EMERGING THREATS IN MANUFACTURING

High Ambition, Ageing Infrastructure

TABLE OF CONTENTS

INTRODUCTION

Manufacturing organisations occupy an unusual position in RealVNC's research: a sector with genuine, growing security ambition, sitting on top of infrastructure that has not kept pace with the threats it now faces.

Manufacturing respondents report the second-highest confidence in their current security of any industry, and some of the strongest forward-looking commitments to employee training, Zero Trust, and compliance readiness in the entire survey. Yet **53% of manufacturing organisations** reported a remote access incident in the **past 24 months**, and platform upgrades, the infrastructure that security controls actually run on, are the most deprioritised task of any sector, a gap that matters to IT and infrastructure teams as much as security, since the same ageing systems that create security exposure are the ones production depends on.

This report explores the unique remote access security challenges facing the manufacturing sector, highlighting where confidence, capability, and capacity diverge.

Should you want to get a picture of what things look like for other industries, feel free to **check out our free Emerging Threats in Remote Access Security Report and Webinar.**

EXECUTIVE SUMMARY

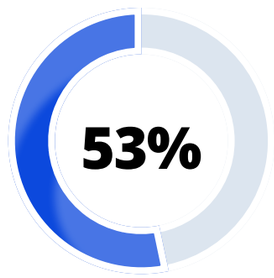
RealVNC commissioned this survey in Q1 2026. The purpose was simple: to understand how IT professionals across industry sectors are perceiving and preparing for emerging threats in remote access security. 323 qualified respondents, all individuals working in organisations that currently use remote access solutions, completed the survey. **Manufacturing organisations made up 11% of respondents.**

The overconfidence finding is not incidental. It runs through every segment of the survey. It's in every role, every industry, every size band, and it points to a structural problem in how security posture is assessed. Teams are measuring activity, not outcomes. They are counting controls deployed, not testing whether those controls actually hold under real-world conditions.

Manufacturing is falling behind on infrastructure modernisation. In Manufacturing, **76% express high confidence in current security**, the second highest rate of any industry, yet the incident rate is **53%**, and **62%** of confident manufacturing respondents have been breached. Manufacturing respondents show the strongest commitment to Zero Trust of any sector not in the MSP/IT Services category, with **74%** citing it as a top priority, and only **29%** have implemented it. Platform upgrades are the most deprioritised task at **56%**, the highest of any sector, and manufacturing is the only industry where platform modernisation outranks security hardening as the dominant operational sacrifice.

This edition brings together the manufacturing findings from RealVNC's Emerging Threats in Remote Access Security report. A closing section then looks at how an on-premise approach to remote access can help address several of the specific gaps this research identifies.

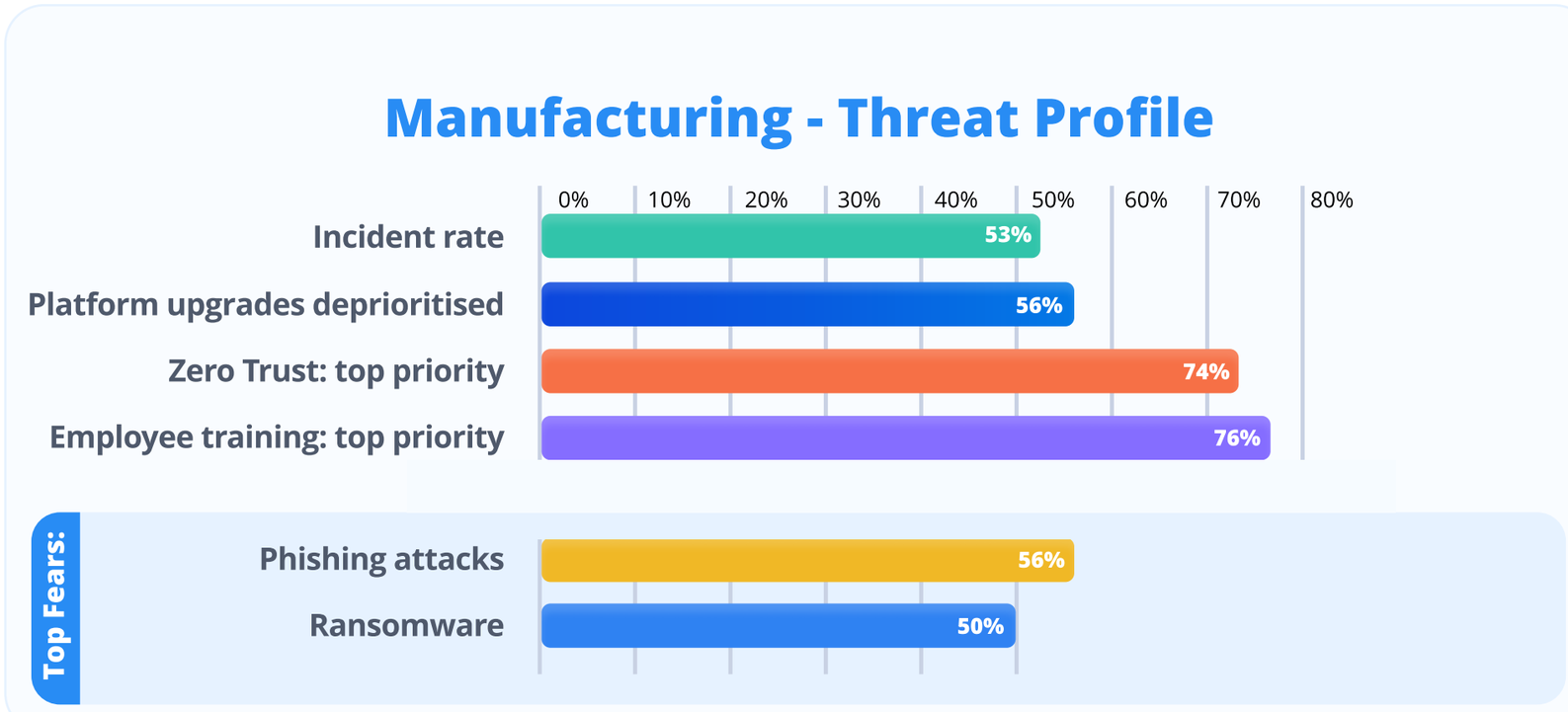
Manufacturing respondents show the strongest commitment to Zero Trust of any sector not in the MSP/IT Services category



Manufacturing organisations reported a remote access incident in the past 24 months.

MANUFACTURING: INFRASTRUCTURE DEBT AND ACCELERATING EXPOSURE

Manufacturing respondents combine a **high incident rate (53%)** with the most significant platform infrastructure lag of any industry. Platform upgrades are the most deprioritised task at 56% (the highest of any sector), and manufacturing is the only industry where platform modernisation outranks security hardening as the dominant operational sacrifice. The implication is a sector operating on ageing infrastructure in an environment of growing threat sophistication.



Ransomware (50%) is a more prominent fear in manufacturing than in most other industries, likely reflecting the operational consequences of production downtime that a successful attack can cause. When experiencing incidents, **56%** involved **vulnerability exploitation** and **56%** involved a **security breach**. That's the joint highest breach rate of any industry alongside retail. Manufacturing's compliance landscape is relatively light compared to healthcare or finance; ISO 27001 (35%) is the most common standard, with 15% reporting no applicable compliance obligations. This may contribute to a lower sense of urgency, despite high exposure.

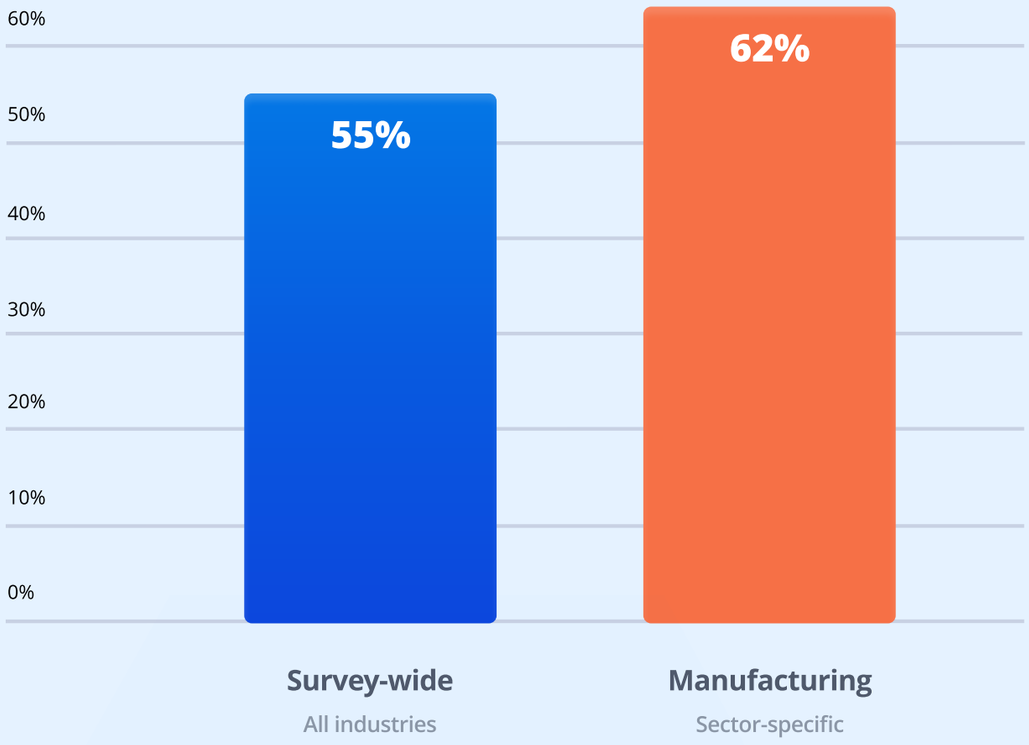
Manufacturing respondents show the strongest commitment to Zero Trust of any sector not in the MSP/IT Services category, with **74%** citing it as a top priority. **Budget (50%)** and **lack of skilled personnel (44%)** are the twin obstacles, making this a sector that knows what it needs but faces the most significant resource constraints in delivering it outside the smallest company sizes.

THE CONFIDENCE PARADOX

Across the full survey population, when asked how confident they are that their current remote access approach meets their organisation's security needs, **66% of respondents** described themselves as very or extremely confident. **Only 10%** expressed low confidence. Taken at face value, this would suggest a market that is managing its risks effectively. The incident data immediately complicates this picture: of respondents who described themselves as very or extremely confident, **55%** had still experienced a remote access incident in the past 24 months.

Overconfidence and breach rate

Survey-wide vs. Manufacturing, percentage of of respondents who rated themselves very/extremely confident, but still had an incident in the past 24 months



In Manufacturing, **76% express high confidence** in current security. It is the second highest rate of any industry, yet the **incident rate is 53%**, and **62%** of confident manufacturing respondents have been breached. The sector's comfort with its current posture is not matched by its outcomes.

Across the survey, this pattern points to a measurement problem more than a security problem: teams are measuring activity, not outcomes, counting controls deployed rather than testing whether those controls hold under real-world conditions.

MANUFACTURING: INFRASTRUCTURE GAPS COMPOUND EXPOSURE

Manufacturing's intention gap is shaped by infrastructure debt more than any other factor. Platform upgrades have been deprioritised **by 56%** of respondents and security hardening **by 47%**.

Security controls are being deployed on infrastructure that is itself overdue for modernisation. This is a combination that amplifies risk.

Encryption at rest has been implemented **by only 29%** of manufacturing respondents, which is the lowest rate in the industry breakdown, and session recording **by 26%**. Audit logging at **38%** is also below average. These are foundational controls for any organisation subject to regulatory scrutiny or operating technology environments where access control matters. The combination of a **74% Zero Trust priority rating** and **29% Zero Trust implementation rate** represents a gap that is only likely to widen as the threat environment evolves.

> Encryption at rest implemented by only 29% — the lowest rate in the industry breakdown.

Budget (50%) and **lack of skilled personnel (44%)** are twin obstacles. Manufacturing is a sector that knows what it needs, cannot fully fund it, and does not have the people to deliver it without additional investment.

OPERATIONAL BURDEN

One of the most counterintuitive findings in the entire survey is this:

> The effort of managing remote access security challenges is actively preventing organisations from becoming more secure.

The time and resource devoted to dealing with security problems is consuming the bandwidth that could be used to prevent them.

This is at its worst in Education, where **60%** of respondents deprioritise security hardening, which is the highest rate of any sector. **Manufacturing (47%)** and **technology (52%)** also show high rates. In each case, the operational drain of managing the existing security challenge is consuming the investment that would reduce future challenges.

Across the survey, AI adoption is accelerating, but unevenly: **39%** of respondents are already using AI-powered tools to support remote access security monitoring or threat detection. Adoption varies significantly by sector, MSPs lead at **51%**, followed by technology organisations at **47%** and manufacturing at **44%**, all above the survey-wide figure.

LOOKING THREE YEARS AHEAD

The survey's forward-looking questions reveal a market that is clear-eyed about what needs to change, and equally clear about what is getting in the way. The tension between aspiration and reality is visible in every segment, but the specific shape of that tension varies significantly by industry and company size. Understanding those differences is the starting point for building security programmes that are realistic, rather than just ambitious.

Across the full survey population, improving employee training **(66%)**, enhancing compliance readiness **(60%)**, implementing Zero Trust architecture **(58%)**, and consolidating remote access tools **(57%)** are the top four priorities. The convergence around these four themes is not coincidental: each addresses a different dimension of the same underlying structural problem. Training addresses the human attack surface. Compliance readiness addresses the governance gap. Zero Trust addresses the architecture gap. Tool consolidation addresses the complexity that makes all three of the others harder to deliver.

Manufacturing shows some of the strongest forward-looking commitments in the survey: employee training **(76%)**, Zero Trust **(74%)**, and compliance readiness **(68%)** are all above the cross-industry average. The intent is genuine and urgent. But the obstacles are the most constraining of any sector: budget **(50%)** and lack of skilled personnel **(44%)** rank one and two.

> Manufacturing's combination of high intent and high constraint creates a particular risk: organisations that know what they need, cannot fully fund it, and cannot find the people to deliver it are likely to make partial investments.

These certainly will create the appearance of progress, but they won't fully close the gaps. Platform upgrades, **deprioritised at 56%**, are a visible symptom of this dynamic. The infrastructure work that would support modern security architectures keeps getting pushed behind more immediate demands.

KEY TAKEAWAYS

Manufacturing understands the threat landscape and has some of the clearest forward-looking commitments of any sector: strong Zero Trust ambition, high training priority, and above-average compliance readiness.

However, ambition alone is not translating into stronger outcomes.

The research points to a recurring challenge: manufacturing security teams know what needs to be done, but budget constraints, a shortage of skilled personnel, and infrastructure that is itself overdue for modernisation continue to slow progress.

> As threats evolve and production environments become more connected, the organisations most likely to succeed will be those that treat infrastructure modernisation as a prerequisite for security investment, rather than a parallel track.

These findings matter beyond the security function. The same infrastructure gaps that create security exposure also carry operational risk. A remote access incident on a production system doesn't just raise a security question, it raises a downtime question, which is why this is as much an IT and infrastructure conversation as a security one.

The closing section of this report looks at one practical starting point: how an on-premise approach to remote access can help close some of the specific gaps identified here.

> "Manufacturing teams know what they need. The limiting factor is budget, people, and infrastructure that has not caught up."

ON-PREMISE REMOTE ACCESS: A PRACTICAL NEXT STEP

For organisations working through the gap between security ambition and available budget, people, and infrastructure, an on-premise approach to remote access is worth considering.

Keeping remote access on-premise means session data, credentials, and connection activity stay inside an organisation's own network instead of an outside cloud provider. That matters for data sovereignty as much as for security: it reduces dependency on external connectivity and outside infrastructure, and keeps control over security settings and access permissions inside the organisation rather than a third party. Layered with strong encryption, two-factor and device-level authentication, and the option of an air-gapped deployment, it also supports the compliance readiness priority that manufacturing respondents flagged for the years ahead, including alignment with frameworks like ISO 27001 and GDPR.

What to Look For in a Manufacturing Remote Access Platform

Before choosing a platform, it's worth being specific about what to look for: granular access control and network segmentation, a full audit trail of who connected to what and when, centralised visibility across sites and devices, straightforward identity and license management, and the option to keep it all on-premise. The five capabilities below map directly onto those criteria.

Below are five specific pain points this report surfaces, and how the RealVNC On-Prem Management Console addresses each one.

1 Zones, for Segmented Networks

Manufacturing environments are rarely flat: office IT, plant-floor systems, and third-party vendor equipment often need to stay apart. Zones let you enforce stricter rules for how traffic flows across segmented or complex topologies, and edit them as your network evolves. It's a practical route toward the Zero Trust architecture that 74% of manufacturing respondents cite as a top priority, without a full overhaul of existing infrastructure.

2 Who Accessed That, and When?

When an incident happens, or an auditor asks who connected to a particular machine or line and when, you need an answer fast. Audit logs give real-time records of every connection: when it started, whether authentication succeeded, and when it ended, searchable by date or event type and exportable as a CSV file. Because users sign in with individual credentials, every connection, including those from external vendors and contractors, ties back to a named person.

3 A Quick Health Check of the Environment

Rather than piecing together information from multiple sources or sites, the Dashboard gives IT admins a single view of license usage, active and dormant devices, and session counts across the environment. That makes it easier to catch problems, like usage creeping toward a limit, before they escalate. This is useful for a sector managing equipment across multiple plants and sites.

4 Lots of Licenses and Endpoints

Manufacturing environments often mean large numbers of endpoints spread across sites, some with limited or no internet connectivity. Licensing is held centrally, so admins upload a key once and devices pick it up automatically when they check in, removing the need to deploy licenses across every server individually, a task that only gets more tedious as the endpoint count grows.

5 A Staff Member Left, We Need to Tidy Up

Manufacturing environments often rely on contractors, shift workers, and third-party vendors who need temporary access to specific machines or systems. When someone leaves or a contract ends, the console makes it easy to remove access and cancel a device's license without uninstalling anything, including bulk user management via CSV upload. Credentials and licenses don't linger as security or cost liabilities.

None of this replaces the budget and skilled personnel manufacturing teams still need to invest in. For organisations looking to reduce their attack surface and bring some of these findings under control, an on-premise approach, including the centralized control the On-Prem Management Console provides, is a practical place to start.