Zero Trust Strengthens Security Across Manufacturing Supply Chains

While digital modernization is now a given for manufacturers and industrial enterprises to remain competitive, undesirable consequences have resulted in new vulnerabilities. In the process of digitally transforming their operations and connecting heterogeneous devices and systems, enterprises are also significantly expanding their attack surfaces.

Manufacturing supply chain security vulnerabilities involve the flow of data, with risk factors across the enterprise and partner networks, systems, applications, and endpoints. Every company within the supply chain has a responsibility to protect their data. A manufacturer's supply chain, as a whole, is only as secure as the sum of its parts, as each entity employs effective and coordinated security measures.

Cyberattacks are increasing in virtually every industrial sector and critical infrastructure, including industrial manufacturing, transportation, energy, and water treatment facilities. In their annual Data Breach Investigations Report, Verizon found 73% of attacks against manufacturers were financially motivated, with the balance engaged in espionage. The chances of being the victim of an attack are high. A study of the manufacturing sector conducted by Sikich, found 50% of companies experienced a cyberattack or breach during the previous 12 months.

ICS equipment is at risk

The damages cybersecurity breaches can inflict are many, including shutting down systems, manipulating industrial control system (ICS) behavior, overriding safety, backup and failover systems, and more. Common attack methods include malware, ransomware, phishing, DDoS attacks, remote access intrusion, USB drop attacks and others.

A core protection against cybercrime is the use of cybersecurity platforms with zero trust network access (ZTNA). This approach protects the confidentiality of data on endpoints transmitted over networks, and stored within cloud and on-premises servers and storage systems. Modern cybersecurity platforms can include endpoint security, email security, zero trust networking, privileged access management, deception technology and other security capabilities. A cybersecurity platform is a crucial part of the complete security stack that helps protect manufacturers and industrial facilities from infiltration.

"A manufacturer's supply chain, as a whole, is only as secure as the sum of its parts, as each entity employs effective and coordinated security measures"

Modern technology transformations are putting OT at risk

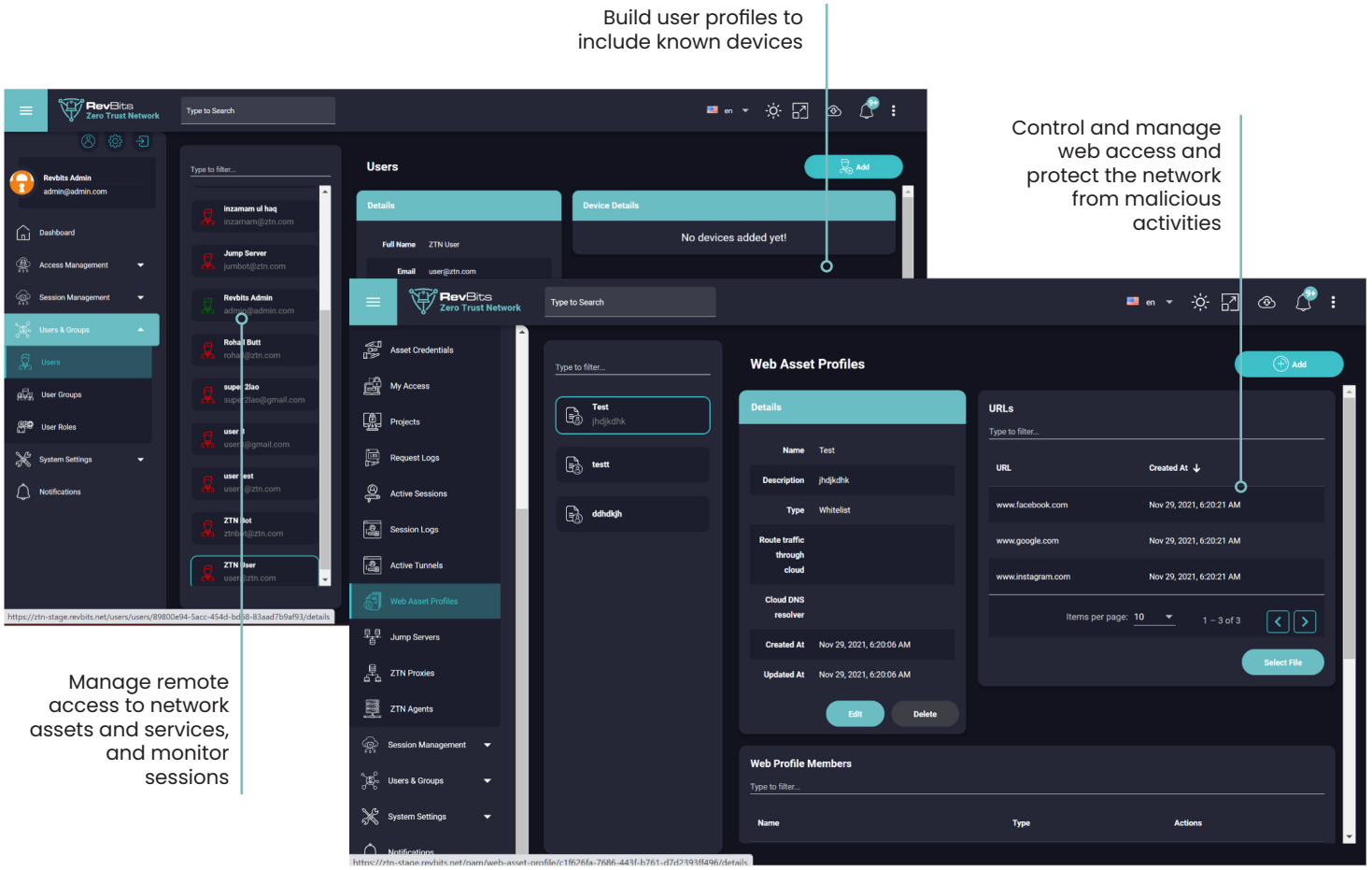
Manufacturers and industrial enterprises still rely upon legacy equipment, like supervisory control and data acquisition (SCADA), distributed control systems, and industrial automation control systems. Cybersecurity threats are increasing with the exponential growth of IoT, industrial IoT and technology integration gaps between enterprises and their supply chain partners.

Security was often a peripheral concern during the early meteoric proliferation of IoT devices. Today, it's a different story, as these network-connected devices are now highly vulnerable. Protecting IoT, and particularly legacy systems, has its challenges. Critical ICS and SCADA infrastructure, where there is a convergence of OT and IT networks, are expanding cyberattack surfaces, creating more security vulnerabilities.

RevBits ZTN locks down access to enterprise assets

Zero trust is a strategic approach that helps prevent breaches by removing trust from an enterprise's digital infrastructure. It isn't about creating trusted systems; it's about removing trust as a factor from entities accessing digital infrastructure from inside or outside the enterprise. It treats every user, device, application and workload as untrusted.

Zero trust isn't represented by a single product or solution, but requires a range of strategies, policies and solutions. RevBits ZTN enables a zero trust network architecture for manufacturers and industrial enterprises. Multifactor authentication (MFA), a core building block of the zero trust framework, is an inherent feature of RevBits ZTN. MFA provides multi-layered authentication protection against attackers using stolen identities to gain access to a network and its resources. RevBits ZTN includes embedded



RevBits ZTN admin dashboard for creating user profiles to manage remote access

privileged access management (PAM), with native identity-based authentication, MFA, single sign-on (SSO), end-to-end encryption, session recording and more. Remote access authentication and authorization protect resources inside the network, and encrypted tunnels secure connections for outside network traffic.

Zero trust that scales to meet dynamically changing needs

RevBits ZTN meets the system resource and scalability demands of legacy systems, IoT, and industrial IoT devices, as well as the security demands required for use in OT/ICS environments that manage critical infrastructure.

RevBits ZTN is based upon an award-winning privileged access management solution, with the understanding that the key to securing assets is ensuring access is tightly controlled and monitored. RevBits ZTN architecture expands PAM capabilities to control access for all users and devices, regardless of what they want to access, or their geographic location.

Built on a service-initiated zero trust network access model, RevBits ZTN is free of client-side installs. User onboarding is efficient and seamless, and resource access is quick, requiring only a few clicks. In addition, a thin-client approach provides access from any web browser or smart device.

As business expansion grows, RevBits ZTN scales effortlessly, through its dynamic autoscaling architecture. As a result, increased access demands on corporate resources are easily handled, regardless of geographic location, or time of day. With pre-positioned Proxy Servers distributed across twenty-four worldwide geographic cloud regions, RevBits ZTN is always available, and ready to handle all requests.

In this ever-changing anywhere work environment, the remote workforce continues to grow, expanding perimeters. RevBits ZTN is ready to manage the demand. Auto-scaling ensures that access demand loads are balanced and resources are highly available. If additional security is needed to monitor access, kill sessions, or record activity, natively pairing ZTN with RevBits PAM provides the ultimate access management and control.

To remain competitive, manufacturers and industrial enterprises must provide secure and reliable access and connectivity with their supply chain partners. Today's technology-driven business environment has enabled enterprises to leverage digital transformation to unlock a value chain of capabilities that bring operational efficiencies and competitive advantages. RevBits ZTN enables the control and access protection they need today, and for the future.

Identify, isolate, and monitor remote network connections and access to corporate resources in real-time. **Learn more** about RevBits ZTN. Watch an informative **RevBits ZTN video**.

RevBits®, LLC • 34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248)