REMOTE ACCESS IN MANUFACTURING:

Concerns, Challenges, & Guidance in 2024

REALVNC®

WHITE PAPER

The Manufacturing industry is a unique beast from a technology perspective; the equally important information technology (IT) and operational technology (OT) environments alone make it vastly different from almost every other industry. And then there's the need to support, secure, and access those environments that add to the complexity; the disparity of devices, operating systems, and communication protocols only makes keeping a Manufacturing business operational that much more difficult.

Remote Access solutions have made the work accomplished by IT, OT, and Security teams much easier for nearly every aspect of their jobs – from supporting employees to providing access to servers and network devices within the IT environment and providing access to OT devices. The everyday regular user also benefits from Remote Access, as it enables them to be productive – whether it's internal system access to remote workers or performing process tasks like securely transferring files.

Given the unique IT/OT environment within Manufacturing organizations, the Remote Access solution chosen has the unique ability to impact an organization's state of security and productivity materially – positively or negatively – while also impacting the bottom line.

In this paper, we'll look at whether Remote Access is meeting the needs of the Manufacturing industry, where the challenges are, and what Manufacturing organizations can do to improve their current state of security and productivity through the use of Remote Access solutions.

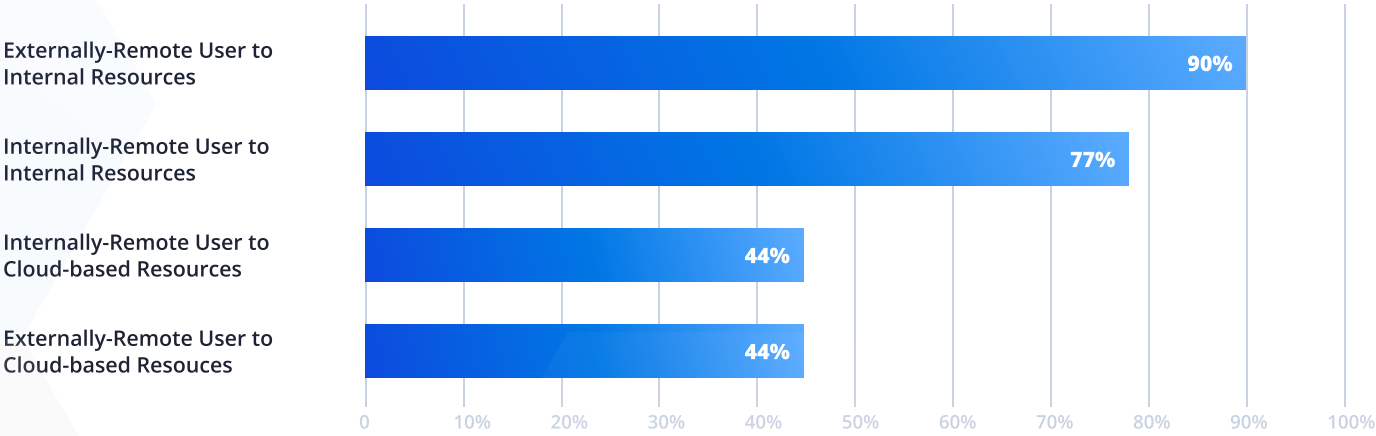
To provide context, we surveyed over 450 members of IT, ranging from Support Desk Analysts all the way up to IT executives, from within the Manufacturing industry to better understand how organizations are using Remote Access, what are the overarching top concerns, and how the use of Remote Access can be improved to overcome current challenges.

Let's begin with a brief overview of how Manufacturing utilizes Remote Access.

MANUFACTURING'S USE OF REMOTE ACCESS

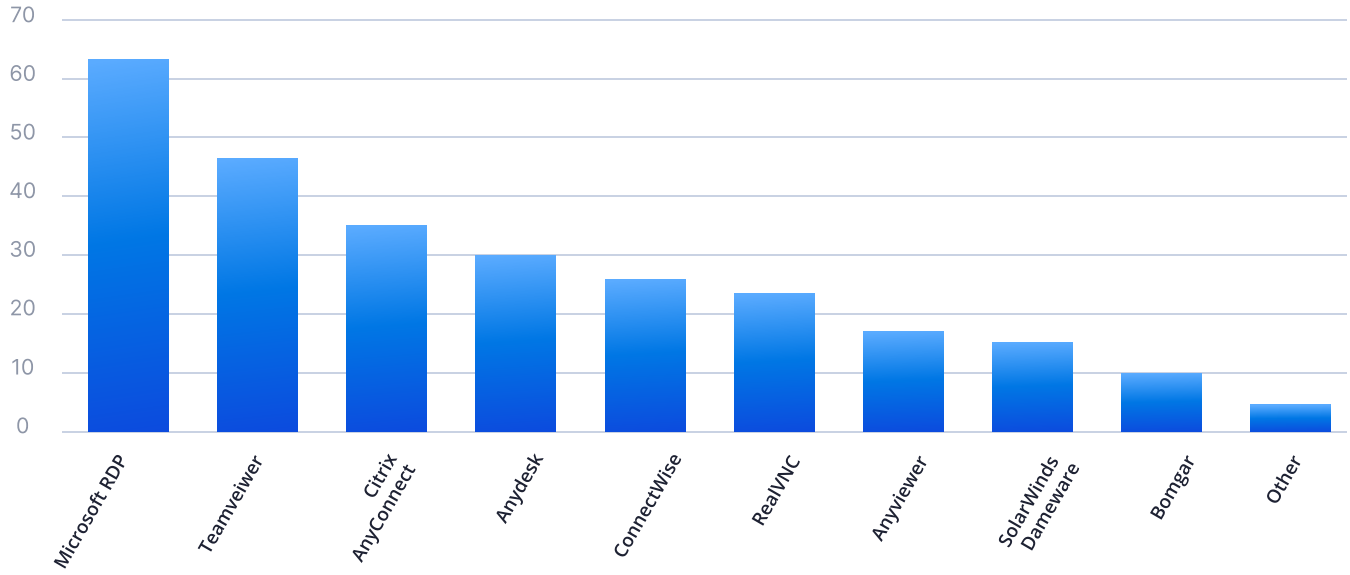
A part of every Manufacturing organization's operation is not unlike organizations in any other vertical industry where Remote Access solutions are regularly used. According to our recently released State of Remote Access Security report, in 73% of Manufacturing organizations, Remote Access solutions are used by IT, and in 68% of them, regular non-IT users also utilize it.

When digging a bit deeper into the data in the same report (as shown below), 90% of Manufacturing organizations are using Remote Access to provide *externally remote users access to internal resources* – this is much higher than the average of 74% across all industries. A little over three-quarters (77%) of them also use Remote Access to provide *internally remote users access to internal resources,* which aligns with the overall average. Manufacturing's use of Remote Access to connect users to cloud users is much lower (44% of organizations) than the average (around 57% of organizations). An explanation could be the use of direct access to connect to various pieces of equipment, allowing the data to remain on the organization's network.



WHICH SOLUTIONS ARE IN USE?

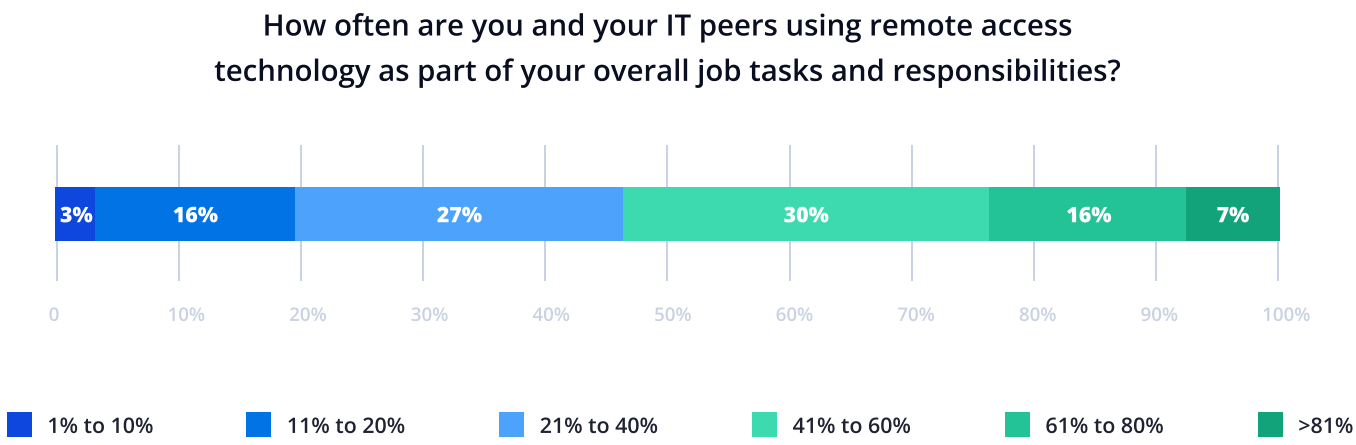
Then there's the question of which Remote Access solutions are being used. According to the survey, Manufacturing organizations use an average of just under three different solutions. The following chart summarizes the percentage of organizations using a specific Remote Access solution:



"...Manufacturing organizations use an average of just under three different solutions."

IT’S USE OF REMOTE ACCESS

Let's focus momentarily on Manufacturing's use of Remote Access by IT. According to our most recent survey of Manufacturing IT, IT uses Remote Access an average of around *42% of the time* to accomplish their job, with the breakdown of that use shown below.



And according to respondents, *this dependence on Remote Access will increase by an average of 26%* in 2024. We found that IT uses Remote Access for four primary use cases:

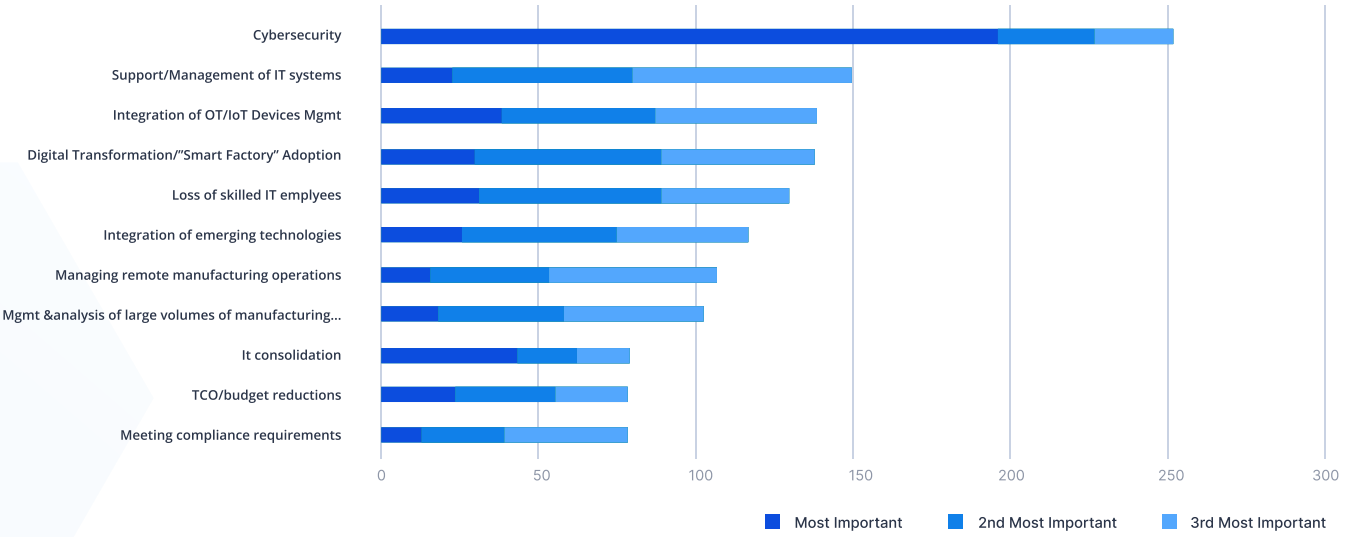
- Remote access to servers and network devices
- Remote desktop access of employee devices
- Remote monitoring of manufacturing equipment maintenance
- Remote access to manufacturing devices & equipment

With Remote Access playing such a critical role in what will end up being over half of the time IT spends performing their job in 2024, organizations should consider how Remote Access should be more than just a tool used to access remote hosts, rather than one that’s playing a key role in how organizations solve their major IT challenges.

MANUFACTURING'S BIGGEST IT/OT CHALLENGES

While IT within a Manufacturing organization has many priorities similar to other industry verticals, there's an entirely different dynamic to every challenge faced because of the addition of OT (Operational Technology) environments. Our recent survey asked organizations to rank the top 3 most critical technology issues facing Manufacturing. *As shown below, cybersecurity was the top priority; the support and ongoing management of IT systems ranked second; and integrating the management of specialty devices, IoT devices, and sensors that control manufacturing equipment* ranked third.

What are the most critical overall IT, OT, & technology issues facing the manufacturing industry in 2024?



With Remote Access potentially having a material impact on an organization's state of cybersecurity and IT's productivity because of the wide use of Remote Access within Manufacturing, it's vital to find ways to ensure Remote Access actually *improves* an organization's security and operations. So, let's look at the top 3 most critical overall IT, OT, & technology issues facing the manufacturing industry in 2024 and see how Remote Access can help be part of the solution.

CYBERSECURITY

It's a no-brainer that this should be the top concern for Manufacturing. Take **the ransomware attack that targeted the $25 billion U.S.-based manufacturer Johnson Controls,** which produces fire, HVAC, and security equipment for buildings. The 2023 attack sought a $51 million ransom and took the company nearly two months to address once detected, affecting operations and public shareholder filings.

Because of the mix of IT and OT, attacks like the one on Johnson Controls can put manufacturing companies out of business or, at the very least, in a world of financial hurt. In our survey, nearly half of organizations responded with this concern at #1, dwarfing every other concern by as much as 13:1! And rightly so, as Manufacturing is a very popular target of cyberattacks:

"The 2023 attack sought a $51 million ransom and took the company nearly two months to address once detected"

- In North America and Europe, Manufacturing is the second-most targeted industry[1].
- Within industries supporting OT, Manufacturing is the most targeted[1].
- Of all ransomware attacks in 2023, Manufacturing was the most targeted[2].

44% of Manufacturing organizations faced at least 1 cyberattack in the last 12 months, with 19% of organizations experiencing 10 or more[3].

The presence of Remote Access solutions creates risk for the organization. This is because Remote Access has the potential to facilitate initial access by a remote threat actor into the IT environment and can also be used for lateral movement to both IT and OT systems and devices.

The concern for the organization's state of cybersecurity – and the role Remote Access plays – was a theme that resonated throughout our survey responses. The top concern organizations have with their existing Remote Access solution or solutions is *solution security* for 59% of organizations.

[1] IBM Security X-Force, Threat Intelligence Index (2023)
[2] Guidepoint Security, Ransomware Report Q3 2023 (2023)
[3] RealVNC, State of Remote Access Security Report (2023)

CYBERSECURITY CONTINUED

In our State of Remote Access Security report, we asked if any of the following seven security controls were in use:

- Authentication against AD, via RADIUS, TACACS, etc.
- Multi-factor authentication (MFA)
- Policy-based access control
- Least privilege / Zero Trust
- Session encryption
- Session auditing
- Single Sign-On

On average, Manufacturing organizations use between two and three security controls, with MFA (used by 67% of organizations), session encryption (54%), and single sign-on (48%) being the most popular.

So, how can Remote Access improve the organization's cybersecurity stance?

IMPROVING CYBERSECURITY WITH REMOTE ACCESS

Let's consider the two most common misuses of Remote Access in cyberattacks that have been previously mentioned: initial access and lateral movement. To help mitigate the risk of misuse for either of these threat actions via your Remote Access solutions, consider the following recommendations:

Make Security a Remote Access Solution Priority

41% of manufacturing organizations didn't even choose solution security as a strength of their current solution, focusing more on ease of use and *speed/performance*. If your organization sits in that 41%, it's time to realize that the security of your Remote Access solution is as critical (if not more critical) as its great functionality is. Otherwise, all you have is a fantastic solution that will likely provide threat actors with relatively easy access to your network.

Join the MFA Crowd

If you're still in that one-third of organizations that do not have multi-factor authentication implemented so that all Remote Access logons require a second authentication method, it's time you join it.

Implement More Security Controls

As the solution(s) you have allows, consider putting additional controls in place to secure better initial authentication, better control access to and use of a remote session, and provide better oversight and accountability to remote session use.

Be Concerned About RDP

Just over two-thirds of Manufacturing is still using RDP. RDP! You know... that protocol that cybercriminals LOVE to take advantage of for initial access and lateral movement! You should strongly consider eliminating it entirely in favor of another Remote Access solution with solid security controls.

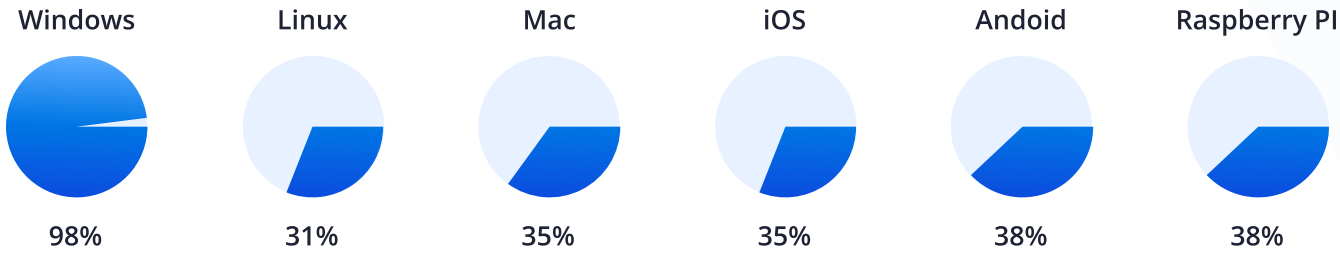
Consolidate Remote Access Solutions

It's tough enough to secure a single solution. But imagine wanting to establish a "Remote Access Security Policy" where every solution needs to have a minimum set of security controls in place. It's highly unlikely that all three solutions will have the same security features and functionality. And then there's the implementing and ongoing administration – both done three times. Do the organization a favor – if you're serious about the cybersecurity stance of your Remote Access solutions, find the one that is the most secure and use it enterprise-wide. This will allow for consistent policy, improved visibility, and better control.

SUPPORT & MANAGEMENT OF IT SYSTEMS

IT needs a Remote Access solution that will make them productive, one that can quickly provide a reliable connection to a remote system and give them the tools required to accomplish the job at hand. And yet, when we consider that average of three solutions in use, it's a clear indicator that any one Remote Access solution isn't meeting the need.

One of the likely reasons why so many solutions are used is the disparate mix of operating systems IT needs to connect to get the job done. According to the survey data, the top use of Remote Access was to *remotely access servers and network devices*, with the second most frequent use being to access the desktops of employee devices remotely. From our *State of Remote Access Security report*, we find that Manufacturing is, indeed, needing to access a wide range of operating systems remotely:



One of the weaknesses of the primary remote access solution used by Manufacturing organizations today that was raised repeatedly was the lack of breadth of platform and device support, signaling a continual need to expand the operating systems and devices supported by Remote Access solutions.

IMPROVING IT SYSTEM SUPPORT AND MANAGEMENT WITH REMOTE ACCESS

To enable Remote Access solutions to improve IT productivity in the context of support and management, consider the following recommendations:

START WITH IT NEEDS AND WORK BACKWARDS TO A SOLUTION

So often, IT starts with a *really cool* technology and then tries to simply "make it work" with all its inefficiencies and feature flaws. Given you have some very specific IT systems to support, it's critical to start with the technical needs (e.g., which platforms you are using today and are considering for tomorrow) and work to find a solution that meets the need.

REALIZE THERE WILL BE OS LIMITATIONS

Not every operating system can allow Remote Access solutions to have every capability, such as remote control, file transfer, session recording, and more. These aren't necessarily a problem with the Remote Access solution, rather than a limitation of the host OS.

CONSOLIDATE REMOTE ACCESS SOLUTIONS

IT will always figure out how to work with multiple solutions... if necessary. But the reality is – in a perfect world – every IT pro would much instead use a single console with complete visibility into all the devices they can remotely access. This eliminates any need to learn "yet another" solution, worry about proper access to ensure a productive support session, and put a consistent set of tools (barring those limited by the host OS) in the hands of IT.

INTEGRATING OT & IOT DEVICE MANAGEMENT

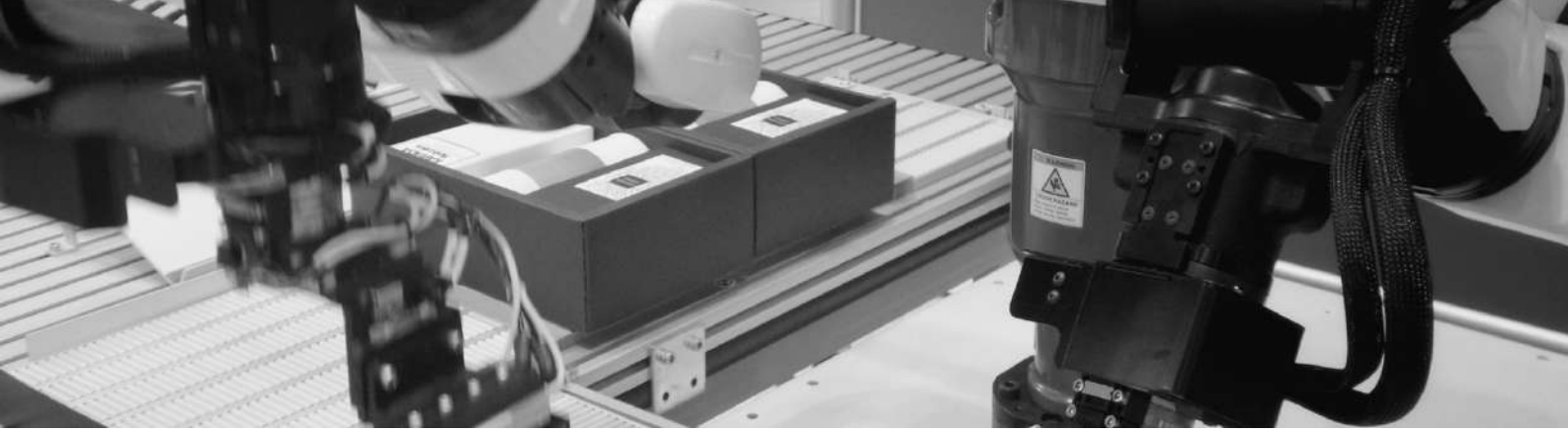
If IT had its way, IT and OT systems management would follow much the same steps using the same tools. The two environments may need to be separated into logically different networks for security or performance purposes. Still, the IT pro responsible for assisting with an OT problem would love to simply manage it in the same way they do an IT system.

But today, according to the survey data, it's not the case.

The second most critical need in 2024 for remote access solutions within Manufacturing is *supporting a new/ increased number of manufacturing equipment and devices*. **And it's reasonable to pull in Remote Access challenges from the survey, like managing remote manufacturing operations and integrating emerging technologies under the umbrella of this integration challenge, making it even more critical to address.**

OT and IoT devices will continue to be built (for the foreseeable future) in a vacuum (that is, without consideration for how the Manufacturing organization is supposed to manage it… and every other device built with the same lack of consideration). The good news is that operating systems like Windows and Linux are widely used in Manufacturing, making robust Remote Access a given. Despite many vendors vying for OS/platform dominance in the IoT world, single-board computers like Raspberry Pi are utilized for a broad range of sensors and management.

As long as vendors supporting the needs of Manufacturing continue down this path, it draws the world of Manufacturing closer and closer toward an environment where such devices' management becomes almost homogeneous.



IMPROVING OT & IOT DEVICE MANAGEMENT WITH REMOTE ACCESS

While this last challenge is going to be the most difficult to improve through Remote Access, there still are a few recommendations:

1. **Include Remote Access Manageability When Considering Devices** – This isn't solved through a specific Remote Access solution or feature. Instead, it's about putting Remote Access on the same level of importance as the OT or IoT device's functionality. When trying to find an IoT device that will monitor the pressure in a hydraulic system, the considerations should go beyond *"Can it monitor the system we have?"* and include questions like *"Can we easily access and manage it?"* Sure, it's easy to say since IT isn't always a part of the conversation, but elevating the discussion to your CISO or CTO to, in turn, bring the issue to the board may be all that's needed to make sure IT is included in the selection process to make certain the device can be supported.
2. **Ensure Remote Access Sees OT/IoT Like it Does Infrastructure** - It's one thing to see, say, all the Windows desktops in the organization from a Remote Access solution, but it's equally essential to be able to have visibility into all the devices under management in some organized fashion. With the possibility of thousands of sensors, IT is still expected to be able to support a device in short order – meaning the Remote Access solution doesn't just provide an ability to connect to the device remotely but to find it quickly, determine its current state, and potentially send it commands all without needing to establish a remote session.

REMOTE ACCESS: ONE OF THE KEYS TO IMPROVING MANUFACTURING OPERATIONS

IT departments within Manufacturing organizations likely experience more challenges than an equivalently sized organization in another industry without any form of OT. Because of this, IT – in addition to handling all things IT, like every other organization – needs an edge to improve the security of their organization, make supporting and managing IT easier, and make the support and management of OT function and feel a lot like it does when working on IT.

There are very few solution types that cross over between IT and OT. Remote Access is one of them. Therefore, it makes sense for Manufacturing organizations to look for ways to ensure the security of remote sessions better. All this while finding ways to leverage Remote Access solutions they implement to meet the needs of both IT and OT environments.

By using the data found in this white paper as a potential context for your organization and following the recommendations herein, you create an opportunity to make IT's life more accessible, the organization's operations more productive, and the organization itself more secure.

INVESTING IN THE FUTURE

This survey demonstrates that manufacturers face significant challenges in 2024 and beyond. Survey participants reported that the top challenges they expect this year include managing OT and ICS devices, continuing to support digital transformation, and ensuring network security. Selecting a remote access vendor that can address these challenges will be critical to their IT strategy.

RealVNC has a demonstrated history of supporting manufacturers with their IT needs, including:

- **Ensuring data privacy and security:** RealVNC can help improve security with the only remote access solution with a “white box audit” certification. RealVNC has the strongest focus on security with AES encryption and proven SSH tunneling.

- **Reducing costs:** RealVNC is one of the most cost-effective remote access solutions on the market, with transparent pricing, no hidden fees, and a total cost of ownership that is one of the lowest in the industry. With RealVNC, there are no in-session restrictions. You can connect as many times as you want for as long as you like from any device.

- **Support for digital transformation:** According to the survey results, supporting digital transformation is a top challenge for IT staff in Manufacturing. RealVNC can help support digital transformation by supporting IT staff needing to connect with remote staff and devices securely, quickly, and efficiently in real-time.

- **Support for Operational Technology (OT):** It is no secret that OT is a manufacturing trend. RealVNC can help IT and OT staff access, manage, and monitor OT devices, whether it is a sensor on a consumer packaging machine in a plant in Atlanta, Georgia, or a remote sensor measuring pharmaceutical material quality from a plant in Greensville, North Carolina.

www.realvnc.com

RealVNC®'s remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC® is the original VNC remote access software developer and supports an unrivaled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology directly into their products through OEM agreements.