NOVEMBER 4, 2021

Industrial Connected Workers Require Zero Trust

By Sid Snitkin

Keywords

Industrial/OT Cybersecurity, Connected Industrial Workers, Zero Trust, BeyondTrust

Summary

Connected workers are creating many benefits for industrial companies. But the associated risks demand more advanced, zero trust cybersecurity programs.

Leading industrial companies are using anywhere, anytime access to systems, apps, data, and people to drive higher productivity, better quality, and lower costs. While these benefits are large, they come with increased cyber risks. Every interaction opens a new attack pathway. Devices used outside facilities also increase opportunities for malware infection and data loss. Current industrial cybersecurity programs were not designed to manage these threats. Companies need to implement zero trust security to securely reap the full benefits of connectivity.

Connectivity has changed the way we live. Leading industrial companies are also using anywhere, anytime access to systems, apps, data, and people to drive higher productivity, better quality, and lower costs.

This ARC View reviews the cybersecurity challenges of industrial connected workers and offers recommendations on the changes companies will need to make to ensure secure rollout of these new business strategies.

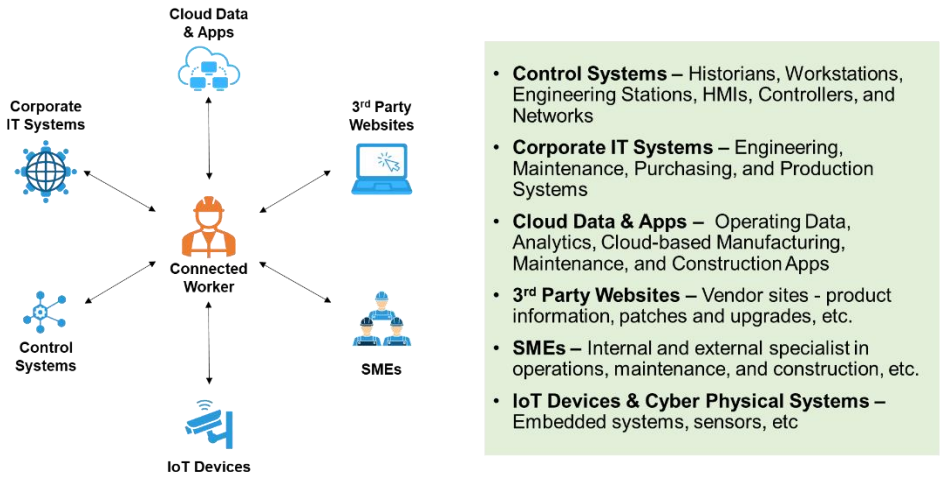
Recently, ARC Advisory Group discussed industrial connected worker security challenges with executives of BeyondTrust, a company with extensive experience in enabling secure, connected workers. A brief overview of their security offerings is included in this report.

The Industrial Connected Worker

Connected workers are driving higher performance in every industrial activity. Workers with remote access to systems and assets are reducing facility downtimes and travel costs. Site personnel with instant access to project

information are reducing construction delays and costly errors. Instant access to cloud resources and subject matter experts (SMEs) is improving the productivity of factory workers. Remote operation of equipment in distant and hazardous areas is reducing safety risks and travel costs. Connectivity is also enabling broader use of productivity-enhancing technologies, like cloud analytics, smart glasses, and augmented reality.

All these benefits rely upon anywhere, anytime access to a wide range of devices, apps and data in corporate IT and OT systems, the cloud, and embedded physical systems.



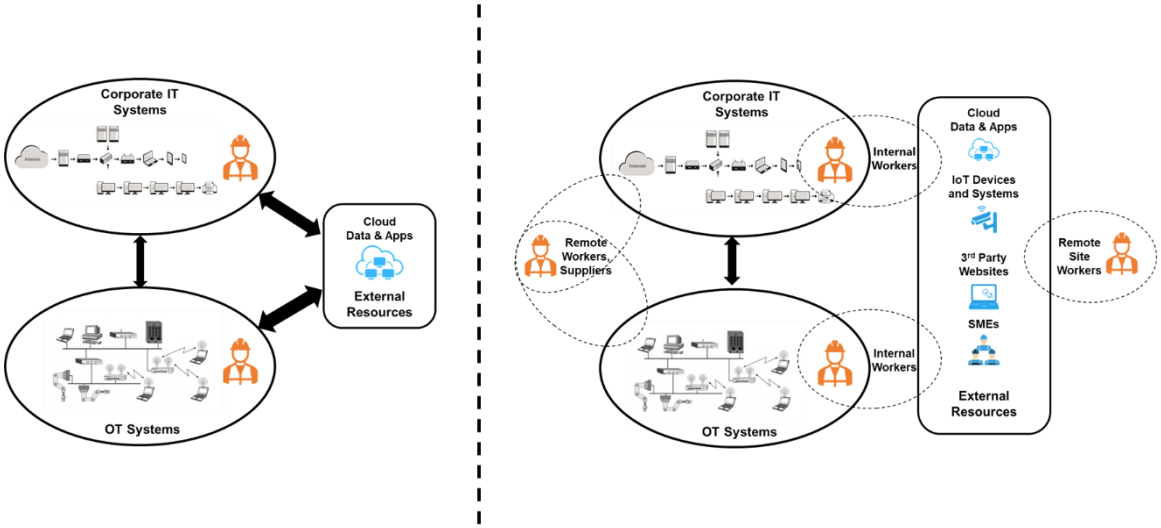
Connected Industrial Workers Need Secure Access to a Diverse Set of Resources

Connected Worker Cybersecurity Challenges

Connectivity increases opportunities for attackers to compromise critical systems and steal confidential data. Left unaddressed, these threats can impact safety, environmental compliance, and business continuity, with costs that far outweigh connected worker benefits. Concern about cyber risks also constrains adoption of performance-enhancing processes and technologies that are sorely needed in many industrial sectors. Upgrading industrial cybersecurity programs to address these issues is essential.

Conventional industrial cybersecurity programs, especially those for OT systems, place strict limitations on communications across system boundaries. Isolation is considered essential to protect legacy assets and networks that can't support modern security defenses. External connections are severely

limited and require well-defined use cases and time for implementation of strong defenses.



Connected Workers Require Expanded Industrial Cybersecurity Strategies

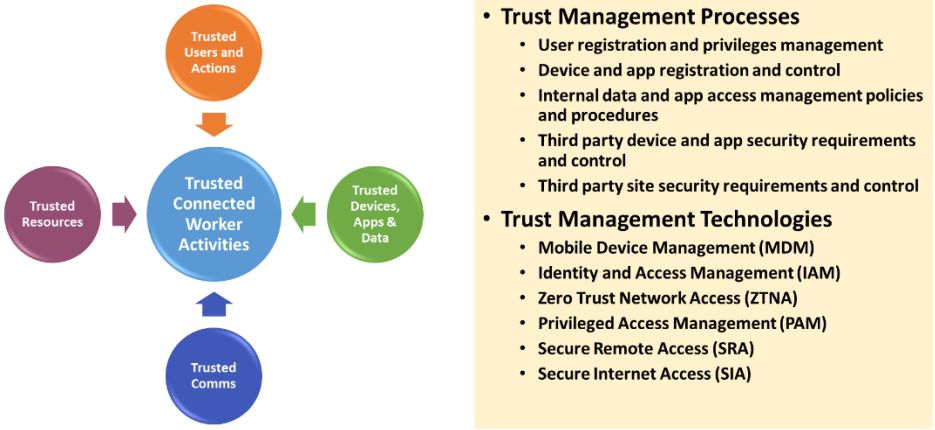
Rigid, restrictive connectivity constrains connected worker benefits. Remote workers can only help operations if they have convenient access to internal systems. Internal workers can only leverage SMEs and external information when they are readily available. Each of these situations presents a unique, time-sensitive opportunity to improve productivity, but only if security strategies support on-demand, end-to-end protection of individual interactions. To maximize benefits, companies need to provide this kind of security for three common use cases:

- Secure remote access to assets within IT and OT system perimeters.
- Secure access to corporate data, apps, and IoT devices by workers at remote sites.
- Secure access to cloud apps, data, and SMEs by internal workers.

Connected Workers Require Zero Trust Cybersecurity

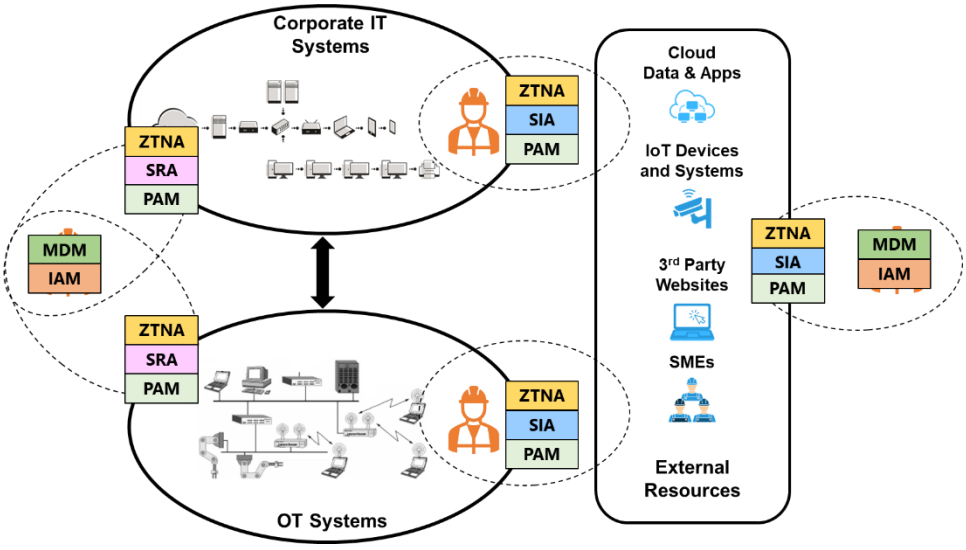
Trust is the foundation for secure interactions. Trust is traditionally implicit within system perimeters because companies have control over the internal people, devices, apps, and networks. But activities, like connected workers, that involve external resources require explicit trust management regardless of where the resource is located. This is commonly referred to as Zero Trust

and includes validating the trustworthiness of people and their actions, devices and apps, communications, and resources being accessed.



Connected Worker Interactions Require Zero Trust

Managing trust in connected worker activities requires a robust set of processes and technologies. Industrial systems already have some of these processes, for user privileges management, use of BYOD devices, and third-party access. But connected workers require more stringent management of basic security controls as well as new processes to ensure trust of external resources.



Zero Trust Enabling Technologies for Industrial Connected Workers

Zero trust enabling technologies help companies ensure that policies are consistently and continuously enforced throughout every connected worker session:

- **Mobile Device Management (MDM)** - Manages the integrity and trustworthiness of portable, company-managed devices, as well as the information they contain.

- **Identity & Access Management (IAM)** - Authenticates basic, non-privileged users and applications that want to gain access to company systems, devices, applications, and data. This includes user rights and privileges management, secure MFA session establishment, and management of security throughout the session.

- **Zero Trust Network Access (ZTNA)** - Manages user, device, and application access to network resources and ensures secure delivery of messages from network entry to exit. These solutions include IAM-like functionality to control access to networks and message encryption.

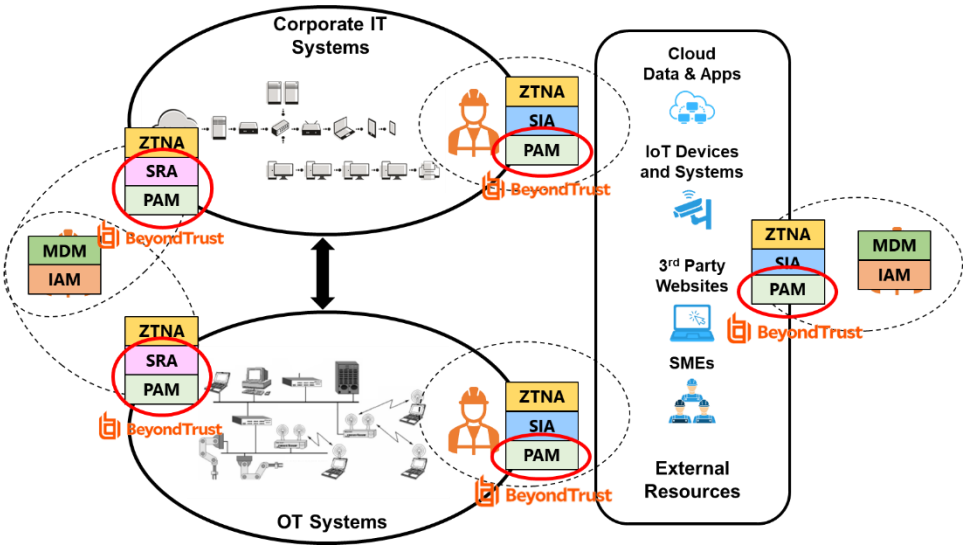
- **Privileged Access Management (PAM)** - Manages access to and use of privileged accounts and credentials within protected systems, devices, and applications. This includes privileged account and credential discovery, vaulting, randomization, and privileged session management; IAM-like functionality to ensure the trustworthiness of users requesting privileged access; and least privilege control of privileged credentials throughout the session.

- **Secure Remote Access (SRA)** - Manages the end-to-end security of remote connections into protected systems, devices, applications, and data. These solutions protect assets from compromise and exfiltration of confidential information. This includes secure external communications, secure connections with protected networks and assets, and secure management of connections and activities throughout the session.

- **Secure Internet Access (SIA)** - Enforces company policies regarding access to websites and sharing of data with external sites/parties. SIA also protects user devices from external compromises. These solutions include security features like DNS-layer security, URL filtering, cloud access security broker (CASB), data loss prevention, remote browser isolation (RBI), and malicious code detection in downloads and messages from external sites.

BeyondTrust Manages Privileges and Access

BeyondTrust offers a suite of comprehensive PAM solutions to address the risks of today's IT and OT security challenges. The company's Privileged Password Management, Secure Remote Access, and Endpoint Privilege Management product suites offer a range of capabilities to protect industrial IT and OT systems from internal and external threats. The company also has a Cloud Privilege Protection solution to support industrial companies as they transition to cloud-based services.

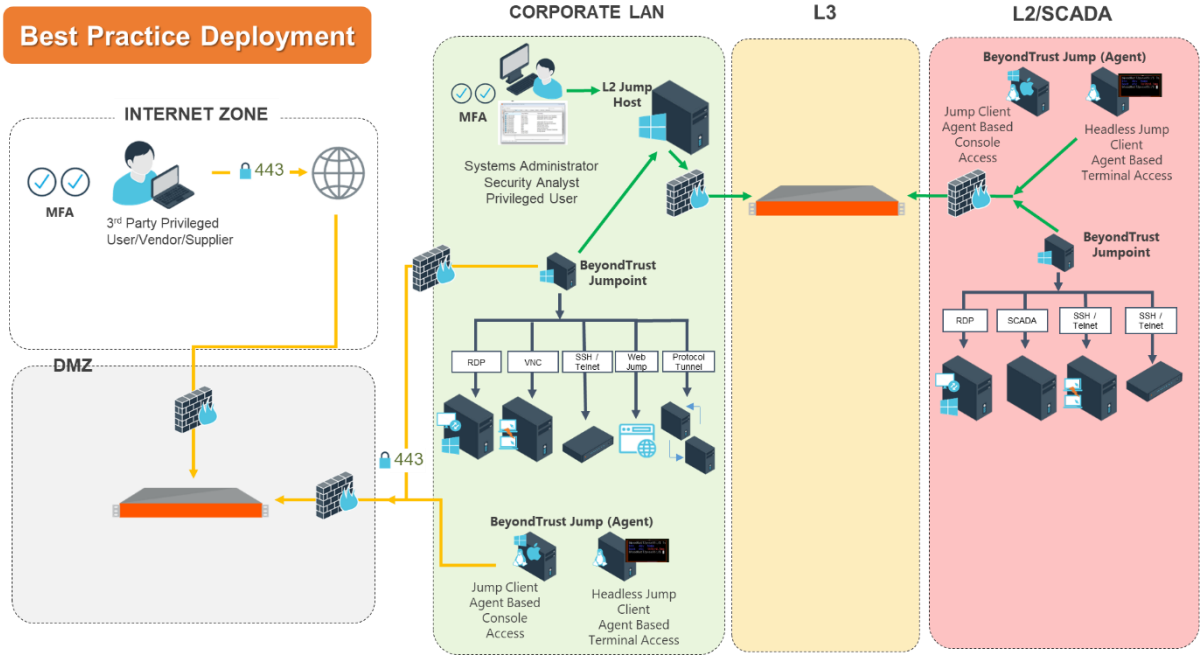


BeyondTrust SRA Solution for Industrial Connected Workers

ARC's discussions with company executives demonstrated BeyondTrust's deep understanding of the challenges IT and OT security teams face in enabling connected workers. This understanding is particularly reflected in the company's powerful Secure Remote Access solution. This solution includes functionality that spans ARC's requirements for SRA, PAM, and SIA. According to BeyondTrust, this product is being used by industrial companies for every industrial connected worker use case discussed in this report.

Secure Remote Access Capabilities

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. The company offers several different cloud-based (private cloud, hosted, etc.) and on-premise deployment options. However, for OT environments, the recommended DMZ approach entails on-premise deployment. The figure below shows how this product accomplishes its goal with minimum disruption to existing security programs.



BeyondTrust SRA Solution DMZ Deployment

BeyondTrust uses an SRA appliance to coordinate all communications between external user devices and internal assets. In the recommended approach shown above, the remote user's device communicates through SSH (port 443) messages to the SRA appliance, which is located within the DMZ. The appliance filters and forwards messages to Jump points (agents or jump servers) located within internal network segments, and the jump points manage the final connections to critical internal assets. Communications between the appliance and jump points use outbound (port 443) connections to ensure isolation.

Use of the SRA appliance and jump points has many benefits. It isolates external devices from internal assets and provides agentless MFA of users and access privileges. The solution also supports ushered access, monitoring, and session recording. Filtering of all user actions is also included to prevent unauthorized actions. Combined, these capabilities ensure that trust is properly established and maintained throughout each session. As the BeyondTrust approach completely isolates system assets from remote devices, the product can support remote access by users with managed or unmanaged devices.

Privileged Access Management (PAM) Capabilities

BeyondTrust's approach to secure remote access reflects many years of experience in protecting privileged accounts from theft and misuse. This is

particularly important when potentially untrustworthy users and devices are granted access to critical corporate systems and assets. Eliminating credential theft and privilege escalation opportunities is essential to reducing the risks of serious system compromises, like ransomware.

The PAM capabilities included in BeyondTrust's SRA and Privileged Password Management (PPM) solution support all of ARC's PAM requirements. This includes discovery, vaulting, and randomization of privileged accounts; removal of the need to share privileged accounts with external parties; and least privilege management of credentials throughout connected sessions.

Secure Internet Access Capabilities

While BeyondTrust's SRA solution is designed to protect system assets from compromise during remote user sessions, the company reports that some of their customers also leverage these capabilities to manage internal worker access to external resources. In this case, the SRA solution controls the sites that internal workers can access and the information they can download; isolates internal devices from external compromises; and protects privileged accounts and credentials.

Conclusion

Industrial companies are rapidly recognizing the benefits of enabling connected workers. The COVID-19 pandemic demonstrated how remote workers can effectively perform a wide range of critical activities and provide 24/7 support when operational issues arise. Internal workers also learned how fast, direct access to external resources helps them work more productively. Managers are embracing connected workers as a strategy for improving productivity and lowering costs. All these lessons are driving significant growth in the demand for open connectivity across the industrial spectrum.

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. The review of BeyondTrust's Secure Remote Access solution highlights the availability of effective solutions to address the secure connectivity needs of industrial control environments and to enforce the principles of zero trust. Inertia and lack of urgency to

update security stand as the biggest connected worker cyber risk for industrial companies.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com.