# THE OT REMOTE ACCESS CHALLENGE

Avoid Downtime by Protecting Your Operational Technology (OT) Systems From Cyber Attacks

BeyondTrust

## The OT Landscape Has Shifted

For many years, industrial systems relied upon proprietary protocols and software. These legacy solutions lacked automation, required manual administration by people, and had no external connectivity.

Today, the operational technology (OT) landscape is very different. More and more industrial systems are being brought online to not only adopt new capabilities and efficiencies through technological integrations, but also to deliver big data and smart analytics. These modernized systems require off site vendors, employees operators, suppliers and contractors to remotely access these systems.

This transition from closed to open systems has generated a slew of new security risks. Cyberattacks of critical infrastructure are at an all-time high, increasing 2,000% in 2019. Yet only 23% of manufacturers are compliant with minimal mandatory industry or government guidance and regulations around cybersecurity of industrial control systems. Enabling secure remote access to your OT systems is critical to maintaining the productivity and business continuity of your organization.

**Enabling secure remote access to your OT systems is critical to maintaining the productivity and business continuity of your organization.**

## Security Gaps: VPN & Legacy Remote Access Technology

These trends have accelerated with the massive shift to remote working. Workers and 3rd party vendors are using personal laptops other devices (also known as BYOD, or "Bring Your Own Devices") to connect remotely to OT systems from their home networks, that have fewer security controls compared to the corporate environment. **These remote connections have blurred the IT-OT segmentation and expanded the attack surface by providing new entry points for hackers to exploit.**

As industrial systems become more connected, they also become more exposed to vulnerabilities. VPNs are adequate for providing basic remote employee access to non-sensitive systems but lack the advanced security features, visibility, scalability, and cost-effectiveness needed for today's remote access to OT/IoT devices.

Hackers are taking advantage of the increased dependence on VPNs by finding many new vulnerabilities in these systems. VPNs have become highly attractive targets for malicious actors.

If you oversee the OT/IoT infrastructure of your organization, you have the fundamental responsibility of protecting your company, infrastructure, and the security and privacy of your clients.
Key considerations include:

- Maintaining compliance and business continuity while protecting critical system
- Keeping your OT environment and IoT devices secure without inhibiting business agility or compromising safety

Does your team have the appropriate remote access solution in place to handle a large volume of operators, contractors and vendors connecting remotely into your network?

# The Remote Access Challenge

Use these questions as a guide to identifying the right remote access solution for their OT environment.

## 1 Do you know who is accessing your OT network, and what they are doing, and for how long?

"Always-on" VPNs provide no visibility or control over individual user activity, especially on a shared device.

Restricting unapproved protocols and directing approved sessions to a predefined route reduces the attack surface.

## 2 Are you able to capture detailed session data for all remote access sessions, for review in real time or later on?

The inability to review or track activity of remote users is problematic to security and compliance.

Capturing detailed session logs creates an audit trail that enables accountability and compliance.

## 3 Do you follow the principle of least privilege for your OT network?

"All or nothing" VPNs enable greater levels of access than operators, suppliers or vendors need for their job functions.

Role-specific access and individual accountability for shared accounts enables a comprehensive approach to remote access security.

## 4 Do you protect credentials used by remote operators and vendors, and limit knowledge of privileged passwords?

Credentials are often stored insecurely.

Securing privileged accounts in a password vault protects them while automatically injecting them into user sessions.

## 5 Do you enable the Purdue Model by only interacting one layer up or down in the industrial network?

"Air-gapping" isolates plant and enterprise networks through separation of layers and defining how machines and processes should interact.

Using appliances that can be paired together ensures logical and physical network separation to comply with the Purdue model.

YES

NO

## 6 Do you have a single path for scheduling and approving timebound remote access to your OT network?

Inefficient workflows slow down OT and IT teams, frustrate end users, and create security gaps.

Consolidating the scheduling, tracking, approval, and auditing of remote access reduces the administrative burden and speeds the process.

## 7 Are your IT and OT Networks segragated?

The use of personal devices by remote workers has blurred the IT-OT segmentation, expanding the attack surface.

Deploying an appliance-based remote access solution allows for OT and IT networks to work separately, keeping data segregated.

## 8 Do you use Multi-Factor Authentication (MFA) for remote access?

Not enforcing MFA makes it easier to compromise privileged credentials, one of the most common types of breaches.

Utilizing native MFA or Time-based One Time Password (TOTP) capabilities protects against a common attack vector.

## 9 Do you have a structured process for provisioning and deprovisioning remote access?

Provisioning access can be a complex process flow consisting of many different directories and systems.

Applying policies and controls to users that access dispersed sets of endpoints – even spanning geographic regions – results in a more efficient & accurate process.

## 10 Is all data in transit encrypted when using remote access?

Older devices or operating systems may not support newer encryption standards, making them susceptible to "Man In the Middle" attacks.

Using the latest encryption standard, such as TLSv1.2, even when accessing older devices, enables a higher standard of security for remote access.

If you answered "no" to any question, **YOUR ORGANIZATION IS AT RISK.**

## Secure Remote Access to OT Systems With BeyondTrust

BeyondTrust Privileged Remote Access enables organizations to secure industrial networks without disrupting operations, compromising safety or risking non-compliance. Our solution provides secure remote access in a single, flexible solution that simplifies deployments and ensures maximum scalability—while empowering remote operators and vendors to be productive.

Key capabilities include:

- Complete visibility and control over OT remote access
- Least privilege enforcement with granular access controls
- Network segregation
- Reduced administrative burden and simplified workflows
- Creation of comprehensive audit trails

Using Beyond Trust Privileged Remote Access as a replacement to your corporate VPN for operators, suppliers or third-party vendors to access OT environments eliminates remote access blind spots, reduces the attack surface, and drives productivity. Protect your processes and profits while significantly reducing security vulnerabilities and incidents.

### VPN vs. BeyondTrust Privileged Remote Access

| CAPABILITY | VPN | BeyondTrust |
|---|---|---|
| Remote Access | ✓ | ✓ |
| Secure Connectivity | ✓ | ✓ |
| Network Layer Access (Protocol Tunneling) | ✓ | ✓ |
| Encrypted Traffic | ✓ | ✓ |
| Application Layer Virtualization | | ✓ |
| Non-RDP Desktop | | ✓ |
| Proxied RDP Access | | ✓ |
| Proxied VNC Access | | ✓ |
| Proxied SSH Access | | ✓ |
| Application Session Monitoring | | ✓ |
| Application Session Recording | | ✓ |
| Just-in-Time Access | | ✓ |
| Zero Trust Architecture | | ✓ |
| Privileged Access Management (PAM) Integration | | ✓ |
| ITSM Integration | | ✓ |
| Password Management & Credential Storage | | ✓ |
| Cloud or On-Premises Deployment (Physical or Virtual Appliance) | | ✓ |
| Agentless Access | | ✓ |
| Extensive Operating System & Platform Support | | ✓ |
| Prevention of Lateral Movement | | ✓ |
| Audit Trail & Session Reporting | | ✓ |

## Zero Trust & OT Systems

NIST defines Zero Trust as "an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.[1]" Zero Trust is increasingly relevant for industrial control systems, as technologies and have blurred or dissolved the idea of a traditional firewall and network-zoned perimeter. The seismic shift to remote working has also accelerated the demise of the traditional perimeter and is driving an increased focus on Zero Trust.

NIST's guidelines provide a clear playbook for organizations seeking guidance on how to adopt Zero Trust principles. Many organizations have begun to embrace Zero Trust frameworks and are building these into their security strategies.

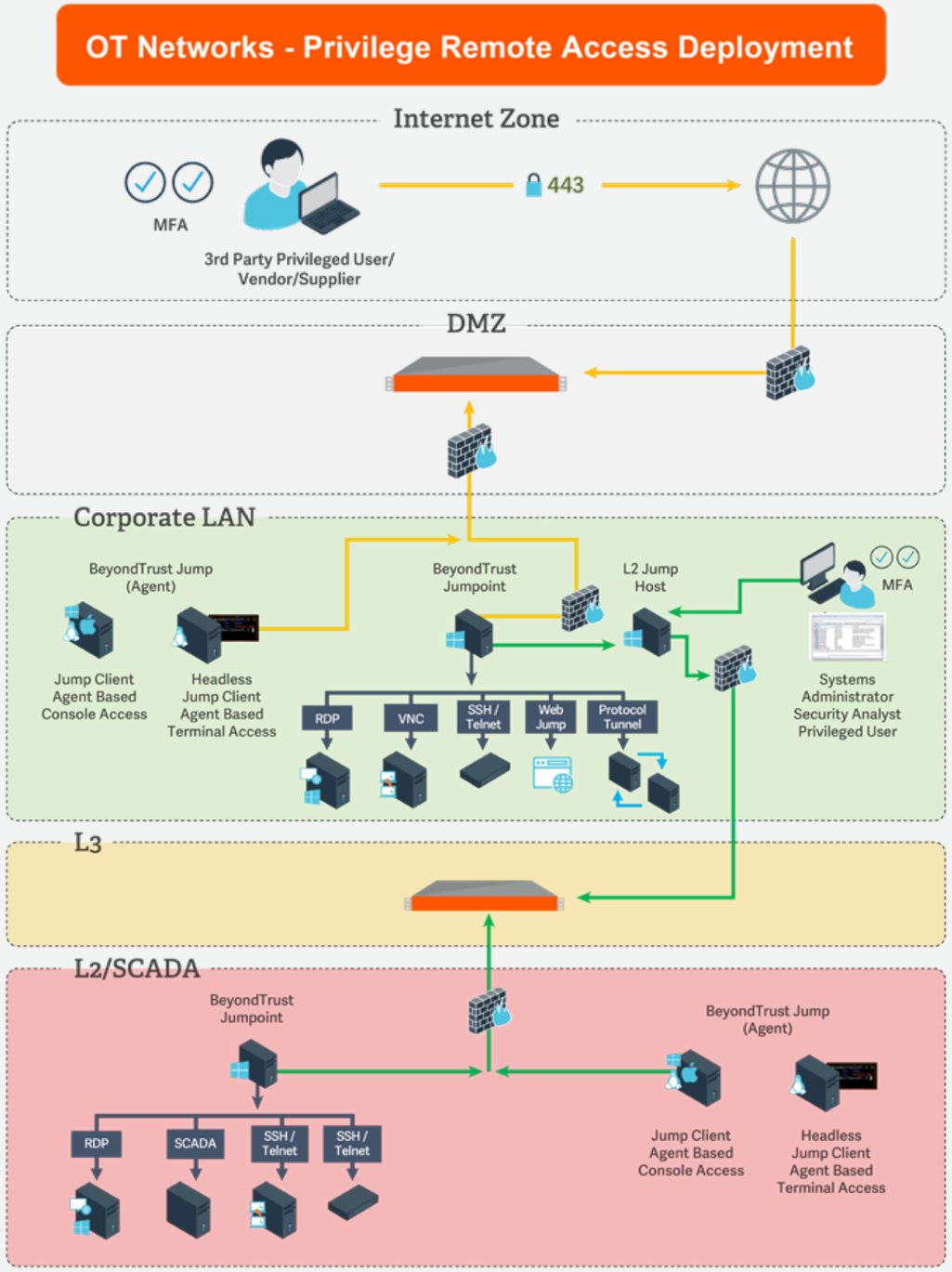
BeyondTrust Privileged Remote Access helps organizations adopt a Zero Trust approach by:

- Enforcing the philosophy of least privilege for remote access sessions
- Treating managed devices with the same level of trust as an unmanaged device – which is zero
- Providing application access independent of network access
- Recording all activities performed using remote access and disabling functionality such as copy/paste
- Enabling API security to protect the integrity of data being sent from IoT devices to back-end systems

Applying the granularity of Privileged Remote Access to achieve Zero Trust objectives ensures all access is appropriate, managed, and documented, regardless of how the perimeter has been redefined.

For more information, download the white paper "A Zero Trust Approach To Secure Remote Access."

[1] NIST Special Publication 800-207, Zero Trust Architecture




*Based on the Purdue Model

BeyondTrust

## Learn More or Schedule a Demo

https://www.beyondtrust.com/solutions/operational-technology

## About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. We are trusted by 20,000 customers, including 75 percent of the Fortune 100, and a global partner network.

Learn more at beyondtrust.com

V2021_03_ENG