SECURING INDUSTRY 4.0 AND THE IIoT WITH STEALTH™

STEALTH™

If you're an industrial operator, your world is changing rapidly. Digitalization and the adoption of Industrial Internet of Things (IIoT) devices, sensors, and networks are having a profound impact on everything from how you manage your supply chains to the types, quantities, and level of customization of the finished goods and services you produce.

Referred to collectively as Industry 4.0, these digital technologies and low-cost sensors are upending centuries-old business models to help industrial organizations increase efficiency, improve safety, gain visibility into supply chains, and to predict and avert machine failures before they happen. By effectively leveraging these technologies, you can deliver a superior customer experience, reduce costs, and generate greater profits. To reap the benefits of Industry 4.0, however, it is critical that your IIoT networks and devices are secure.

Many moving parts make up the digital value chain enabling these benefits: high-speed wireless data networks and protocols, cloud computing, AI and machine learning, big data, analytics, mobile devices, cheap data storage, faster CPUs—the list is long, and as one technology improves it tends to enable yet more innovation in other areas.

As with past technological and industrial advancements such as robotics and automation, operators who embrace these technologies are expected, over time, to outperform those who do not. And though digitalization and the IIoT present multiple benefits and new business opportunities, they do come with some risk – specifically, an increased threat of cyberattacks on operational infrastructure and systems.

What Is an IIoT Device?

The Industrial Internet Consortium (IIC) defines an IIoT device or endpoint as a "component that has computational capabilities and network connectivity." This can include a lot of things in an industrial setting; from simple temperature sensors to connected pumps and valves to fully functioning, autonomous robots. For the purposes of this paper, we are focusing on the sensors, actuators, and industrial control points that make up the vast majority of IIoT deployments and serve as the foundational elements of most IIoT ecosystems.

While industrial operators have been using these devices in their operations for decades, what's changing today is the different types and ever-increasing number of these devices being put into operation; the operating systems they run on (and vulnerabilities of each); where they are being used; the use cases to which they are being applied; the increasing connectivity between IIoT devices, controls systems and other IIoT devices; and the fact that the communications networks they use no longer are isolated from the outside world.

With digital factories and a digitally connected value chain, traditional IT security is not enough to protect the business. To overlook this reality is to compromise the stability and security of the company.

– CGI report:
Industry 4.0 Making your business more competitive

Taken together, these various factors can make each IIoT device a potential point of vulnerability attackers can use to infiltrate your operational systems. Granted, a temperature or vibration sensor doing little more than reporting back to a control system via a secure gateway that prohibits bidirectional communications is much less of a threat to you than an unpatched actuator connected to the control system of a chemical plant. But even these types of sensors are getting smarter and more powerful all the time. As their capabilities increase, so will the number of places where they will be deployed.

Over the next five years the adoption of IIoT devices, platforms, and applications is predicted to be significant. Growth estimates vary widely because of the many use cases, different definitions of what IIoT is, and the verticals into which IIoT devices and applications can be applied. Studies have placed the Compound Annual Growth Rate (CAGR) anywhere between 8% and 18% through 2024. The dollar value estimates of these markets are in the tens to hundreds of billions.

The Myriad Benefits of Industry 4.0

The reason for such rapid growth is the promise of Industry 4.0, which brings together and integrates a range of disparate operational and IT technologies such as sensors, networking, the SCADA control system architecture, and cybersecurity to help industrial operators reap the benefits of connected ecosystems. IIoT devices are central to these efforts because they generate the massive amounts of data that serve as the foundation upon which Industry 4.0 is built.

In the near term, industrial operators are looking to use IIoT data to improve operations through increased insights into how their operations actually are performing, rather than how they were designed to perform. Specifically, they are using this data to streamline processes, optimize inventory, gain visibility into their supply chains, and conduct predictive maintenance.

According to a 2016 presentation by Stephen Ezell, vice president, Global Innovation Policy at the Information Technology and Innovation Foundation, the auto maker BMW already knows the real-time status of all the machines producing parts from all of its suppliers. Toyota is reducing recalls by tracking exactly what machine produced which components and onto which vehicles they were installed. And, at Ford, downstream machines can tell if parts are out of spec even by fractional amounts, triggering maintenance activities in upstream machines.

In a more recent example, McKinsey reports that, "[a] top ten global energy company has used IoT applications as part of a broader process- and technology-upgrade program to reduce unit production costs by 33% over five years. In the last three years, it has saved more than $9 billion in capital costs. Applying IoT-enabled analytics to drilling-well data has also helped the company increase the yield of mature oil wells."

The Challenges Are Many

For most organizations, though, these types of returns are aspirational. Given the obstacles that can prevent Industry 4.0 deployments from moving beyond pilot projects, the majority of industrial operators still are working through the early stages of adoption.

A 2019 Bain & Company survey report, *Beyond Proofs of Concept: Scaling the Industrial IoT*, concluded that, "... although the long-term predictions remain positive, in the short term, customers expect implementation to be a bit slower than they did in 2016."

Bain cites IT/OT integration issues with existing systems, a lack of in-house expertise, data portability issues, transition risks, and unclear ROI, among others, as the current barriers to adoption. Topping this list of concerns is cybersecurity. And for good reason.

Most executives we surveyed (60%) said they were very concerned about the risks IoT devices pose to their companies—not surprising, given the damages that an IoT security breach can cause to operations, revenue and safety.

– Bain & Company brief: Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

As once-isolated systems become exposed to external networks such as the internet or are linked to production networks using newer communications protocols such as Zigbee, Wi-Fi, or LoRaWAN, they can become visible to hackers.

Compounding the problem, the vast majority of IoT devices aren't manufactured with security in mind: firmware cannot be updated; usernames and passwords, when present, are unchangeable and often easily guessable (think "admin/admin" easy); devices that can be updated keep ports open to listen for the latest patch or upgrade; some devices can be physically accessed via a USB port that could allow attackers to place malware directly onto the device without ever infiltrating the network; and misconfigured devices, applications, and networks can open up holes for attackers to find using publicly available IoT search engines such as Shodan that seek out connected IoT devices broadcasting their locations. These are just some of the potential avenues of compromise.

In January 2018, for example, the Okiru botnet (a variation of the infamous Mirai botnet that took over connected CCTV cameras in 2016 to take down DNS servers across the internet) was found to be actively targeting the ARC processors sitting at the heart of billions of IoT devices worldwide. According to CSOOnline.com, Okiru is targeting devices running the insecure TelNet protocol, which, like many older industry protocols, exchanges information (like passwords) in plain text.

Fortunately, there are solutions still in use worldwide that can protect even the most insecure devices and oldest insecure protocols, such as TelNet. Prime among these is the idea of Zero Trust. Zero Trust assumes that all network users and endpoints are compromised from the start. In Zero Trust cybersecurity ecosystems, all users and devices can access only the predetermined data and applications they need to do their jobs or execute, in the case of an application, a function. These least-privilege environments, as they are called, provide a powerful means of keeping people from accessing data and applications they have no reason to access.

Unisys Stealth - Zero Trust Security for IIoT Environments

Unisys Stealth® is software-defined security. It simplifies yet improves your network security and serves as the backbone of your whole-network Zero Trust strategy. Stealth™ blankets every corner of your organization's computing environment with one holistic, consistent, and unwavering security policy—from mobile phones and desktops, to servers, to cloud, and even IoT. In fact, Stealth orchestration and deployment are highly automated and centrally managed.

As your security policies evolve, changes can be made and instantly propagated across the enterprise. Meanwhile, Stealth monitors and enforces all your Zero Trust policies, automatically isolating violators and alerting administrators. With Stealth Zero Trust, security is seamlessly woven into the fabric of your entire network. It's the engine that drives your speed to security.

By creating cryptographic zones, Stealth delivers Zero Trust through micro-segmentation, compartmentalization that place users and devices into Communities of Interest (CoIs). These secure enclaves rely on hypersecure IPsec tunnels between CoI endpoints to encrypt data from end to end. Outsiders cannot gain access into the CoI, and data cannot be exfiltrated out.

Applications and servers within the CoI will not respond to pings, scans, or other means of network reconnaissance, rendering attackers blind to network topology and application dependencies, thanks to Stealth's patented SCIP protocol that "cloaks" endpoints. All elements within the CoI are invisible to outsiders. Best of all, Stealth scales quickly, easily, and works on any existing TCP/IP network—on-prem, in the cloud, or integrated into a partner's network.

Because Stealth is an overlay networking technology that works at OSI Layer 3, the network layer, application latency is not an issue. Lightweight agents are installed on your endpoints to facilitate authentication. Roles and authorizations come from either Microsoft's Active Directory or LDAP calls to Identity and Access Management (IAM) systems.

Most importantly, endpoints such as low-power IIoT sensors, devices, or servers that cannot accept agents can be protected via the Unisys Smart Wire component that sits between the device(s) and your control system. Secure Virtual Gateways (SVGs) act as the de facto agent for these devices allowing them to be assigned to CoIs. You can configure SVGs to apply different roles to a single IP address or ranges of IP addresses.

Stealth also provides a valuable tool that is essential for security and operational awareness. Stealth Security Dasboard is a comprehensive, real-time security dashboard that provides you with a clean, simplified look at the status of your network in a single view. This enables you to safely address your business outcomes with immediate insights about the environment, your users and their devices that were isolated, your isolations trends and statistics. This will in turn help you make informed decisions, meet compliance requirements, and improve the overall security of your enterprise.

Stealth Is a Compliant Solution

While cybersecurity frameworks and standards ffor IIoT device manufacture do exist, they have not yet been widely adopted by device makers. Given the concern over connected device security, lawmakers are stepping in. On January 1, 2020, for example, California's new IoT cybersecurity law, SB 327, went into effect. This bill requires IoT manufacturers to incorporate "reasonable security" features (such as updateable passwords) into their products. Similar legislation is being pursued in the U.S. Congress, the U.K., and Japan.

Few manufacturers adequately test hardware against known vulnerabilities before shipping, and far more devices fall short during ongoing tests for new vulnerabilities.

– Bain & Company brief: Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

Until this situation changes, and IIoT device makers manufacture products that are Secure By Design (SBD), it will be up to you to ensure your IIoT ecosystems are secure. And even when SBD devices are the norm, you still will need to keep your operations secure.

That's why Unisys has worked with standards-setting bodies IEC/ISA and North American Electric Reliability Corporation (NERC) as well as Colombia's CNO (which sets safety guidelines for electricity generators in that South American country) to ensure that Stealth's cryptographic zoning is an acceptable technology for organizations that need to show compliance with either IEC/ISA 62443-1-1, NERC/CIP 6.0, or CNO 1241.

In Summary

Unisys Stealth provides you with a flexible, compliant, extensible security solution based on one software-defined security fabric. You can set policies and role-based protections from one central console, eliminating complex management and the need for multiple security point solutions.

Real-time proactive isolation of malicious devices and operations when threats are detected ensures protection from both internal and external threats. In short, Stealth improves security, reduces costs, and streamlines management of your entire Industry 4.0 environment.

Contact us today at Stealth@unisys.com Visit us at www.unisys.com/stealth

For more information visit www.unisys.com