Pulse Secure Expands Zero Trust Security for IoT with Firewall Auto-provisioning and Behavioural Analytics

Pulse Secure version 9.0R3 helps customers secure industrial IoT and streamline maintenance activities for greater production line output as well as reducing costly production downtime

Pulse Secure, a provider of Secure Access solutions to both enterprises and service providers, has announced the release of Pulse Policy Secure (PPS) 9.0R3 to extend its Zero Trust Security model to IIoT devices and smart factories. The new version enables factories to streamline machinery repairs and diminish costly production downtime through IT-managed secure access. It also secures networks by expanding its behavioural analytics to IoT devices, detecting anomalies and preventing their compromise.

"Manufacturing customers are using IoT to retool their factory floors, creating smart production lines that report their health and operational efficiency. One benefit of this approach is that customers can proactively perform preventative or predictive maintenance on machines to avoid costly production outages," said Prakash Mana, Pulse Secure's Vice President of Product Management. "Our latest Pulse Secure release helps customers not only secure the smart factory floor, but it also helps streamline their maintenance activities by giving service technicians remote access to the equipment they maintain. Regardless if they are on the factory floor or in their remote office, our Zero Trust Security limits technician access to the equipment they maintain and requires that they use secured end-user devices to perform their work."

Pulse Policy Secure (PPS) is an integral part of Pulse Secure's combined VPN and NAC solution that provides corporate networks with Zero Trust Security through visibility, "comply to connect" policy enforcement and security orchestration with popular network and security infrastructure. PPS dynamically profiles the network to discover, classify and apply policy to IoT devices, and includes a built-in IoT device identification library. The solution also integrates with Next Generation Firewall (NGFW) solutions to provide identity and device security state data, as well as to fortify micro-segmentation to isolate and manage IoT devices on enterprises networks.

PPS 9.0 extends the Zero Trust Security model to IIoT devices used in smart factories and buildings, with blended IT and OT environments. It automatically discovers and profiles IIoT systems, such as factory floor SCADAs, PLCs and HMIs, or office building HVAC systems, providing dynamic visibility and securing them by enforcing policies for local and remote access by authorized users and contractors. PPS 9.0 also automatically provisions IIoT devices to next-generation firewalls (NGFWs) to facilitate remote access without provisioning overhead.

> **"Manufacturing customers are using IoT to retool their factory floors, creating smart production lines that report their health and operational efficiency.**

"A top priority for manufacturing customers is complete visibility and security of IIoT devices on smart factory floor environments. Because failing systems may lead to loss of revenue or human life, customers must emphasize rapid remediation of machines to avoid system outages," said Tony Massimini, Frost & Sullivan Senior Industry Analyst, Information & Network Security. "The latest Pulse Policy Secure release helps customers protect factory floor system integrity by providing technicians secure remote access. New Behavioural Analytics features also safeguard against attacks by detecting anomalous activity."

The latest release of PPS also provides sophisticated behavioural analytics that alert security teams of anomalous IoT device behaviour and automatically requires added factors of authentication. PPS 9.0 builds baseline behaviour profiles for managed and unmanaged IoT devices utilising information correlated from multiple sources such as NetFlow, user and device data. With these profiles, the platform detects anomalous activity, malware infections and domain generation attacks, allowing security teams to be more responsive to threats and take preemptive measures before attacks succeed.

The new PPS 9.0 IoT support also provides practical relief for the frequent and costly issue of factory floor equipment outages. Aberdeen recently reported that 82% of companies reported unplanned downtime in the past three years, which can cost a company as much as $260,000 an hour.

The resulting downtime breaks production and lowers profit, because factory floor repairs often take days when security requirements mandate that service technicians physically visit the factory to diagnose and repair the problem. The latest PPS release works seamlessly with Pulse Connect Secure to solve the problem in an innovative way. The combined NAC and VPN approach enables IT teams to grant remote secure access—authenticated and encrypted—to support contractors for expedited repair and return to service of factory IIoT systems for greater uptime and productivity. IT teams ensure security with remote zero-trust access via auto-provisioned NGFWs, and by enforcing security policies that authenticate contractors based on their technician role, endpoint device status and authorisation to work on the targeted IIoT device.

"Some of our customers operate among the manufacturing and transportation industry's biggest and most distributed internet-connected device deployments. These IIoT networks help our customers gain real-time system diagnostics, reduced downtime and overall lower operational costs," said Kirk Hanratty, Vice President and Chief Technical Officer at IT security and solutions company SynerComm. "For these and other customers, IIoT drives their business where assuring availability and secure access throughout an IIoT infrastructure is paramount. We have found Pulse Secure's platform to offer our customers the usability, interoperability and reliability necessary to support large scale IIoT applications."

Availability

The latest features of Pulse Policy Secure 9.0 are available on physical or virtual Pulse Secure Appliances (PSA). Existing customers with PSA appliances under PPS subscription or software maintenance can readily upgrade at no charge. PPS on a virtual appliance with a three-year subscription starts at $31,000 MSRP for 500 concurrent connections. Pulse Connect Secure customers can cost-effectively extend their VPN investment to include network visibility, access control and mobile security with the Pulse Access Suite.

Those interested in learning more on the topic are invited to register for the January 8th, 1 p.m. EST webinar, "Zero Trust Secure Success for the Industrial Internet of Things."

Pulse Secure, LLC offers easy, comprehensive Secure Access solutions that provide visibility and seamless, protected connectivity between users, devices, things and services. The company delivers suites that uniquely integrate cloud, mobile, application and network access to enable hybrid IT. More than 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data centre and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.