FORTINET

THE CRITICAL ELEMENTS OF AN IoT SECURITY SOLUTION

WHITE PAPER

The Internet of Things (IoT) is revolutionizing the way the world works and plays. In our pockets, on our desktops, and even on the walls of our homes and offices, IoT devices capture and transmit the details of our location, spending habits, and the very environment in which they operate. IoT is an enabler of a larger digital transformation that will produce vast quantities of data to be stored, parsed, and transmitted over an ever-expanding global network. This treasure trove of data will feed artificial intelligence platforms and data analytics applications and will impact nearly every aspect of our daily lives.

But IoT is not without its risks and downsides, and concerns over IoT security are only growing. A recent survey of attendees at the Black Hat USA 2017 conference conducted by UBM ranked digital attacks on non-computer devices and systems as the No. 1 greatest concern two years from now. In fact, we've already seen major outages, including the widely reported attack on the DNS provider Dyn where attackers used a botnet and employed IP cameras, printers, and perhaps even baby monitors to disrupt the services of global web brands. In addition to commercial impact, the risks of IoT-related service disruptions extend to the critical infrastructure in our communities. Imagine the implications of an attack on the switching infrastructure of a metro subway line, a wireless pacemaker becoming compromised, or a power grid shutting down. Lives would be at risk. Security professionals must be prepared to define solution requirements thoughtfully to guard against these new threats. A new solution approach must account for the fact that these devices, now part of a blurring network edge, were not designed with security in mind, and as such, are directly in the cross hairs of would-be attackers.

With this as the backdrop, how should security professionals assess the IoT threat landscape and define a solution that is both comprehensive enough to meet these challenges and flexible enough to grow into the future? To answer this requires that we first understand what we are protecting against in IoT security and how these devices create unique vulnerabilities

DEFINING THE IoT THREAT LANDSCAPE AND SOLUTION REQUIREMENTS

IoT expands the threat landscape and attack surface. Beyond simply the dangers of leveraging network endpoints without control over security measures, IoT presents four fundamental risks security professionals must be mindful of in developing a security approach and defining solution requirements:

Vulnerabilities—IoT devices are often not designed or deployed with security in mind. Some are even considered "headless," without the ability to run security protocols or be updated. Companies never envisioned a printer or a thermostat being involved in a botnet attack. But it has already happened. Also, even devices where security was considered can't easily be identified or updated in the field to address new threats. *How will you deploy a solution to identify, categorize, and manage*
new devices?

Unsecure Communications—Devices leveraging public networks often communicate without encryption and send data on unprotected networks. Traffic is unmonitored, unmanaged, and unprotected. Public Wi-Fi and new approaches that leverage Bluetooth are of particular concern. *Are you defining your IoT security requirements with access exposures in mind like public Wi-Fi?*

Data Leaks—IoT devices represent an unmonitored and unmanaged entrance and exit point to the network. As such, policies set to prevent data leaks may fail to flag data passing through these devices. Devices must be brought into the larger network fold for policies to be enforced. *How will your solution apply and enforce policies to devices that may not be in your control?*

Malware Infections—Unsecured devices may ship with or proliferate malware. Once on the network, malware spreads from device to device. *Will you be able to segment critical resources on the network so they only access devices they are meant to access?*

DEFINING YOUR REQUIREMENTS

- √ How will you deploy a solution to identify, categorize, and manage new devices?
- √ Are you defining your IoT security requirements with access exposures in mind like public Wi-Fi?
- √ How will your solution apply and enforce policies to devices that may not be in your control?
- √ Will you be able to segment critical resources on the network so they only access devices they are meant to access?

Answering these threat questions will provide a starting point for security professionals to define the requirements of an IoT security solution. Transforming the IoT frontier into a hardened perimeter or at least gaining the visibility to see threats coming and be able to react to and prevent an attack is the baseline for any new solution.

CRITICAL ELEMENTS OF THE IoT SECURITY SOLUTION

To manage risk, security professionals must exert a degree of control over IoT infrastructure or, at the very least, its communication with the network. Three strategic areas must be addressed when developing solution requirements to minimize these threats: Learning, Segmentation, and Protection.

LEARNING

In the age of IoT, it may very well be that the network perimeter cannot be defined. For the secure enterprise, however, visibility is everything. This may be as simple as seeing a new employee's laptop power on and loading the appropriate security patches automatically. It might mean auto configuring access to a software program with a credential-based user policy. The critical piece is that the network must be aware of devices communicating on the network and be smart enough to know how to classify and learn how best to secure them. Without the capability to learn about devices, intelligent threat protection is impossible. When evaluating a solution, look for functionality in two key areas:

Device Identification and Discovery—If you are like most organizations, a full view of every device on the network from a single dashboard is elusive. And the moment that snapshot is complete, it often changes. A solution must be able to automatically detect, profile, and classify what's on the network and develop a comprehensive inventory of devices. Once detected and profiled, security teams will be able to answer questions such as: What's the OS and how is it configured? Is the device managed? Is it trusted or rogue? Once discovered and visible, the proper policies can be applied.

Predictive Action—The next challenge is to learn behaviors and predictively react to an attack before it happens. For example, by classifying a device in terms of three categories—Managed Devices (the devices you control), Allowed Devices (the ones you accept but don't control), and Rogue Devices (suspicious devices not in policy compliance)—the fabric can learn the normal baseline activity for each category. This also helps in assigning a risk score to a device for segmentation and policy purposes. Once the normal behavior is known for these categories, the fabric can monitor for anomalies that will be more easily recognizable, whether it's a policy violation, unusual traffic for the time of day, or systems communicating that don't usually need to. Only with visibility at the macro level, across all categories of device, can an intelligent fabric learn to adapt and take action, becoming more predictive over time.

STRATEGIC AREAS TO ADDRESS

LEARN

- √ Device Identification and Discovery
- √ Predictive Action

SEGMENT

- √ Identifying Risk
- √ Managing Policies and Devices
- √ Exerting Control

PROTECT

- √ Policy Flexibility and Enforcement
- √ Threat Intelligence

SEGMENTATION

Segmenting the network and devices is about assigning policies and managing risk. When countermeasures fail in a more vulnerable or less critical part of the network, segmentation also protects more critical areas from being compromised. When defining solution requirements, security professionals must have the ability to manage policies, gain insight, and see trends based on risk profiles and type of infrastructure. Consider functionality in three areas when defining requirements for segmentation:

Identifying Risk— The first order in segmentation is classification. Users, data, devices, locations, and a host of other criteria must be used to identify categories and assess risk. Systems that hold customer or financial data, for example, should be grouped with the network resources that directly access those systems.

Managing Policies and Devices— As the network fabric expands, new devices must be not only discovered but configured based on existing device policies. A solution must provide the granularity to see all device activity and set policies appropriately. The fabric should know that when a new switch goes live, it will automatically inherit predetermined security policies. Networks grow too fast for this to be a manual process. A solution must have the flexibility to set policies by type of device or by users, traffic type, or perhaps even traffic by location or time of day. Policies should be the vehicle by which security professionals manage risk across the network.

Exerting Control— Once an intruder gains access, an attacker could roam the network for weeks before acting. Segmenting the network, for example, isolating IoT devices and the other devices, servers, and ports they communicate with, allows the organization to separate resources on a risk basis. Choosing to treat parts of the network that interact with IoT devices differently from a policy standpoint allows the organization to control risk.

This type of solution can secure critical network zones and grant IoT devices privileges, based on their risk profile, without compromising other segments of the network.

PROTECTION

The mission in IoT security is to first protect the device, then protect the network. Once an IoT device is secured and becomes part of the network, it must be protected in a coordinated fashion with all other network elements. Protection in the IoT realm becomes a matter of policy enforcement. When considering an IoT security solution, focus on one that can flexibly apply policy and enforce policy with automation across the following areas:

Policy Flexibility and Enforcement— A flexible solution will have the ability to define and enforce policies on multiple levels across both type of device and access. To meet the challenges of IoT, rules must be enforced governing device behavior, what kind of traffic a device is allowed to generate, where it can be on the network, and even whether it can be on the network at all. BYOD, social media applications, and cloud-based applications are all examples where different policies must be established and enforced.

Threat Intelligence— Once controls are established, a solution must be able to consistently enforce policies and translate compliance information across the network to all devices to create an intelligent fabric capable of learning and responding to threats. A solution where this intelligence is distributed throughout the security fabric ensures that the actions taken will be as close to the threat as possible. Even further, this threat intelligence should be capable of soliciting information from sources globally, including from other vendors, to identify threats before they happen and connect the dots with trending and threat information from inside the network.

For a comprehensive solution, IoT devices must be subject to the same multilayered monitoring, inspection, and enforcement policies as the rest of the devices on a distributed network. Only then can all parts of the network communicate with each other to share policy information and threat intelligence and protect application data.

THE EVOLUTION OF SECURITY—A FABRIC-BASED APPROACH

To meet these requirements, an intelligent fabric-based solution is required. It must be broad enough to guard the entire network, powerful enough to provide threat protection without an impact to performance, and deliver high levels of automation.

Current security approaches today rely too heavily on point solutions that guard their area of the wall but don't communicate or share information. Without the breadth of visibility across the network, including application security, cloud security, network security, access security, and of course client and IoT security, there is no holistic view of threats in real time. Attackers will exploit the lack of a broad and holistic view.

The performance delivered by a solution must not only deliver the required functionality but do so without inhibiting access or other network function. As users move to adopt applications like the cloud, big data, and others that demand an ever-increasing volume of information, firms will be upgrading networks to their core to 100 Gbps and considering migrations to IPv6. These moves will rapidly expand the volume of data on the network and introduce requirements to process new protocols without adding latency. This requires a security solution that not only meets performance requirements but enhances performance with dedicated processing. This dedicated processing power is required to accelerate increasing volumes of network traffic, properly inspect the content, and optimize overall performance. Without it, users on the network will see a security performance penalty, causing a loss of focus on protection of the network or driving users to bypass security procedures, exposing the enterprise.

Lastly, the complexity of the modern network and threat landscape demands that functions be automated. This would include activities such as the basic provisioning of new devices and policy configuration, all the way through to response. Combatting today's threats requires automation that can tap into both global and local sources of threat intelligence, coordinate a response to those threats, and continually learn, audit, and recommend changes on the network to improve protection.

CONCLUSIONS

IoT will cause a sea change in the way businesses leverage data to make decisions, and in the way we manage our personal lives. This change will also require a rewriting of the network security playbook. When defining the requirements for an IoT security solution, firms must consider an approach anchored with an intelligent, network-wide security fabric that can learn and share information.

This new approach must accept that when there is no clear delineation between the network and the outside world, everything that touches the network must be visible. We must assume that all devices at the edge and the core are vulnerable, regardless of how effective we view our perimeter defenses. We must understand that when threats can come from any direction or any source, only an approach that allows us to see everything, segment based on risk, and teach the network to defend itself through intelligence and automation will help us to successfully navigate the waters of IoT security.

With this IoT security solution requirements primer as a guide, IT security professionals can demand solutions that look at security holistically, recognizing that IoT devices, like all other elements of the network, must be visible, segmented, and protected.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

105727-B-0-EN August 10, 2017 8:29 AM

Macintosh HD:Users:mbunnell:Documents:Egnyte:Shared:CREATIVE SERVICES:Team:Michael-Bunnell:WP-Critical-Elements-IoT-Solution:wp-critical-elements-IoT-solution