JACK BROWNE, Technical Contributor

Cybersecurity Critical to Safeguarding IoT/IIoT Connections

Learn how the latest IoT and IIoT devices ensure secure connectivity against cyber threats, whether wired or wireless. Explore cybersecurity measures in this comprehensive guide.

Secure connections are essential for many internet-based devices. As the number of devices connected to the internet escalates, opportunities to steal data or information also increase, heightening the need for internet cybersecurity protection. Networked information can be captured from any internet interconnection, including Internet of Things (IoT) and industrial IoT (IIoT) devices.

If not properly protected, those devices can become unintended access points. They can allow data to be subtracted and malware to be added to a network. It's possible to make safer IoT/IIoT devices by adding circuitry and software to the devices, although more-effective IoT/IIoT protection is usually achieved by incorporating cybersecurity circuitry and software at the network level.

Understand Cybersecurity Risks with IoT/IIoT Devices

As the number of global IoT/IIoT devices grows steadily, and in turn adds network access points with each connection, services, software, and solutions to boost cybersecurity for those devices and their networks become vital for practical internet use. Furthermore, the number of people and things seeking to take advantage of any internet-based network access points also ramps up.

The total amount of IoT and IIoT devices already exceeds the number of people in the world, with IoT activity expected to expand significantly in the coming years. Increasing IoT use signifies how fully these devices have been embraced across major industries.

IoT devices are things that can provide information about themselves or their surroundings via the internet. They use sensors, control circuits, and communications devices to interact with the internet and enable visitors to the internet to remotely use them.

Such devices ultimately become part of the internet, allowing instant access to information like rainfall in a forest, the presence of an intruder within a home or facility, or temperatures throughout a warehouse or production line. IoT and IIoT devices serve a variety of markets, including automotive, building security, government, healthcare, information technology (IT), manufacturing, retail, transportation, and utility areas.

How IoT and IIoT Devices Differ

IoT and IIoT devices differ from one another because of their typically different operating environments (see *Table 1* for salient characteristics of both categories). Often located in homes or small offices, IoT devices usually communicate data to cloud-based computers for analysis.

IIoT devices, typically located in factories and manufacturing facilities, are more likely to interact with a local server for data analysis, although that server will be connected to the internet. Because of their greater isolation, they tend to be more secure than IoT devices, although they too can benefit from cybersecurity solutions. And because of the nature of their data, such as supply-chain statistics, better security is needed for the increased capital nature of their data.

Connected IoT devices offer many benefits, including remote monitoring and control of their associated equipment. Because multiple IoT devices may be used in some applications, they're often designed to be cost-competitive. But to keep costs low, they may be limited in computing power, meaning the lack of resources for some functions, such as data encryption, needed for essential cybersecurity.

Without integrated protection, IoT and IIoT devices are vulnerable to those seeking external access to a network, such as hackers. Hackers may desire access to a network to steal its data or introduce damaging malware into that network. An IoT device may not contain harmful data, but it

can serve as an access point for cybercriminals. Thus, cybersecurity supporting these devices on any network is essential for the protection of that network and all networks it interconnects via the internet.

Assessing Safety Measures to Enhance IoT/IIoT Cybersecurity

Multiple safety measures are practiced for enhanced IoT/IIoT cybersecurity. Identification of all IoT devices authorized for a business or home network is usually a first step, followed by some form of authentication of those devices within the application software, such as by password. Carefully planning the addition of any IoT/IIoT devices to a network, rather than using automatically connected IoT/IIoT devices, such as plug-and-play components, helps maintain cybersecurity when adding IoT/IIoT devices.

Security of the IoT control software can be maintained by software patches, especially after the software is found to have flaws that can be compromised. Encrypting data handled by IoT/IIoT devices helps strengthen network security, too.

Authentication is critical when maintaining cybersecurity for any IoT/IIoT devices added to a network. Rather than a simple one-step process, greater cryptosecurity is possible via a two-factor authentication or identification process.

Any IoT device can serve as an entry point to a network if not guarded by suitable cybersecurity, and some IoT devices, e.g., routers and webcams, are difficult to secure. Smaller IoT devices, such as smartwatches, can also be security risks, making it possible to track a wearer's location. Cybercriminals will tirelessly probe any internet interconnection endpoints, such as IoT and IIoT devices, for an opening.

For those in need of an introduction to issues caused by widespread use of IoT, the IoT For All site offers a wide range of educational articles.

Key Players and Strategies in IoT and IIoT Cybersecurity

Along with identifying and authenticating as many IoT/IIoT devices on a network as possible, reasonable network cybersecurity can be achieved with edge- or cloud-based systems and software (see *Table 2* for a summary of cybersecurity vendors). For example, Alarm.com works closely with a customer and its connected IoT and IIoT devices to develop the optimum security solution.

Alarm.com's sensor-enabled IoT/IIoT solutions provide intrusion detection, video perimeter protection, and automated lock control. They also enable energy monitoring so that power and thermostat schedules can be controlled cost-effectively according to a facility's requirements.

An organization synonymous with telecommunications, AT&T, and its Business Center provides security for highly IoT-populated networks. Its product lines used licensed frequency spectrum to avoid interference from too many IoT/IIoT devices within a small area, in contrast to wireless connectivity methods such as Wi-Fi. As an example, the LTE-M/NB-IoT product line supports low-power, wide-area (LPWA) networks and provides effective cybersecurity for IoT/IIoT devices integrated into utility meters, smart homes, and wearable devices.

AT&T's Cybersecurity business unit aids the AT&T Business Center with its array of cybersecurity consulting services and network security solutions. The firm recently announced its intention to create a standalone cybersecurity services business, with funding help from WillJam Ventures, an investor from the cybersecurity industry. The new business will provide security software and consulting services while AT&T will retain an ownership stake in the new operation.

The action enables AT&T to boost enhanced network-based security capabilities without disrupting its existing Managed Security Services. Products from the new entity will enhance network-embedded security for small- and medium-sized businesses.

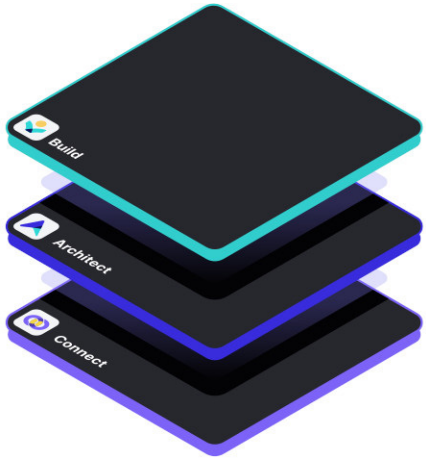
Siemens employs a risk-based, "zero-trust" approach to IoT cybersecurity *(Fig. 1)*. Its tools analyze the types of data to be processed and model responses to develop cyber controls that will protect the data.

In partnership with Siemens, Anguil has developed an

1. Device makers such as Siemens are rapidly deploying IoT/IIoT cybersecurity solutions to protect homes and businesses from cybercriminals. (Courtesy of Siemens)

IIoT-based solution for environmental pollution control. Siemens employs a risk-based approach to IoT cybersecurity tools, analyzing data and modeling responses to best protect the data. Anguil teams Siemens' Insights Hub program with their own IIoT software. The resulting IIoT platform saves data from connected IIoT devices via an Ethernet IP connection to an on-site edge computing device. Raw data is transferred from an edge device to an Insights Hub cloud platform, where it can be analyzed and used to create formatted results.

The formatted data includes graphical presentations of trends useful to engineers for equipment maintenance and making improvements in performance. Anguil is working with pilot customers to enhance and refine the IIoT platform according to feedback from those customers.



2. Running on Google Cloud, the Leverege IoT Stack is a three-layer software solution for IoT/IIoT cybersecurity. (Courtesy of Leverege)

IoT/IIoT Cybersecurity Heads to the Clouds

Another partnership, software developer Leverege and Google Cloud, has resulted in a multilayer IoT software stack from Leverege. Building upon its own BigQuery software, which analyzes IoT data for problems, Leverege developed its Leverege IoT Stack. The three-layer software stack consists of Leverege Connect for device management, Leverege Architect for data management, and Leverege Build, for creating optimized applications from the analyzed data *(Fig. 2)*. The Leverege IoT Stack, which runs natively on Google Cloud, uses artificial-intelligence (AI) and machine-learning (ML) technologies to gain the greatest benefits from data collected from millions of IoT/IIoT devices.

The Proficy Smart Factory software suite from GE Vernova protects IIoT devices in industrial and manufacturing facilities. Featuring Manufacturing Execution System (MES) software for smart factories, the software suite provides in-process quality management via IIoT control using cloud-based and on-premises software access.

A firm long associated with the Internet, Microsoft, provides IoT/IIoT software tools through its Azure cloud platform of products and services. By taking advantage of widely distributed data and tools available on cloud-connected computers, Azure can help customers to develop applications using IoT/IIoT data more quickly *(Fig. 3)*. Using cloud-based resources helps overcome challenges often associated with applications developed from IoT/IIoT data, such as fragmented data and lack of standardization. Azure applies AI and ML technologies for high-resolution analysis of captured data and identification of usable trends in the data.

Lumen offers security services to battle problems left by cybercriminals, such as malware and distributed denial of service (DDoS) attacks. A DDoS attack attempts to disrupt the traffic of an organization's server or network by creating

3. The Azure cloud-based platform of products and services works with IoT/IIoT data to develop optimum cyber-protection solutions. (Courtesy of Microsoft)

4. A system-level approach developed by Texas Instruments provides IoT/IIoT cyber protection for smart offices, factories, and cities. (Courtesy of Texas Instruments)

a flood of internet traffic, usually from multiple previously compromised computer systems. A DDoS attack is noticeable when a site becomes slow or unavailable. But Lumen's AI-based tools and services have been effective at mitigating cyberattacks, many against government users.

For many organizations and their networks, adding a large amount of IoT and IIoT devices has resulted in a splintered security perimeter. Symptoms include inconsistent communications and slow response times across the network. For a network with a large population of IoT/IIoT devices, a perimeter-based security model may not apply. For that reason, Fortinet developed an AI-powered end-to-end network security approach using what it calls zero-trust network access (ZTNA) to ensure high security at all access points.

As a self-contained solution for IoT/IIoT connectivity, emnify.com provides full, redunworldwide coverage for IoT devices using what it calls its IoT SuperNetwork. The network

TABLE 1: SALIENT CHARACTERISTICS OF IoT AND IIoT DEVICES

Aspect	IoT devices	IIoT devices
Operating Environment	Typically located in homes or small offices	Typically located in factories and manufacturing facilities
Data Analysis	Communicate data to cloud-based computers	Interact with a local server for data analysis
Security	Less secure due to cloud-based data transmission	Typically more secure due to local server interaction
Computing Power	Limited due to cost constraints	May have more computing power due to industrial usage
Data Sensitivity	Often involves less sensitive data	Often involves more sensitive data due to industrial processes
Connection Method	May use Wi-Fi or other wireless connectivity	Often connected through wired networks
Functionality	Designed for remote monitoring and control	Focuses on process control and automation
Application Areas	Commonly used in consumer electronics, home automation, etc.	Predominantly used in manufacturing, utilities, and industrial sectors
Security Concerns	Vulnerable to cyberattacks due to limited security features	Potential targets for cyberattacks due to critical infrastructure involvement

combines cellular and satellite-communications (satcom) technologies to reliably interconnect IoT and IIoT devices. The firm's low-power Global IoT SIM cards enable over-the-air (OTA) updates to adapt IoT devices to available communications methods, including 5G. The firm provides secure IoT/IIoT access via more than 540 global cellular networks in more than 180 countries in addition to satellite coverage.

For network protection from advanced threats, the CrowdStrike Falcon software from CrowdStrike is an AI-based cloud-native platform that analyzes IoT data for problems. The extended detection and response (XDR) tool incorporates an extensive high-threat library and modular program design with built-in automation to quickly adapt and respond to new threats. Based on the company's Threat Graph security analytics software engine, it automatically detects and prevents internet threats in real-time.

Texas Instruments provides a system-level approach to IoT/IIoT cyber protection. It offers IoT building blocks for all major applications, including interconnections for wired and wireless devices in smart offices and cities *(Fig. 4)*. Components include MCU, Zigbee, and power control devices (including devices for harvesting power and extending battery life), as well as hardware and software to establish gateway reference designs for enhanced protection of servers and network-interconnected devices.

When setting out to enable users to manage fleets of IoT/IIoT devices securely and as simply as possible, qbee.io considered available software development tools and decided that Go was the optimum programming language to create a dependable, efficient, and secure IoT/IIoT control platform. A complete suite of IoT protection tools from Bosch Global Software Technologies GmbH is contained in the firm's IoT Suite.

For educational purposes, it offers users faced with IoT/IIoT cybersecu-

TABLE 2: COMPANIES CONTRIBUTING TO ENHANCED IoT/IIoT CYBERSECURITY

Company	URL	Product types
Alarm.com	www.alarm.com	Smart homes, offices
Alibaba.com	www.alibaba.com	SKYLAB software
Alleantia	www.alleantia.com	IoT device drivers
Amazon Web Services	https://aws.amazon.com	End-to-end network security
Amper Technologies	www.amper.xyz	Amper FactoryOS
Armis Security	www.armis.com	IoT network protection
HPE Aruba Networking	www.arubanetworks.com	ClearPass Wi-Fi security
AT&T Business	www.business.att.com	Network security
Augury	www.augury.com	Machine monitoring
AutomationDirect	www.automationdirect.com	MQTT gateways
Axonius	www.axonius.com	Asset management software
Bosch	https://bosch-iot-suite.com	IoT Suite
Broadcom	www.broadcom.com	Industrial networking
CDW	www.cdw.com	Encryption
Cisco	www.cisco.com	IoT threat defense
CradlePoint	https://cradlepoint.com/	NCX services
CrowdStrike	www.crowdstrike.com	Network security software
Dell Technologies	www.dell.com	Network security software
Enmify	www.emnify.com	Wireless SIM cards
Entrust	www.entrust.com	Encryption
Ericsson	www.ericsson.com	AI-based network security
Fortinet	www.fortinet.com	AI-powered cybersecurity
FreePoint Technologies	www.shiftworxmes.com	ShiftWorx software
GE Digital	www.ge.com/digital	MES software
Google Cloud	https://cloud.google.com	IoT protection
Honeywell	www.honeywell.com	Industrial IoT sensors
IBM	www.ibm.com	Risk-based cybersecurity
Infineon Technologies	www.infineon.com	IoT for "green" buildings
Intel	www.intel.com	IoT platforms
Intertrust	www.intertrust.com	PKI for IoT
Karamba Security	www.karambasecurity.com	ADAS vehicle security
Leverege	www.leverege.com	IoT network security
Lumen	www.lumen.com	Endpoint threat detection
Micron Technology	www.micron.com	Memory support for Intel IoT
Microsoft	https://azure.microsoft.com	Azure IoT software suite
NXP Semiconductors	www.nxp.com	IoT security tools
Palo Alto Networks	https://www.paloaltonetworks.com/	IoT security
Portainer	www.portainer.io	IIoT container devices
qbee.com	www.qbee.com	IoT protection suite
Relayr	www.relayr.io	IoT predictive maintenance
Rockwell Automation	www.rockwellautomation.com	Industrial automation
Samsung Electronics	www.samsung.com	AI-based software
Schneider Electric	www.se.com	Software, services
Siemens	www.siemens.com	Risk-based cybersecurity
Texas Instruments	www.ti.com/iot	IoT protection devices
Telefonica	www.telefonica.com	Secure communications
Thales	www.thalesgroup.com	IoT cybersecure solutions
Trend Micro	www.trendmicro.com	VPN for homes/home offices
Trihedral	www.vtscada.com	SCADA software suite
Verizon	www.verizon.com	Network protection
Webroot	www.webroot.com	MSP program
Wi-Next	www.wi-next.com	end-to-end IoT protection

rity issues several excellent white papers including "White paper: 12 tips for successful IoT data management" and "A guide to successful IoT device management" free of charge from their website.

Trend Micro assists operators of smaller networks with software protection for IoT devices. While the company's Trend Micro Security Suite serves users of larger networks, its VPN Proxy One Pro established virtual private networks (VPNs) within homes and home offices for enhanced cybersecurity. It works with any devices, such as computers, tablets, and smartphones, as well as with all operating systems including MS Windows and macOS.

Navigating Regulations for IoT/IIoT Security

The importance of IoT/IIoT cybersecurity is apparent from attention given to it by government organizations. The U.S. Food and Drug Administration maintains a page on cybersecurity and how it relates to various IoT devices, in particular medical equipment. The organization provides recommendations on medical-device cybersecurity in its "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" guidance.

In addition, the National Institute of Science and Technology (NIST) provides multiple publications with guidance on IoT security, including government agencies and businesses. NIST's studies, which consider different device types and network architectures, emphasize that IoT/IIoT devices are now a permanent part of life and achieving security for them is an essential part of sustaining life.