NETOP

Securing Remote Access: A Netop Perspective

Introduction

For years, the vulnerabilities inherent in remote access technologies have been a prime target for cyberattacks, allowing malicious actors to penetrate organizations inflicting significant damage. While remote work remains a preference, there is a new trend towards hybrid models with a mix of remote and in-office work. Thus, enhanced cybersecurity measures remain a critical requirement moving forward for IT organizations.

As of May 2025, the latest attacks from artificial intelligence (AI) and machine learning (ML) identify and exploit vulnerabilities across networks and memory with a 30% increase year-over-year increase in cyberattacks per organization per week. Cybercrime estimates for 2025 are $10.5 trillion up from $9.5 trillion in 2024.

These escalating threats have understandably created a climate of concern among CISOs, security experts, and IT professionals regarding the security of their remote access infrastructure.

Remote Access for Modern Enterprise

Remote access is fundamental for today's enterprises, enabling them to harness the power of network connectivity to access devices, networks, and platforms across geographical boundaries, thereby boosting productivity and operational efficiency. Despite the inherent security challenges, completely restricting remote access is simply not a viable option for most organizations, as it remains an essential operational tool.

Consider global companies that require the ability to remotely manage their diverse device inventories, irrespective of physical location. Internal IT teams rely on remote access for critical tasks like patching and repairing devices, especially during global software updates. Similarly, Original Equipment Manufacturers (OEMs) often need remote access to customer devices for essential services such as repairs, troubleshooting, file transfers, and log collection.

The proliferation of the Internet of Things (IoT) has connected traditional industrial equipment in factories, mining operations, power plants, and other critical infrastructure, enabling remote monitoring and management. Remote access to these devices allows organizations to leverage valuable IoT sensor data for enhanced efficiency and to maintain uptime, regardless of the physical location of their IT personnel.

However, this essential connectivity comes with increased security and compliance responsibilities. The devices accessed often handle sensitive data pertaining to customers, patients, and employees. A data breach can lead to significant compliance violations and reputational damage. Furthermore, operational devices in industrial and healthcare settings frequently run on outdated operating systems like older versions of Windows or Linux, making them attractive targets for hackers seeking a foothold within an organization's network.

Companies in highly regulated industries must exercise extreme caution regarding devices connected to their networks, including ATMs, point-of-sale (POS) systems in retail environments, kiosks, HVAC systems, Industrial IoT robots on factory floors, and critical healthcare devices such as imaging machines, MRI scanners, and X-ray systems. In sectors like healthcare, professionals must transmit sensitive patient data via secure encrypted channels and remotely monitor specialized medical devices while adhering strictly to regulations like HIPAA, PHI, and ISO standards.

Addressing Security Limitations of Remote Access solutions

The permanence of remote employees and the expansion of cloud infrastructure have made managing the security perimeter more challenging than ever before. IT security teams must be able to rapidly detect unauthorized access and limit lateral movement within the network to safeguard sensitive data. For example, Yale New Haven Health System disclosed in April 2025 that over 5.5 million individuals' sensitive health information and social security data were compromised through unauthorized remote access.

Historically, organizations have relied on Virtual Private Networks (VPNs) to secure remote access. However, VPN connections alone offer limited protection.

A significant vulnerability is that once an attacker gains access to a VPN, they can often navigate the network with ease, bypassing many legacy firewall rules that grant broad access. The complexity of managing VPNs at scale can also introduce additional security weaknesses.

Another widely adopted remote access solution is RDP. While integrated into the Windows operating system, RDP can also be installed on macOS, Linux, and Android. However, without robust security measures, RDP can become a gateway for malware deployment and targeted ransomware attacks. Security firm Kaspersky reported a staggering 377.5 million brute-force attacks targeting RDP by February 2021, a dramatic increase from the 91.3 million observed just a year prior which continues as RDP remains a primary attack vector.

Freeware RDP and VNC solutions introduce significant vulnerabilities. A recent research report highlighted that targeting Microsoft RDP servers, commonly used by IT and field engineers, was identified as potentially the most damaging attack scenario among eleven analyzed. Even the use of secure 5G cellular connections does not automatically protect RDP traffic, leaving connections vulnerable to attackers who can exploit them to deploy malware and ransomware or to sabotage industrial control systems (ICS).

Other internet-based remote access solutions, such as TeamViewer and LogMeIn, raise both security and compliance concerns. For instance, TeamViewer's default setting allows full control over the remote host with a simple password. These solutions often lack the inherent security and flexibility offered by fully self-contained, point-to-point tunneling tools like Netop, which is designed to seamlessly integrate with zero-trust and privileged access management frameworks.

Banks and financial institutions rely on secure remote access to monitor ATM activities, supervise remote settlements, and perform updates and maintenance, significantly reducing travel costs and the need for costly on-site repairs. This necessitates a remote access solution that adheres to Payment Card Industry (PCI) compliance standards. While compliance is essential, it does not equate to comprehensive security. True enterprise security demands a robust remote access solution with stringent controls.

Unmatched Security Benefits of Netop

It's a well-known challenge that IT teams often lack the necessary skilled personnel to effectively combat the evolving threat landscape. When staffing up isn't feasible, the solution lies in deploying superior technology that provides robust remote access security without sacrificing simplicity.

A secure remote access tool like Netop serves as an excellent complement to VPNs, providing enhanced protection and compliance for devices with heightened security requirements. Unlike VPNs, which have open ports that can be scanned for vulnerabilities, Netop utilizes outbound-only connections, rendering ports invisible to external threats.

Netop operates seamlessly through firewalls without requiring VPN tunneling, helping to maintain the integrity of security perimeters. While some companies attempt this through modified RDP or VNC connections, this approach introduces significant risks. OEMs must carefully consider the security implications of including less secure modified RDP and VNC in their devices, as this directly exposes their customers to potential threats. Any specialized device deployed in sensitive environments like hospitals, banks, retail locations, or factory floors should be shielded from RDP and VNC-based attacks.

Customers must exercise equal vigilance in ensuring that their OEMs do not incorporate insecure remote connectivity via RDP, VNC, or remote access providers that expose connections to the internet, as these can leave the organization vulnerable to severe threats. Instead, OEMs should implement a self-contained secure remote access function like Netop. It offers full encryption, adheres to relevant regulations, and incorporates role-based access features to ensure comprehensive device protection.

Netop's self-contained remote access solution empowers OEMs and technology partners such as Diebold Nixdorf, NCR, Radiometer, Gilbarco Veeder-Root, Toshiba Global Commerce Solutions, and Nautilus Hyosung to service ATM and POS devices for their customers without exposing them to third-party risks.

Netop's robust security controls include time-of-day access windows, IP address filtering, Confirm Access via Email (CAvE), and application whitelisting. These features provide customers with a firm and granular set of controls, mitigating the risk of exposing specialized devices to the internet while maintaining essential remote access capabilities.

Conclusion: Architecting a Secure Remote Future with Netop

As organizations increasingly deploy virtual desktops, they add another critical use case to their growing remote access needs. With Netop, users can securely connect to virtual desktops, eliminating the reliance on less secure alternatives like RDP.

In this era of remote operations, integrating secure remote access is no longer optional – it's a necessity. A remote access solution like Netop prioritizes the security of your enterprise while simultaneously enhancing efficiency and productivity. Netop stands as a simple, flexible, and highly scalable solution, delivering the comprehensive benefits of a self-contained remote access platform that meets the diverse needs of today's distributed world.

Vistit www.netop.com to learn more.