UNDERSTANDING THE IoT EXPLOSION AND ITS IMPACT ON ENTERPRISE SECURITY

Enterprises and government agencies are embracing a digital transformation that is reinventing business models to better serve customers and drive new growth. The rapid adoption of new technologies and innovations is driving a global rethinking of traditional business processes and creating new ways to generate better business outcomes and quality-of-life improvements. This is being called the Fourth Industrial Revolution—a period of explosive productivity improvements driven by innovation, and the combination of technologies that unlock new business models.

In Industry 4.0, industrial processes and associated machines become smarter and more modular, while new protocol standards, like UPC UA (Open Platform Communications Unified Architecture), allow previously isolated control equipment to communicate with each other, enabling a hyperconnected network across multiple industrial ecosystems. All this is driving higher levels of utilization and greater flexibility for meeting customer demand.

The Internet of Things (IoT), cloud computing, and ubiquitous broadband are the key technologies enabling this digital transformation. Smart, always-connected things with instant access to contextual information, as well as devices and applications with artificial intelligence designed to optimize processes and improve how we live, work, and interact with each other, are all changing the way we conceive, produce, deliver, and consume goods and services.

Industry 4.0 will drive huge disruptive changes on both the demand and supply side, as consumers and corporations apply greater influence and purchasing power to an expanded array of suppliers. Greater integration of business processes means accelerated decision-making and the need to keep pace with rapid market changes. Enterprises are increasingly seeking faster productivity improvements to avoid losing relevance as new competitors emerge. The global rise of Uber as a leader in transportation and the associated disruption of traditional taxi services are examples of how DX can radically reshape markets.

THE IoT SECURITY CHALLENGE

IoT is a game changer for security. Everything is moving faster than we thought, and many security vendors are not prepared. Because of the ubiquitous interconnectivity between devices, users, and distributed networks, something now being referred to as an ecosystem, traditionally siloed security devices defending a single place in the network are increasingly ineffective. Even worse for most IT teams, many traditional security standards and best practices are not as effective in addressing IoT challenges.

And from a security perspective, IoT manufacturers aren't helping. The practical reality is that most IoT devices are not designed with security in mind. In fact, most IoT devices are headless, meaning they don't have a traditional operating system or even the memory and processing power necessary to build in security or install a security client.

25%

of attacks on enterprises will be targeted at IoT

THE EXPLOSION OF IoT DATA

Over a million new IoT devices are being connected to the Internet daily, and that process is accelerating. Experts predict that as many as 25 to 50 billion new IP-enabled IoT devices will be deployed and online by 2020. As a result, IoT has created an explosion of data that is designed to move freely between devices and locations, and across network environments, remote offices, mobile workers, and public cloud environments, making it difficult to consistently track and secure.

Traditional global data center traffic is currently measured in the zettabytes, and is predicted to more than triple to 15.3 ZB annually by 2020. However, according to Forbes, the total volume of data generated by IoT will reach 600 ZB per year by 2020, which is 275 times higher than projected traffic going from data centers to end users and devices (2.2 ZB), and 39 times higher than total projected data center traffic (15.3 ZB.) The resulting wave of structured and unstructured data will challenge the ability of even the largest security teams to identify anomalous behavior across the global ecosystems of smart enterprises and cities.

These changes have already begun to tax saturated access points, networks, and data centers, not to mention overburdened IT staff. And cybercriminals, always seeking to exploit the weakest link in the data chain, have begun to take notice. So by 2020 it is also predicted that over 25% of attacks on enterprises will be targeted at IoT.

And as we saw in two recent massive IoT-based attacks, these devices are vulnerable to being collected and weaponized to deliver DDoS attacks. They are also vulnerable to such things as targeted code injection, physically altering their firmware, man-in-the-middle attacks, remotely controlling devices to alter or disable their functionality, spoofing other IoT devices, or simply hiding more traditional malware in the volume of IoT data.

In addition, organizations are now converging previously parallel networks, including IT, OT, and IoT, in order to leverage real-time data and information, which allows them to be more responsive to customer needs. But traditional security models have a difficult time providing needed protections as computing and data move back and forth between edge devices and the cloud. This confluence of distributed networking, computing, and security is driving the consolidation of point defense devices to platforms that can automate the sharing of threat intelligence, collaboration to detect and isolate threats, as well as the real-time orchestration of incident response.

IoT TRENDS

Most of us only have a passing familiarity with IoT. When asked, most of us think of smart appliances and connected cars providing users with related information. But that is only the most visible surface of IoT. Beyond the traditional Internet connecting people via networks, expanding networks of billions of connected devices are collecting and sharing data to make semi-autonomous and autonomous decisions. These automated decisions and microtransactions across the digital economy are beginning to unlock the new productivity and growth that are hallmarks of Industry 4.0. IoT and the associated confluence of highly distributed networking, computing, and security is rapidly connecting every facet of our lives and changing the ways we communicate, conduct commerce, and play. Following is a brief overview of several emerging trends around IoT, as well as their potential risks from a security perspective.

DATA ANALYTICS

The big payoff for IoT for enterprises comes in the form of real-time information and data analytics driving enhanced decision-making capabilities. Enhanced productivity and new market opportunities will drive highly disruptive growth for enterprises and government agencies, which can effectively harness the power of their data. But that data in its raw form is not very useful. That is why, according to ABI Research, businesses will spend more than 26% of their entire IoT solution cost on technologies and services that store, integrate, visualize, and analyze IoT data by 2020, which is nearly twice what is being spent today.

One of the emerging high-demand jobs will be for data scientists who can build algorithms to parse through and analyze that data for critical information. Based on that same research data, the currently very manual nature of data scientist activities means that the cost for professional analysis is expected to represent over one-third of enterprise IoT data and analytics spend through 2021.

It is pretty easy to predict that the next big breakthrough in IoT will be automation of many of the more manual activities related to analytics. The efficiencies that automation can provide to data scientists will enable more and more difficult problems to be solved, and employees and business units will be better able to use analytics data to increase productivity and efficiency. Analytics automation will also enable innovative companies to break away from their competitors, as it lowers their total cost of analytics while raising the bar on more responsive, best-in-class offerings and services.

Of course, analytics automation requires a platform that can easily ingest new data, make adjustments to analytics models in real time, and even automate prescriptive analytics. These solutions will initially be very expensive, and due to their proprietary nature and the growing gap in the availability of competent data scientists, these processes and data will naturally become a high-value target for cybercriminals and industrial espionage.

APPLICATION ENABLEMENT PLATFORMS

Application enablement platforms (AEPs) were created to simplify the extraction of data from devices and machines, transmit that data efficiently over a network, and convert it into a form that is easily consumable by an IoT application. That application can then use that information to do such things as maintain just-in-time inventories, reset priorities on the manufacturing floor, or provide critical updates to data consumers. As a result, many of these AEPs are converging traditionally distinct networks of OT and IT. The security implications are significant.

OT networks are often more vulnerable than IT networks. They often use proprietary and legacy operating systems and devices that may have never been designed to be IP-enabled and that can sometimes be broken simply by scanning the devices, let alone targeting them with malware. And while it is one thing to hack a website or steal data, shutting down an active manufacturing floor can be devastating to a business. Attacks in the last few years that caused the destruction of industrial furnaces, centrifuges, and computers are harbingers of what can happen.

THING IDENTITY AND MANAGEMENT

As the number of IoT devices grows, it is inevitable that organizations will want things to participate in multiple ecosystems, interact with other things, and be accessible to new services. We are already seeing IoT device and services suppliers in smart home, connected car, entertainment, and mobile healthcare markets beginning to cross-connect their devices and services.

Critical to facilitating these opportunities is thing identity. Thing identity facilitates the creation of thing management services and can expand the opportunities available through cross-AEP analytics.

Given that many simple IoT devices are difficult or impossible to secure, thing identity and authentication is the front line for IoT security. Security solutions need to be able to identify and analyze things connecting to the network, and at wire speed. They then need to determine what

rules apply to these things and dynamically route them to their appropriate protected network segments. This information needs to be shared across the security fabric so that associated policies can be enforced anywhere across the distributed ecosystem, anomalous behaviors can be quickly detected and thwarted, and changes in policy can be immediately enforced regardless of the location of an IoT device or its data.

EDGE COMPUTING

Traditionally, IoT data is collected by a remote sensor and sent back to a cloud environment, where it is either stored or acted upon using business rules or sophisticated analytics. Deep analysis of this IoT data is used to create new products and services, as well as perform predictive and prescriptive analytics.

However, market forces increasingly demand that computing be done where the device is located rather than make a round trip to the central data center. Edge computing helps limit the amount of data transmitted back to the cloud, which also reduces connectivity costs over metered networks, along with data storage, analysis, and integration costs. Given the nature of some applications, such as automatic braking in smart cars to avoid a collision, edge computing is necessary because the application cannot wait for analysis and response from the cloud.

In addition, the high volume of data that comes from sensors and smart devices will quickly overwhelm networks and data centers if all the data processing needs to be done centrally. Sensors and other smart devices generate vast numbers of small data packets that are not always best handled by simply flooding the data center with them.

Likewise, traditional data models—for which many legacy security solutions were designed—require information to be created in the data center and then pushed to the edge for consumption by employees and customers. However, as IoT devices and sensors begin to provide analysis at the edge, they are fundamentally changing the polarity of data so that the creation and consumption of data will become more balanced between the edge and data centers.

These edge devices will aggregate data, make autonomous or semi-autonomous decisions, and only then will they sometimes send that data back to the cloud for further analysis, which may result in cyber instructions being sent back to the IoT device or devices. As a result, it is expected that edge analytics will generate almost as much data as the data center.

Here are a couple of examples of the advantages that edge computing can provide through IoT:

Driverless cars will be tied bidirectionally to GPS, weather, and traffic systems, along with a meshed network of other connected cars. This will allow them to make split-second decisions locally, say avoiding a pothole, and then share that information in real time so that other cars are prepared to avoid that same road hazard and municipalities can schedule an emergency road repair.

Smart cities will look to dynamically optimize and shuffle energy and other resources, such as traffic patterns and parking spaces. Data collection and analytics will be able to determine such things as if turning on the streetlights earlier in the evening will reduce the crime rate in a section of the city, or if shortening or lengthening the available time on parking meters during the day will generate more foot traffic and thereby increase shopping revenue for downtown retailers.

This change in data collection, processing, decision-making, and analysis also greatly expands the potential attack surface. Connected smart devices can potentially download or spread malware that can do such things as affect city traffic, disrupt critical infrastructure, or put auto passengers at risk. Likewise, distributed ransomware could potentially shut down critical infrastructure or lock out people from things like cars and medical devices.

Addressing this challenge will require a partnership between security companies, telcos, and service providers because IoT is going to need to operate across the entire ecosystem of deployed networks, including Wi-Fi, wireless, LANs, metro WANs, and satellites.

LPWA AND LORA TECHNOLOGIES

Low-power wide-area (LPWA) and long-range (LoRa) technologies are the latest in a portfolio of connectivity technologies that includes cellular, short-range wireless, satellite, and fixed-line connections. LoRa standards have recently been established, and standardized LPWA technologies are slated to start becoming generally available during 2017.

Besides opportunities in established markets such as smart metering, smart home, and commercial building automation, LPWA and LoRa technologies make IoT solutions affordable for the nascent markets of asset tracking, agriculture, and environmental monitoring. These solutions provide long-range connectivity of greater than 15 km, high capacity that can currently support up to 1 million nodes, over 10 years of battery life, and reduced synchronization overhead with no hops in the meshed ecosystem.

These solutions are also enabling new ideas such as the emerging sharing economy, where personal assets can be shared by communities or loaned to individuals for a fee. In sharing economies, anything from lawn mowers and garden tillers to surfboards and bicycles to tools and musical instruments can be tracked and monitored using LPWA technologies for much less cost than with existing wireless technologies.

The risks can range from the simple, such as locating and disabling connected devices, to determining where valuable assets are located, to quickly injecting and spreading malware across these networks of connected devices, to weaponizing these assets for such things as DDoS attacks.

MANAGING RISK

Another challenge many organizations face is security sprawl. Dozens of isolated devices with separate management interfaces have placed a strain on limited IT resources. Over the last few years, CISOs have been focused on consolidating their security resources, moving from devices to platforms, and they have actually reduced the number of security devices deployed

at large enterprises from around 70 to about 30. But with the advent of cloud and IoT, and the specialized security tools being created and promoted for these environments, we are about to start to once again expand the number of deployed hardware-based and virtual security devices.

For cybersecurity to be effective, organizations have to protect things that have already been deployed, things that are now being deployed, and things that have not yet been deployed in scenarios that they haven't even thought of yet. And today they usually need to be able to detect and respond to advanced threats in less than 10 minutes before irreparable harm is done. And that time frame is getting smaller every day.

Organizations need to understand their risk profile—what level of risk they can absorb and what level they should transfer to MSSPs or cyber insurance providers. As the number of high-profile data breaches increases, and boards become more aware of their financial liability, cybersecurity has become a risk-management exercise. CISOs are focused on managing the risks associated with their shifting business goals, measuring the risk associated with the devices, services, and protocols they need to implement in order to meet those goals, articulating their tolerance for risk, and then putting a plan in place to mitigate that risk.

Finally, to effectively compete in the new digital economy, organizations need to be able to tie together what is happening in their IT network, their operations network, their IoT network, and in their public and private cloud networks in an automated fashion. Security needs to have visibility across this ecosystem of networks, collect and correlate threat intelligence, and automatically orchestrate a response to stop threats anywhere across the ecosystem attack path.

Beginning in the late 1990s, we approached security with a prevention strategy—building walls and moats around networks to keep the bad actors out and to protect information. As threats became more sophisticated and adept at breaching perimeters, we met each new challenge with incremental improvements—moving from network security to information security to data security. Today we know that even the best defenses can't stop determined advanced threats and attack campaigns. The number of high-profile breaches is evidence that prevention, while important, is simply not enough. Cybersecurity is a multidimensional operating domain. Indeed, for the U.S. Department of Defense and NATO, cyber is the newest operating domain after air, land, and sea.

Cybersecurity encompasses the traditional three security pillars: confidentiality, integrity, and availability. But it now must go beyond these requirements to also address the physical environment and health and safety issues. The addition of IoT to our networks requires that we address things like physical safety, business continuity, and disaster recovery for such things as driverless or smart cars, connected HVAC systems, online medical devices such as pacemakers and infusion pumps, or interconnected city networks.

Cybersecurity requirements span five key areas:

- *Identification—understanding risk profile and current state*
- *Protection—applying prevention strategies to mitigate vulnerabilities and threats*
- *Detection—detecting anomalies and events*
- *Response—incident response, mitigation, and improvements*
- *Recovery—continuous life cycle improvement*

A SECURITY FABRIC

While many of the security challenges surrounding digital transformation and the adoption of IoT and cloud are new, they can be managed through a combination of proven best practices and a better security framework. Central to securing these new, highly distributed ecosystems are high-speed authentication and monitoring; internal segmentation designed to monitor and protect distributed computing and distributed networking and to enforce and coordinate distributed security; and cloud-based security services that can track and defend devices and data distributed anywhere across the network of networks. Security needs to tie together the entire distributed network and connect IoT devices and data to the edge, across the core and the data center, and out to the cloud.

Securing IoT and digital transformation will require automated visibility from the data center to the cloud and IoT, combined with advanced detection capabilities, powered by the threat intelligence enabling orchestration of responses to mitigate threats at machine speed. What is required is a distributed and integrated, fabric-based approach to security that can cover the entire networked ecosystem, expand and ensure resilience, and secure compute resources, including routing and WAN optimization, to ensure that you are securely connecting that IoT device to the appropriate cloud environment. This approach enables organizations to effectively monitor legitimate traffic, check authentication and credentialing, and impose access management across the distributed environment through an integrated, synchronized, and automated security architecture.

Copyright © 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Feb 09, 2017