BeyondTrust

Operational Technology (OT) Cybersecurity Assessment

Identify and Address Remote Access Security & Compliance Risks to your OT Systems.

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. In the past year, 89% of electricity, oil and gas, and manufacturing firms have experienced cyberattacks impacting production and energy supply. In addition, 72% say they experienced cyber disruption to their ICS/OT environments at least six times during the year.[1]

To better address the risks ushered in by cloud adoption, digital transformation, remote working, and the increasing interconnectedness of everything, enterprises and government agencies are embracing zero trust principles. Yet, almost 80% of critical infrastructure organizations haven't adopted zero trust strategies.[2]

Enabling secure remote access and upholding zero trust principles to your OT systems is critical to maintaining the productivity and business continuity of your organization.

> *"Managing connected worker cyber risks is an urgent issue and demands enhancements to existing IT and OT industrial cybersecurity programs. Conventional VPN and RPC approaches don't provide the security that is needed and are too difficult to manage. Connected workers require zero trust across all industrial systems and resources.*
>
> *Industrial Connected Workers Require Zero Trust. ARC View. 11/2021*

Remote Access Security

Today, workers and third-party vendors are increasingly using personal laptops and other devices (also known as BYOD, or "Bring Your Own Devices") to connect remotely to OT systems from their home networks, which have fewer security controls compared to the corporate environment. **These remote connections have blurred 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 systems
- 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 identify the right remote access solution for your OT environment.

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

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

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

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

No — The inability to review or track activity of remote users is problematic to security and compliance.

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

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

No — "All or nothing" VPNs enable greater levels of access than operators, suppliers, or vendors need for their job functions.

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

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

No — Poor password management practices are rampant in OT and have been exploited in many high-profile OT breaches.

Yes — Securing privileged accounts in a password vault not only protects them, but also enables a smoother user experience by automatically injecting them into the session.

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

No — "Air-gapping" isolates plant and enterprise networks through separation of layers and defining how machines and processes should interact.

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

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

No — Inefficient workflows slow down OT and IT terms, frustrate end users, and create security gaps.

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

Are your IT and OT networks segregated?

No — The use of personal devices by remote workers has blurred the IT-OT segmentation, expanding the attack surface.

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

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

No — Lack of MFA makes it much easier to hijack an account, gain privileged access, and conduct lateral movement.

Yes — Utilizing native MFA or time-based one-time-password (TOTP) capabilities protects against a common attack vector.

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

No — Provisioning access can be a complex process flow consisting of many different directories and systems.

Yes — Applying polices and controls to users that access dispersed sets of endpoints - even spanning geographic regions - results in a more efficient and accurate process.

Is all data in transit encrypted when using remote access?

No — Older devices or operating systems may not support newer encryption standards, making them susceptible to “man in the middle” attacks.

Yes — 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 VPN-less 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 BeyondTrust 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, and secure infrastructure access, while significantly reducing security vulnerabilities and incidents.

"BeyondTrust Secure Remote Access (SRA) offers a high security, zero trust way for authorized remote users to gain access to critical IT and OT assets."

Industrial Connected Workers Require Zero Trust. ARC View. 11/2021

Throughout the process of assessing remote support solutions, keep in mind these business requirements:

VPN vs. BeyondTrust Privileged Remote Access

CAPABILITY	VPN	BeyondTrust
Remote Access	●	●
Secure Connectivity	●	●
Network Layer Access (Protocol Tunneling)	●	●
Encrypted Traffic	●	●
Application Layer Virtualization		●
Remote 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		●
Secure BYOT		●
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.[3]" Zero trust is increasingly relevant for industrial control systems, as technologies and remote working have blurred or dissolved the idea of a traditional firewall and network-zoned perimeter.

NIST's guidelines provide a clear playbook for organizations seeking guidance on how to adopt zero trust principles. Many organizations are building these into their security strategies.

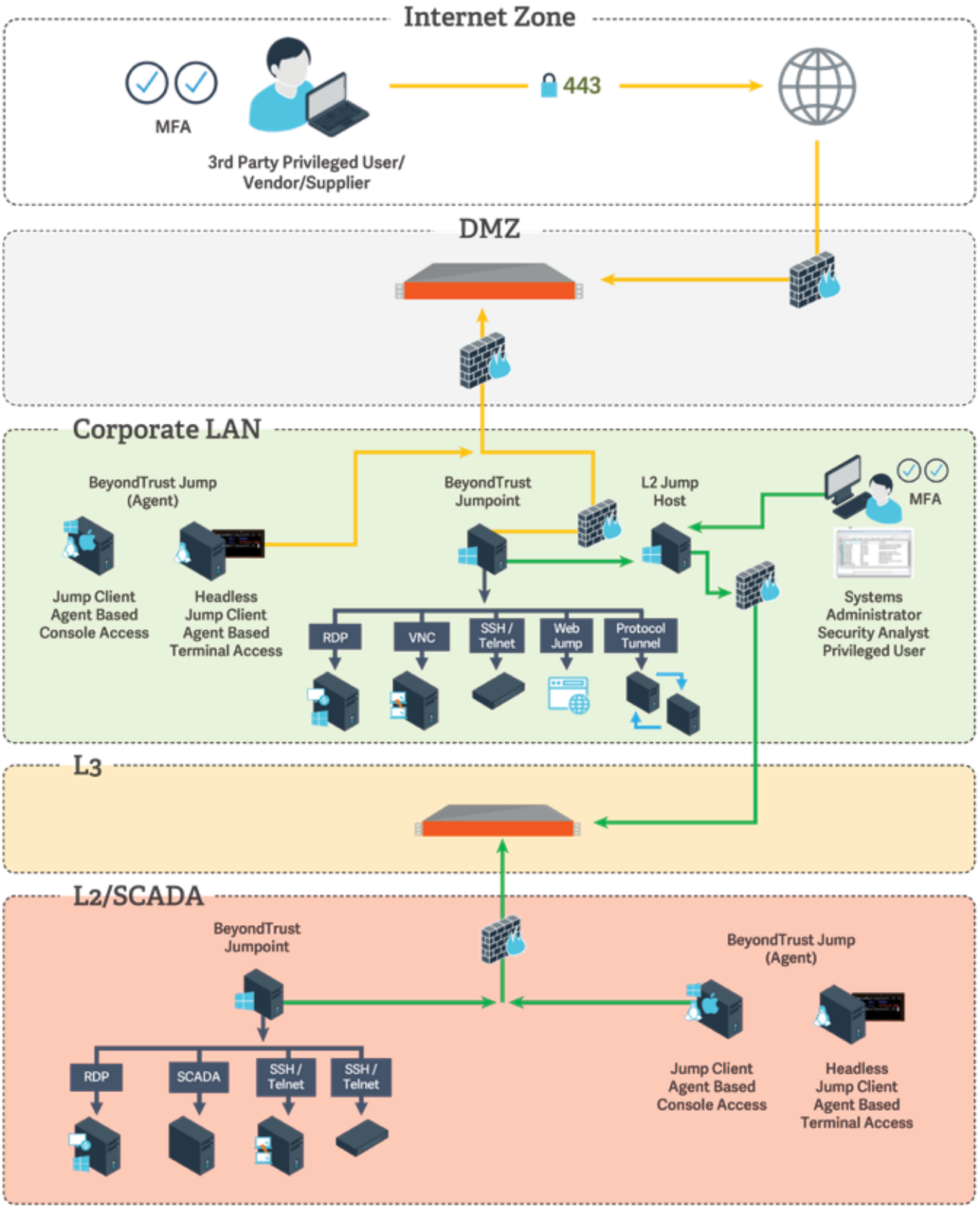
BeyondTrust Privileged Remote Access helps organizations adopt a zero trust approach by:

- Enforcing the principle 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 risky 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 remote user and infrastructure access is appropriate, managed, and documented, regardless of how the perimeter has been redefined.

[1]The State of Industrial Cybersecurity. Trend Micro. June 2022
[2]Cost of a Data Breach Report. IBM. July 2022.
[3]NIST Special Publication 800-207, Zero Trust Architecture. August 2020.

OT Networks - Privileged Remote Access Deployment



Learn More or Schedule a Demo

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

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 75 of the Fortune 100, and a global partner network.
Learn more at **beyondtrust.com**