EMPOWER AND PROTECT YOUR ORGANIZATION WITH AN END-TO-END APPROACH TO IOT SECURITY

vmware

Pulse™

Table of Contents

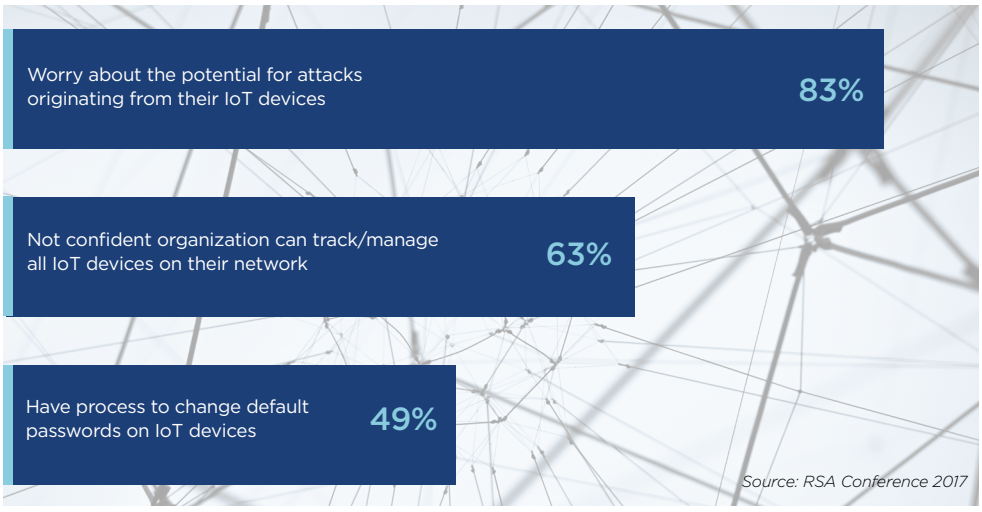
Addressing the security challenges of the Internet of Things (IoT) is one of the most important technology initiatives organizations must tackle in 2018. IoT usage is expanding exponentially—and with good reason. The IoT enables organizations to achieve new levels of insight, productivity, customer responsiveness and innovation. McKinsey predicts the annual economic impact of the IoT could exceed $11 trillion by 2025, an amount larger than the combined GDP of England, France and Germany today.[1]

IoT Has Increased the Surface Area of Attacks

For organizations to tap into the IoT's vast potential they must put comprehensive security protections in place and they must do so quickly. The risks are simply too great. According to a recent study by consulting firm Altman Vilandrie & Co., nearly half of U.S. firms using an IoT network have been hit by security breaches.[2]

We've already seen how devastating IoT attacks can be. The 2016 Mirai attack used IoT devices to attack the Internet infrastructure, resulting in an estimated $110 million in economic damage.[3] Check Point has warned about a massive botnet that is recruiting IoT devices to "create a cyber storm that could take down the Internet."[4]

Organizations Are Worried



1 "Security in The Internet of Things," McKinsey Global Institute, May 2017
2 "Study: 48% of firms using IoT hit by security breaches," Enterprise IoT Insights, June 2, 2017
3 "Security in The Internet of Things," McKinsey Global Institute, May 2017
4 "A New IoT Botnet Storm is Coming," Check Point Research, Oct. 19, 2017

IT and business leaders are increasingly aware of the existential threat that security poses to achieving the IoT's potential. More than 80% of IT professionals say they are worried about attacks originating in IoT devices.[5] Approximately 49% of global technology enterprise security decision-makers expect their organizations to increase spending on IoT security in 2018. And, while 92% of these leaders say they have policies for managing IoT devices, more than 50% say they don't have sufficient tools in place to enforce those policies.[6]

How should your organization move forward? How can you eliminate security gaps to enable secure deployment of IoT devices? How can you avoid risk and empower your organization to drive innovation and competitive advantage through secure IoT deployments?

The answer is to employ a comprehensive, end-to-end approach with security designed in from the beginning. This white paper describes why an end-to-end model is necessary and discusses the features and functions that should be incorporated in your solution. We also provide guidance on how to go about deploying an end-to-end model, with an overview of specific solutions that enable you to maximize protection and minimize risk.

Why Is IoT Security So Hard?

One of the first steps is to recognize that the IoT has characteristics that require new approaches to security. Simply using existing tools, technologies and methodologies won't provide the protections you need. However, it is also important to understand that the IoT is part of your corporate network and thus is subject to the same scrutiny and policies as other connected devices.

Characteristics unique to the IoT include:

5 "Survey Shows Most Organizations Cannot Manage All IoT Devices on Their Networks," IoT Journal, April 20, 2017
6 "47% of Businesses Say They Have the Tools to Support IoT Security Policies," Forrester, Jan. 9, 2018

- **Limited capabilities:** To be effective, IoT devices need to be low cost so they can be deployed in large numbers. They need to operate for years on a small battery. Both of these requirements constrain the ability to include sufficient processing resources for compute-intensive tasks such as encryption. Many devices are mass produced at minimal cost, with no thought given to protecting them from attack.
- **Lack of human control:** Embedded devices are typically headless, which means there is no human operator to input authorization credentials or decide which applications should be trusted, and which shouldn't. Thus, in the IoT world, authentication and identity differ fundamentally from the Internet of people, (PC or mobile) world. It's no longer about user identity, it's about machine identity.
- **Scale:** The sheer numbers of IoT devices is staggering. Gartner predicts there will be more than 20 billion connected devices by 2020.[7] Most of those devices need ongoing patching and upgrading, which must be delivered and authenticated without impacting the performance, security or availability of the device.
- **Complexity and heterogeneity:** It's not just that there will be 20 billion devices, it's that these devices will be of a wide range of functions, capabilities and standards. This cornucopia of non-traditional computers, non-standard devices and a variety of compute power capabilities makes for a very challenging and complex environment to secure, control and manage.

7 "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," Gartner, Feb. 7, 2017

Best Practices in IoT Security

The combination of factors described above means that many approaches to securing an IoT network must rely on technologies outside the devices themselves. For example, networks can be micro-segmented, so a device can communicate only with its assigned destination/applications. Device and network behavior can be analyzed to detect abnormalities that could be the result of compromise.

The key is to look at the IoT holistically and to build in security from the beginning and at every subsequent stage of its development. As noted by McKinsey: "By nature, a complex system of connected devices opens many new attack vectors, even if each device is secure when used independently. Since a system's most vulnerable point determines its overall security level, a comprehensive end-to-end approach is required to secure it."[8]

How do you get there from here? Start with putting your entire IoT portfolio under a unified management umbrella that deploys best practices in IoT management and security. Best practices in IoT security comprise these critical elements:

- **Least Privilege Applied Consistently:** Devices should be allowed only the minimum access needed to perform their job and nothing more. System components should be allowed only the minimum function needed to perform their purpose and nothing more.
- **Micro-Segmentation:** The IoT traffic should be segmented into specific flows to make it more manageable. This contains the damage if one part gets compromised.
- **Three-Tier Architecture:** A three-tier IoT technology stack consists of sensor devices, gateways and the IoT data center or cloud platform. This model limits the attack surface to the link between the gateway and the device, which is typically very small and local.
- **Active Threat Detection:** The threat environment is constantly evolving, so you need to be on top of it at all times. Your end-to-end IoT infrastructure should incorporate continually updated security analytics and threat detection to monitor compute and networking patterns for abnormalities.
- **End-to-end Trust Model:** This includes trusted boot; device root of trust; authentication and secure connections; signed patches; encryption in transport and at rest, and multi-factor authentication.
- **Secure Patching:** This includes reliable and timely over-the-air real-time software patches and firmware updates to devices and gateways, no matter how remote the location. History shows time and again that it is a matter of time before vulnerabilities are discovered.

8 "Security in The Internet of Things," McKinsey Global Institute, May 2017

Choosing the Right IoT Management Solution

Given the importance of the IoT and the inherent challenges in achieving enterprise-grade deployment, management and security capabilities, your solutions should include centralized management with comprehensive oversight and built-in security features and functionality. The management platform should give you complete control and visibility into all aspects of the IoT system from the edge to the cloud. You should be able to onboard, manage, monitor and secure all things and infrastructure for IoT from a single pane of glass.

When it comes to delivering best practices in secure IoT management, VMware Pulse IoT Center is a clear industry leader. Built-in security capabilities include:

VMware Pulse IoT Center delivers these security capabilities in a turnkey enterprise-grade end-to-end IoT infrastructure management solution. Organizations can manage, monitor and secure heterogeneous connected things and gateways with different hardware, operating systems and communications protocols. In addition, VMware Pulse IoT Center empowers IT and operations teams to deploy and scale IoT infrastructure quickly and easily, with visibility and control over connected devices at all times.

NETWORK SECURITY, including SSL certification encryption for server-to-server and client-to-server network communication. Also, active, real-time threat detection in partnership with third-party solutions.

SECURE ONBOARDING, with asset discovery, profiling and tracking. Each gateway is enrolled using a unique username/password and a pre-assigned passphrase is used to decrypt the enrollment staging package.

AUTOMATED OVER-THE-AIR SOFTWARE UPDATES, including content delivery of IoT apps, firmware or software patches and updates, leveraging over-the-air secure channels.

AUTHENTICATION AND AUTHORIZATION: Each gateway uses authorized Access Control Lists for ongoing communication with the server to reduce spoofing.

THREAT CONTAINMENT, with enterprise wipe to protect data from a compromised gateway or edge system.

Conclusion

The potential of the IoT is staggering. It is often described as the foundation for the next industrial revolution.9 But that potential will only be reached if organizations have confidence they can build secure IoT infrastructures and interactions. Each organization has a responsibility -- and an opportunity -- to build in security protections from the ground up, leveraging best practices and unified centralized management.

VMware has incorporated more than three years of IoT security R&D in developing the features and capabilities of VMware Pulse IoT Center. With VMware Pulse IoT Center, IT and operations teams can unify and centralize IoT management, monitoring and security to accelerate their deployments to drive innovation and competitive differentiation.

To learn how you can empower and protect your organization with an end-to-end approach to IoT security, please visit VMware at https://www.vmware.com/products/pulse.html or email IoT@vmware.com.

9 "The Internet of Things Will Power the Fourth Industrial Revolution. Here's How," World Economic Forum, June 24, 2017

vmware

Email us at IoT@vmware.com for more information.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMWARE_TT_WP3_0318_ED

3/18