicle for lateral movement. Once an attacker is inside via a phishing email, they scan for open RDP ports to jump from a laptop to a server.

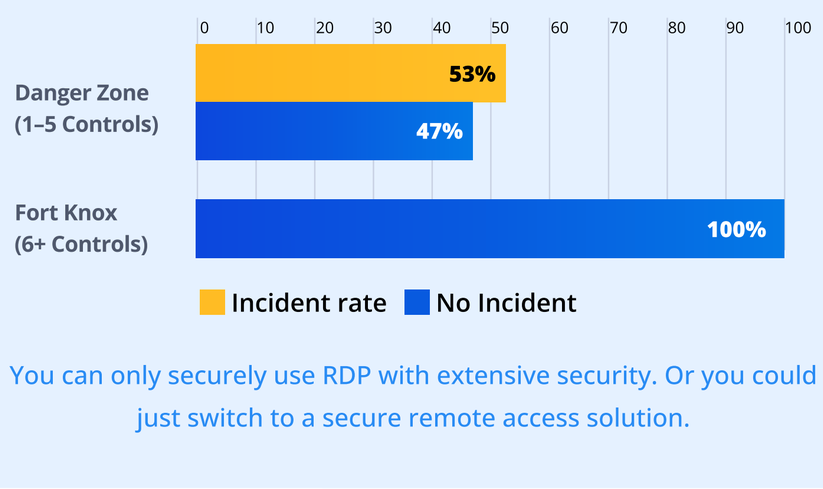
CHAPTER 2: RDP AND THE "UNCANNY VALLEY" OF DEFENSE

The Uphill Climb of RDP Security

The most critical insight from our data is the "Uncanny Valley" of RDP defense. We analyzed the relationship between the number of hardening controls (MFA, NLA, IP allowlisting, etc.) and incident rates.

- **The Danger Zone (1–5 Controls)**: Organizations that implemented a few basic controls, like perhaps changing the listening port from 3389 to 4444 or turned on NLA, reported a 53% incident rate.
  - *The Trap*: These measures are "Security by Obscurity." Changing a port does not fool a modern scanner like Shodan. These admins feel secure because they did something, but they haven't actually stopped the attack vectors.

- **Fort Knox (6+ Controls)**: The data shows a very important threshold. Organizations that implemented 6 or more layers of defense reported 0 incidents.
  - ***The Solution:*** There are two, really. The first one is doing it all: Multi-Factor Authentication (MFA), Network Level Authentication (NLA), a Gateway/ Bastion Host, Account Lockout policies, restricted IP lists, and centralized logging. Or there is a second one. Which is using a secure remote access solution instead of RDP.



You can only securely use RDP with extensive security. Or you could just switch to a secure remote access solution.

The Main Takeaway:

There is no middle ground. You cannot dabble in RDP security. If you aren't going to implement the full 6-layer stack, you really shouldn't be using it at all. Furthermore, if you decide to continue using it, keep in mind that you will need to allocate significant amounts of time and resources to keep it secure. It's for you to decide whether that is worth it or not.

Otherwise, you're exposing yourself and your customers to very serious security risks.

CHAPTER 3: THE GREAT DISCONNECT

The CIO is Screaming, The Admin is Silent

Let's return to the fire alarm analogy. Why did **81% of CIOs** report an incident while only **21% of Sysadmins did?**

This discrepancy is arguably the most dangerous finding in our report. It suggests a fundamental breakdown in communication and observability.

The Visibility Gap

- **The Definition Problem:** A Sysadmin might define an "incident" strictly. For example: Did the server crash? Did data get encrypted? If they caught a malware infection and cleaned it up, they might consider that "business as usual." The CIO, however, sees that as a near-miss compliance failure that needs to be reported to the board.
- **The Culture of Silence:** In many organizations, reporting a problem is seen as admitting failure. Sysadmins may be silently fighting fires, patching vulnerabilities, and restarting services without alerting leadership, fearing they will be blamed. This leaves the CIO thinking the environment is stable, right up until a catastrophic breach that can't be hidden.

"...Sysadmins may be silently fighting fires, patching vulnerabilities, and restarting services without alerting leadership"

CHAPTER 3: THE GREAT DISCONNECT

The Complexity Trap

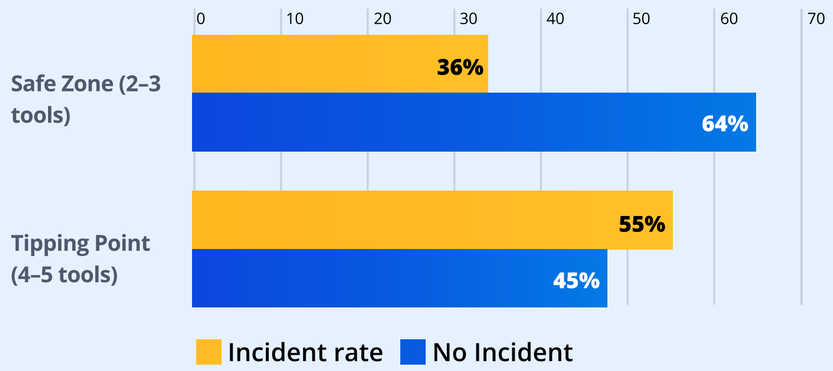
Part of this visibility problem stems from "Tool Sprawl." We found a direct correlation between the number of tools in use and the likelihood of failure.

- **The Safe Zone**: Organizations using **2–3 remote access tools** had the lowest incident rate (~36%).
- **The Tipping Point**: As soon as a 4th or 5th tool was introduced, the incident rate spiked to **55%**.

This is what we call the **Complexity Trap**. Every additional tool creates a new "blind spot." It's another console to check, another vendor to update, and another set of policies to misconfigure. A SysAdmin managing five different remote access tools cannot possibly have a unified view of who is connected to what, using what specific tool. Complexity is the enemy of security.

Title: The Complexity Trap

Incident rates rise with the number of remote access tools in use



Adding more tools increases risk by over 50%.

Advice for CIOs

Don't wait for a report. Walk over to your Sysadmin's desk (or grab them into a video call) and ask this specific question today:

"I'm not asking for a status report. I want to know: What was the closest call we had in the last 6 months? What almost went wrong?"

This question grants permission to discuss near-misses without fear of punishment. It turns "silence" into "intelligence."

CHAPTER 3: THE GREAT DISCONNECT

The Main Takeaway:
The more remote access tools (and especially free remote access tools, with zero auditing capabilities), you use, the bigger the chances of something happening. And that's because your team doesn't have a single pane of glass to look at when it comes to remote access. They have several, in different rooms, possibly situated in different locations. The more tools, the higher the chances of an incident.

The solution is simple: a single, secure remote access solution, with the right auditing capabilities.

CHAPTER 4: THE HUBRIS OF TECH

Why Technology Companies Are the Most Vulnerable

If you assumed that technology companies (Software vendors, SaaS platforms, and MSPs), would have the most sophisticated security, you would be wrong.

Our data uncovered a phenomenon we call the **"Cobbler's Children Effect."** The industry sectors we typically associate with "legacy" thinking, like **Manufacturing and Finance**, are actually running the most secure, professionalized remote access operations. The "modern" Tech sector is lagging.

Data: Confidence vs. Competence

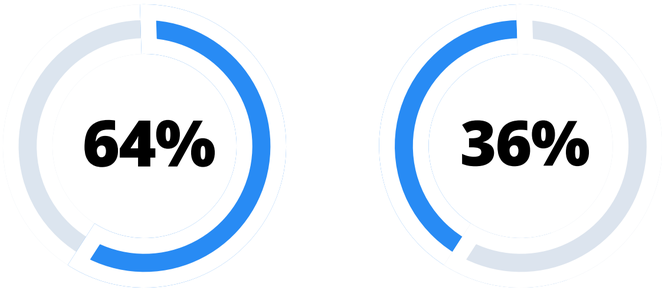
- **Tech/SaaS Companies:** They are the heaviest users of risky "mixed" and open-source models (64%).
- **Manufacturing & Finance:** They overwhelmingly prefer **Business-grade commercial solutions (~70%)**.

> "The industry sectors we typically associate with "legacy" thinking, like Manufacturing and Finance, are actually running the most secure, professionalized remote access operations. "

Tech vs. Regulated Sectors: Who Chooses Risky Remote Access?

Share of organizations using mixed/open source vs. business-grade solutions

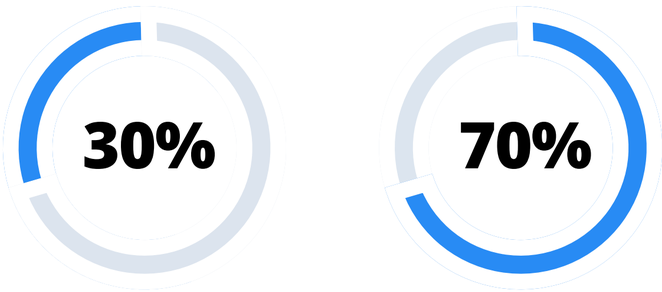
Tech/SaaS companies



Mixed/Open source models:

Business-grade commercial:

Manufacturing & Finance



Mixed/Open source models:

Business-grade commercial:

CHAPTER 4: THE HUBRIS OF TECH

Why? It comes down to **Hubris vs. Regulation.**

Manufacturing and Finance are regulated industries. They have auditors (HIPAA, SOC 2, ISO) breathing down their necks. They cannot afford downtime because downtime equals lost production or lawsuits. Therefore, they treat remote access as a critical utility: they pay for the best tool, they demand an SLA, and they move on.

Technology companies, on the other hand, often suffer from "Not Invented Here" syndrome. They believe they have the in-house talent to stitch together open-source tools, write custom wrappers, and manage security themselves. They view commercial tools as an unnecessary expense.

The result? The tech sector is taking on massive, unmanaged risk. They are building complex machines of remote access that are fragile, expensive to maintain, and, as our incident data proves, highly prone to failure.

"...treat remote access as a critical utility... pay for the best tool, ... demand an SLA, and they move on"

CHAPTER 4: THE HUBRIS OF TECH

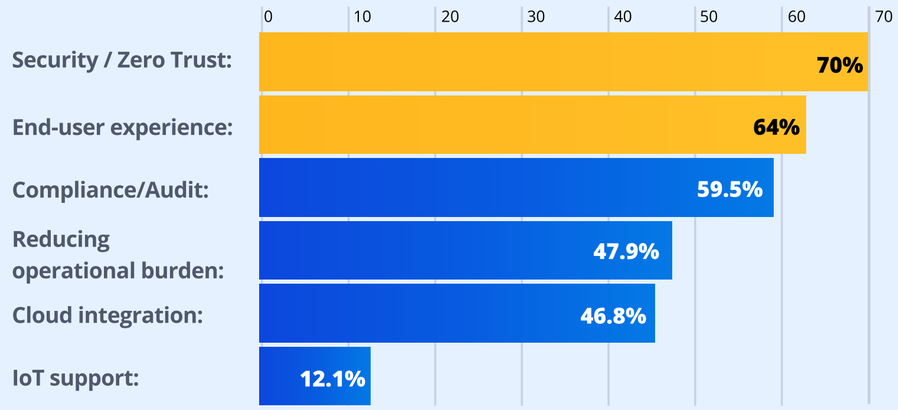
The Strategic Shift: From Utility to Enabler

Despite these challenges, the market is waking up. We are seeing a shift in how remote access is perceived.

- **42%** of respondents now view it as a "Strategic Enabler". This is a competitive advantage, that improves agility, rather than just a utility.
- The top priorities for 2026 are **Zero Trust (70%) and End-User Experience (64%).**

Top Priorities for Remote Access in 2026

What IT leaders are focusing on this year

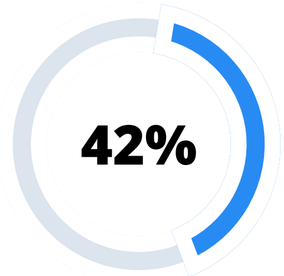


Security and user experience lead the agenda for 2026.

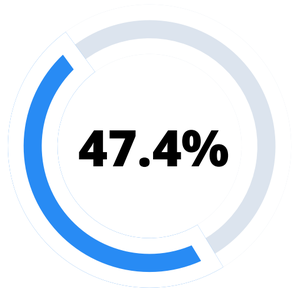
Remote Access as a Strategic Enabler

How organizations perceive remote access in 2026

Strategic Enabler:
Nearly half still see remote access as a utility, **but 42%** now view it as strategic.



Competitive Differentiator



Tactical Utility

“The market is waking up. We are seeing a shift in how remote access is perceived.”

CHAPTER 4: THE HUBRIS OF TECH

This is the path forward. The winners in 2026 will be the companies that stop tinkering with "free" tools and start treating remote access as a premium product experience for their employees. They will prioritize speed, invisibility, and rock-solid security.

The Main Takeaway:

Sometimes, it’s better to be a boring manufacturer than a "clever" tech company. According to our research, tech companies lack more than organizations in other industries when it comes to cyber security. One of the reasons is the stringent regulation that other fields are facing, forcing them to pay for the most secure and compliant tool they can get their hands on. But that’s not an excuse for tech companies.

The Tech Sector Strategy:

Tools: Custom scripts + Open Source.
Mindset: "We can build it better ourselves."
Outcome: High complexity, high incident rate.

The Manufacturing Strategy:

Tools: Commercial, supported platforms.
Mindset: "We need it to work, guaranteed."
Outcome: Lower complexity, higher stability.

REALVNC'S TAKE: ESCAPING THE PARADOX

The data from our 2026 outlook is unequivocal. The era of "good enough" remote access is over. The paradoxes we uncovered prove that the cheapest tools are often the most expensive, and the most familiar protocols are the most dangerous.

To thrive in 2026, you must break the following paradoxes:

Abandon the "Free" Fallacy: Recognize that the operational overhead of open-source tools is a tax you cannot afford to pay. The result? The tech sector is taking on massive unmanaged risk. They are building complex machines of remote access that are fragile, expensive to maintain, and, as our incident data proves, highly prone to failure.

Stop Tinkering: If you are a tech company, swallow your pride. Buy the tool that works so your engineers can focus on building your product, not fixing your remote access.

Simplify the Stack: Consolidate your tools. If you have more than three ways to get into your network, you have too many.

Close the Visibility Gap: Align your C-Suite and your Sysadmins on what constitutes a "breach." Stop punishing bad news.

The future of remote access is secure, simple, and strategic. But to get there, you must stop fighting fires and start building a fireproof house.

LEARN MORE

Find out more about the topics we discussed in this eBook by taking a look at these other great resources from RealVNC:

The Ultimate Toolkit for Remote Access Software Buyers

Click Here to View

Master Remote Access Integration:

The RealVNC OEM & SDK Playbook

Click Here to View