Picture credit: AdobeStock

NETWORK PROTECTION

Tyler Gannon *explains why securing hugely complex OT and IoT networks puts PAM technology centre-stage*

Amid the massive growth in IoT networks, machine identity is fast becoming a major security challenge. The number of IoT devices worldwide is expected to more than double from 16-billion in 2023 to over 32-billion in 2030. Many devices will be in the consumer market, but the industrial, automotive and healthcare sectors are also destined to see major expansion of IoT connections, with Statista forecasting 16 percent compound annual growth in Industry 4.0 technologies up to 2028.

The challenge is to secure data generated and handled by these devices, and to prevent them from becoming botnets or acting as points of entry to connected IT systems where criminals can exfiltrate or ransom valuable data. The CyberArk 2024 Identity Security Threat Landscape Report revealed that more than two-thirds of surveyed security professionals believe as many as half of all the machine identities in their organisation have access to sensitive data.

Across sectors such as manufacturing, energy and logistics, the rapid proliferation of devices introduces new vulnerabilities that traditional identity and access management (IAM) systems were not designed to address. Organisations must therefore rethink their strategies to protect this expanding digital frontier by securing devices, automating identity processes, and implementing effective lifecycle management for a diverse range of devices.

In the manufacturing sector especially, organisations need to take best-in-class privileged access management (PAM) approaches and integrate them fully, extending them across the shopfloor. In effect, this is extending the principles of zero trust access to encompass almost all the devices in an operational technology (OT) network. A zero-trust framework that extends throughout the lifecycle of both human and non-human identities ensures each identity, whether it belongs to a person, device, or process, is verified, authenticated and granted only the minimum level of access required for its role.

Cyber attacks using valid credentials shot up 71 percent last year

Thousands of organisations already apply PAM to the monitoring and protection of privileged accounts, to give staff and authorised partners and suppliers special access to maintain efficiency and security in IT. This covers the principle of least privilege – giving no more access than is strictly required. It also includes session management, password management and multi-factor authentication.

PAM therefore provides the necessary control and oversight when systems access is required by people inside or outside the organisation. These are the protocols that should be extended across OT and IoT networks to cover machine identities and credentials, so that devices are not hacked or logged into by criminals, state-sponsored hackers or malign insiders.

Managing the identity lifecycle of vast arrays of connected devices is critical to prevent serious harm. In poorly secured industrial IoT (IIoT) hackers are not only able to use stolen or unprotected device identities to gain access to sensitive data, but they can also threaten the health or wellbeing of large numbers of people. Causing healthcare devices, water treatment plants or connected vehicles to malfunction is potentially extremely serious.

The identity-related threats are real enough. Cyber attacks using valid credentials shot up 71 percent, according to IBM in its X-Force Threat Intelligence Index last year. As the report's introduction says: "In this era the focus has shifted towards logging in rather than hacking in." Through social engineering, phishing or inadequate or out-of-date device security, criminals can acquire the credentials they need to gain access.

For many organisations, the biggest risk lies in machine identities in OT accounts or IoT devices that allow attackers to operate unnoticed. The 2024 Waterfall ICS STRIVE report found a 19 percent year-on-year rise in OT security incidents with physical consequences, demonstrating that threats are far from theoretical and the repercussions are very real.

Managing identities in OT and IoT environments presents a very different set of difficulties compared with traditional IT however. In typical IT environments, the focus is primarily on human identities – employees, administrators and other personnel. However, in OT and IoT environments, devices can outnumber human users by as much as 45-to-one.

Every device in these environments requires a unique machine identity, sometimes several per device, complete with authentication credentials and specific access controls, so it can interact securely within the network. This complicates the security framework, as each device must be meticulously managed to prevent unauthorised access and potential breaches.

Compounding the complexity is the fact that many devices were designed to function in isolated, air-gapped setups. Many OT devices have little or no in-built security and were never intended for remote access through internet connectivity. Yet these devices must interact with multiple systems in today's IoT/OT networks. Alongside the surge in internet connectivity, IoT networks are also managed from the cloud, 5G and satellite, bringing with them significant security challenges when managing the identity lifecycle of a vast array of connected and diverse devices.

The sprawling and uncharted nature of many networks, which may have been built up over decades, is another major obstacle. Many organisations' IT teams are not fully aware of all the devices for which they are responsible, let alone the state of the security in each of them. As organisations integrate their IoT and OT with broader IT systems, they create extensive attack surfaces vulnerable to malicious actors. But if organisations are unaware of all the devices they own, the task of defending a network is that much harder.

AUTOMATION ELIMINATES MUCH OF THE HUMAN ERROR THAT CAN LEAD TO SECURITY BREACHES

Lifecycle management across these devices introduces an additional layer of difficulty. From deployment to decommissioning, each device's access must be carefully managed, especially as they connect with various systems and even change ownership over time. Traditional manual IAM processes fall short in these contexts, as they cannot keep pace with the rapid evolution and proliferation of devices, each requiring distinct and ever-changing credentials.

The volume of work necessary to maintain protection in industrial IoT is beyond human capacity. Machine identities are complex. Each comes with its own set of digital encryption keys and requires a password which must be rotated. Every access request must be approved and then each device must recognise the approved credentials. When humans are burdened with all this, errors are inevitable, presenting major opportunities for hackers, ransomware gangs and employees or contractors with grudges.

To effectively manage identities in OT and IoT settings, organisations must adopt a comprehensive, automated approach. They need to start by mapping all the devices on their networks. Then they must bring PAM into management of the entire lifecycle of a device's identity.

Integration of PAM solutions safeguards high-risk identities and sensitive systems, extending strategies traditionally used for human identities to encompass device identities as well. Through centralised control and policy enforcement, PAM systems ensure secure access to critical devices and systems while maintaining operational efficiency, seamlessly weaving security into daily operations.

Extending zero trust across a network means benefiting from automation that deploys tested PKI (public key infrastructure), zero trust technology at scale and IAM provisioning. In addition, there is a need for policy-driven data encryption and continuous, automated monitoring of ecosystems. To be effective, that requires AI.

PKI security is vital. It is based on certificate assurance – an approach that has evolved to resolve problems of identity, authentication, integrity and privacy. It has now overcome the difficulties of scaling

for IoT, especially for devices with no UI or associated user. Policy-driven automation ensures IoT device certificates are securely generated, signed and managed. Automation is obviously essential for greater efficiency and removal of human errors, and to enforce uniform security standards across every device and identity within the network.

The benefits of automating identity lifecycle management for OT and IoT devices are substantial, particularly in terms of speed, security, and scalability. Automation eliminates much of the human error that has historically led to security breaches.

This not only improves the accuracy of identity management, but also significantly boosts response times to potential security incidents. Events and alarms from a PAM platform should be fed into SIEM (security information and event management) and SOAR (security orchestration, automation and response) systems to increase speed and effectiveness. Even if a device's credentials are compromised, the damage can be contained to prevent it from spreading across the network.

Security teams can act swiftly to mitigate risks before they escalate, ensuring that vulnerabilities are addressed promptly and efficiently. Such advanced PAM solutions enable organisations to uphold stringent security standards while ensuring smooth, interconnected operations.

Alongside automation, detection and faster incident-response, implementing a comprehensive identity lifecycle management solution simplifies regulatory compliance. This must be a critical consideration for organisations operating in industries where regulation is substantial and the stakes extend beyond financial losses – such as energy, manufacturing and healthcare.

Compliance with strict security regulations is essential and the integration of automated identity management to cover IoT and OT networks provides demonstrable control of access and the constant upgrading of security measures across the lifecycle of each device and system. This consistency not only aids compliance, but also overhauls any organisation's entire security posture, providing peace of mind.

Looking ahead, as the volume and complexity of connected devices grow, identity lifecycle management solutions will need to evolve to keep pace. Emerging technologies, such as AI-driven analytics, offer promising enhancements in real-time threat detection and automated responses, which will be pivotal to future identity management frameworks.

The implementation of smart city concepts and significant initiatives to reindustrialise Europe and the USA to protect supply chains are only likely to further increase the importance of enhanced IoT/OT security based on automation of privileged access management. A survey of 1,300 executives at large companies conducted for the Capgemini Research Institute, found 48 percent of organisations engaging in reindustrialisation plan extensive use (for more than 50 percent of processes and activities) of IoT and industrial IoT technologies.

This is the context in which major companies must plan for scalability, ensuring that their identity management solutions can adapt as their OT and IoT ecosystems expand. Future developments are likely to emphasise even greater automation, more refined real-time monitoring capabilities, and enhanced interoperability across diverse environments in an increasingly interconnected world.

Securing identities in proliferating OT and IoT environments is a multi-faceted challenge that requires a strategic, automated approach. As connected devices perform ever more complex tasks, organisations that take security seriously will need more robust identity lifecycle management to safeguard their digital infrastructure.

By adopting comprehensive, automated solutions rooted in zero-trust frameworks and PAM systems, businesses can effectively mitigate the identity and credentials-based threats they face and ensure the security and integrity of their operations into the future ●

Tyler Gannon is VP North American Ops at Device Authority.

Every device requires a unique machine identity, sometimes several per device, complete with authentication credentials and specific access controls, so it can interact securely within the network