Netop

ATIVION

Build with Secure Remote Access from the Start

Introduction

For years, cyberattacks have exploited remote access vulnerabilities to inflict deeper damages in organizations. But recently, the increasing shift to distributed offices escalated those risks. A more remote workforce, along with complex third-party supplier ecosystems, made remote access a rampant threat vector.

Microsoft's Remote Desktop Protocol (RDP), already a common target for man-in-the-middle attacks, contributed to 90% of attacks handled by Sophos Incident Response in 2023. Moreover, the JetBrains attack in October 2023, conducted by the SolarWinds hackers, exposed around 10% of the company's customers using its servers. These cases show how attackers can compromise a software provider who doesn't use a remote control solutian that lacks in security features.

These evolving threats justify the jittery outlook among CISOs, security experts, and IT professionals with remote access usage.

Remote Access is Essential for Enterprises

Simply put, remote access helps enterprises leverage the power of widespread network connectivity to access devices, networks, or platforms located in different locations to improve productivity and efficiency. Despite security risks, for most enterprises, locking down remote access is not viable as it continues to be an essential tool.

For example, global companies need to remotely manage device inventory, regardless of the devices' physical locations. Internal IT teams use remote access to patch or fix devices, especially if something breaks during a global software update. OEM vendors need to remotely access customer devices for repairs, troubleshooting activities like transferring files or collecting logs.

The Internet of Things (IoT) allows factory equipment, mining rigs, energy plants, and other facilities to be connected to networks for seamless remote monitoring and management. With remote access to these devices, you can utilize IoT sensor data to enhance operational efficiencies and optimize performance.

Remote access also allows you to maintain uptime regardless of where your IT team physically resides. On the hind side, remote access increases security and compliance risks.

It is essential to protect devices from these heightened risks. These devices often process sensitive data from customers, patients, employees and more. If there's a data breach, there's a compliance risk to those individuals and the organization. These operational devices in factory floors or hospitals sometimes run on outdated Windows or Linux systems. Hackers usually target those systems as a way to get a foothold in an organization's network.

Companies in highly regulated industries have to be cautious about devices on their networks. That includes ATMs, POS devices in retail, kiosks, HVAC systems, IIoT factory floor robots, and healthcare devices (imaging machines, MRI, X-ray).

In highly regulated industries like healthcare, medical professionals have to send patient data through secure, encrypted channels or remotely monitor specialized medical devices. This must be done while complying with HIPAA, PHI & ISO.

Banks and financial institutions remotely monitor ATM activities, supervise remote settlements, update and perform maintenance to reduce the cost of travel, truck rolls and costly in-person fixes. This has to be done using a remote access solution that's PCI compliant.

While being compliant is crucial, it is not the same as being secure. To secure the enterprise, you need a secure remote access solution with serious controls.

Overcoming Security Limitations of Remote Access solutions

With remote employees and cloud sprawl to consider, it has never been harder to manage the security perimeter. IT security teams must detect unauthorized access quickly and limit horizontal movement in the network to protect sensitive data. In 2023, Managed Care of North America, a dental insurer, suffered a breach that affected over 8 million people. Hackers accessed and copied sensitive info, including full names, Social Security numbers, and insurance details.

Companies have traditionally relied on Virtual Private Networks (VPN) to secure remote access. But a VPN connection only goes so far. One big challenge is that once attackers get access to a VPN, they can easily penetrate the network like a hot knife through butter. Many legacy firewall rules allow access to practically everything in the network. Management complexities with VPNs at scale expose additional security holes.

A widespread remote access solution among enterprises is RDP. Although it's built into Windows operating system, RDP can also be installed on Apple, Linux, and Android operating systems. Unless adequately secured, RDP can be the gateway to deploy malware and targeted ransomware. ESET reported detecting 55 billion new brute-force attacks in just the second quarter of 2023, a significant increase from previous years. This equates to an average of 37,000 daily attacks on exposed RDP connections.

RDP and VNC freeware open up too many vulnerabilities. Out of eleven attack scenarios from a recent security research report, a potentially most damaging instance involved targeting Microsoft RDP servers that IT and field engineers commonly use.

Even secure cellular connections using 5G don't automatically protect RDP traffic. RDP connections would still remain exposed to attackers who can exploit those to download malware and ransomware, or to sabotage industrial control systems (ICS).

Other remote access solutions like TeamViewer and LogMeIn provide connectivity via Internet, creating security and compliance concerns.

Besides, TeamViewer by default allows full control over the remote host guarded by a simple password.

These solutions cannot offer the security and flexibility of fully self-contained, point-to-point tunneling tool like the Impero remote access solution, which is flexible enough to fit in zero trust and privileged access management frameworks.

Benefits of Remote Access Software with Unparalleled Security

It's no secret that IT teams don't have enough skilled employees to keep up with the threats they face. If you can't staff up, use better tech that offers robust remote access security without compromising simplicity.

A secure remote access tool like Impero is a good complement to a VPN, helping keep devices with higher security needs protected and compliant. While a VPN has open ports that can be scanned for weaknesses, the Netop remote access solution uses outbound-only connections that keep ports invisible.

Netop works through firewalls without VPN tunneling, which helps keep security perimeters intact. Many companies allow this to happen via a modified RDP or VNC connection, but that is risky.

OEMs need to think twice before including less-secure modified RDP and VNC in their devices, as this puts the customers at risk. Any specialized device that ends up in a hospital, bank, retail area, or factory floor should be protected from RDP or VNC-based attacks.

Customers need to be equally vigilant in ensuring their OEMs do not include insecure remote connectiveness via RDP, VNC, or remote access providers that expose connections to the internet, as these can expose the organization to severe threats.

Instead, OEMs should implement a self-contained secure remote access function like Netop remote access. It's fully encrypted and compliant with relevant regulations, and has role-based access features that can keep devices fully protected.

Netop's self-contained remote-access solution enables OEMs and other Impero technology partners like **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.

Conclusion:
Designing a Secure Remote Future

Netop's security controls include time-of-day access windows, IP address filtering, confirm access via email (CAvE), and application whitelisting, all of which allow customers to maintain a firm, tight set of controls and avoid the risk of exposing these specialized devices to the internet, but maintain the necessary flexibility to ensure efficient and secure remote maintenance and support.

As more virtual desktops are deployed, organizations add yet another use-case to the wide variety of remote access needs. Users can securely connect to virtual desktops with Netop rather than relying on less secure options like RDP.

In the remote era, integrating secure remote access is no longer optional. A remote access solution like Netop makes it a priority to secure your enterprise while enhancing efficiency and productivity.

Netop is a simple, flexible, and highly scalable solution that offers the benefits of a self-contained remote access solution that does it all.

Ativion is more than a name; it's a declaration of our cutting-edge vision and our priority to lead the market globally. We are dedicated to providing innovative solutions that meet the evolving needs of our customers, ensuring they have the tools they need to succeed in an increasingly digital world.

Unmatched security and scalability makes Netop the trusted solution of the world's leading enterprises, including over half of the Fortune 100.