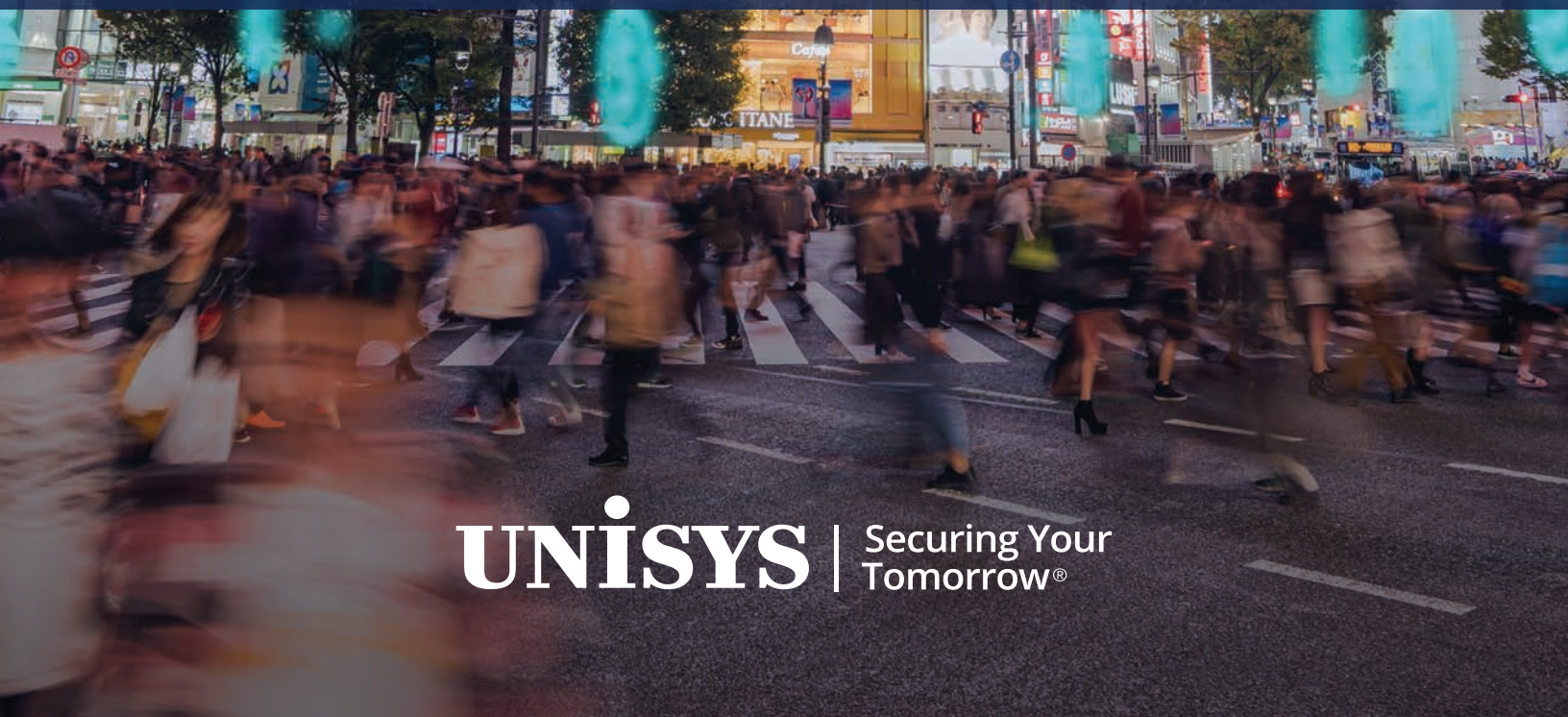
SECURING INDUSTRY 4.0 AND THE IIoT WITH STEALTH™



UNISYS | Securing Your Tomorrow®

Securing the Industrial Internet of Things (IIoT) is critical if industrial operators want to reap the benefits of Industry 4.0.

For industrial operators, the world is changing rapidly. Digitalization and the adoption of IIoT devices, sensors, and networks is having a profound impact on everything from how they manage their supply chains to the types, quantities, and level of customization of the finished goods and services they produce.

Referred to collectively as Industry 4.0, industrial operators across verticals are using digital technologies and low-cost sensors to up-end centuries-old business models (think product-as-a-service), increase efficiency, improve safety, gain visibility into their supply chains, and predict machine failures (and fix them before they happen).

Ultimately, the goal is to simultaneously improve the customer experience, reduce costs, and increase profits using the same set of commercially available technologies like systems-on-a-chip, low-cost sensors, and TCP/IP network protocols that also underpin the consumer IoT market.

There are many moving parts that 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 well.

Just like with past technological and industrial advancements like robotics and automation, operators who embrace these technologies are, over time, expected to outperform those who do not. And while digitalization and the IIoT present a host of benefits and new business opportunities, they do not come without some risk. Specifically, an increased threat of cyber attacks on operational infrastructure and systems.

What Is an IIoT Device?

But before we can talk about the opportunities and risks presented by the IIoT, you have to define it first. 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 are no longer 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 that attackers can use to infiltrate your operational systems. Granted a dumb temperature or vibration sensor that does little more than report back to a control system via a secure gateway that does not allow for bi-directional communications is much less of a threat than an unpatched actuator that is connected to the control system of a chemical plant.

But even "dumb" 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 uptake 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 CAGR anywhere between 8 and 18% between now and 2024. The dollar value estimates of these markets are in the tens to hundreds of billions.

The Myriad Benefits of Industry 4.0

Regardless of which number is ultimately correct, the reason for this 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, SCADA, cybersecurity, and the like 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 serves 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 are actually performing (not 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."

Challenges Are Many

For most organizations, however, these types of returns are aspirational. Given the many challenges facing Industry 4.0 deployments moving beyond pilot projects, operators are still working through the early stages of adoption.

A 2019 Bain & Company survey, *Beyond Proofs of Concept: Scaling the Industrial IoT*, found 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 like the internet or are linked to production networks using newer communications protocols like Zigbee, Wi-Fi, or LoRaWAN they can become visible to hackers.

Compounding the problem is the vast majority of IoT devices are not 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 mis-configured devices, applications, and networks, can all open up holes for attackers to find using publicly available IoT search engines like Shodan that search for connected IoT devices broadcasting their locations... to name just a few potential avenues of compromise.

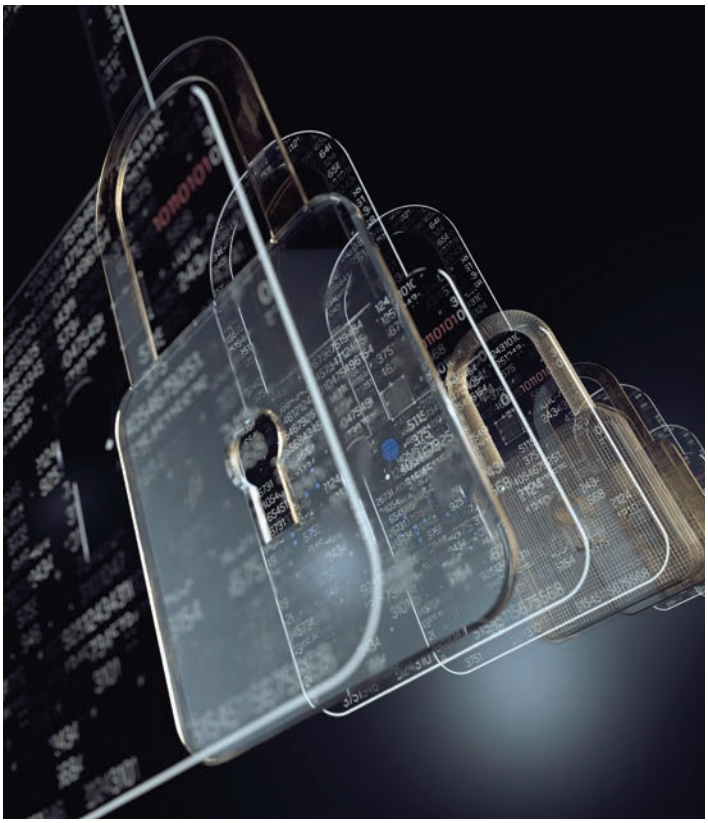
In January 2018, for example, the Okiru botnet (a variation of the infamous Mirai botnet that took over connected CCTV cameras in 2016 to take down DNS servers across the internet) was found to be actively targeting the ARC processors sitting at the heart of *billions* of IoT devices worldwide. According 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 that can even secure the most insecure devices and oldest insecure protocols, like TelNet, that are still in use worldwide. 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 are restricted access to just the pre-determined 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 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 once 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 and speed to market.



By creating cryptographic zones, Stealth delivers Zero Trust through microsegmentation, compartmentalization, that place users and devices into communities of interest (COIs). These secure enclaves rely on hyper-secure IPsec tunnels between COI end points 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. 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 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 to this discussion, endpoints such as low-power IIoT sensors, devices, or servers that cannot accept agents can be protected via Secure Virtual Gateways (SVGs) that sit between the device(s) and the control system. SVGs act as the de facto agent for these devices allowing them to be assigned to COIs. SVGs can be configured to apply different roles to single or ranges of IP addresses.

Stealth Is a Compliant Solution

While cybersecurity frameworks and standards for 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 which requires IoT manufacturers to incorporate "reasonable security" features (like updateable passwords) into their products. Other legislation is be being pursued in the US Congress, the UK, and Japan, as well.

> *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 IoT device makers produce products that are secure by design (SBD), it will be up to operators to ensure their IIoT ecosystems are secure. But, even when SBD devices are the norm, operators will need to keep their operations secure.

That is why Unisys has worked with the standards setting bodies IEC/ISA and North American Electric Reliability Corporation (NERC) as well as Columbia's CNO, which sets safety guidelines for electricity generators in Columbia, 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 industrial operators with a flexible, compliant, extensible security solution based on one software-defined security fabric. Policies and role-based protections are propagated 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