# INTERNET OF THINGS: HOW TO SECURE THIS GROWING GATEWAY TO CYBER EXPLOITATION

## INTRODUCTION

For most organizations, the Internet of Things (IoT) suggests connections to consumer products such as Nest Cameras, Amazon Echos, Fitbits, and Smart Lightbulbs. However, the Internet of Things in enterprise and industrial environments is rapidly growing in importance as a security concern.

***The number of IoT devices is estimated to grow from 15 billion in 2015 to 200 billion by 2020.*** [1]

That's because the number of IoT devices is estimated to grow from 15 billion in 2015 to 200 billion by 2020, based on projections by tech giant Intel Corp., market researcher IDC, and the United Nations. [1] While not all IoT devices have an actual password, they need an authentication method and are likely to store a key or password within the configuration that connects them to a network.

Industrial Controls Systems (ICS) are especially tied to the Internet of Things. Power stations, energy grids, water treatment and cargo ships, for example, are all typically connected to other systems and networks, as well as the cloud. These connections enable control from remote locations and the performance of big data analysis using sensors and monitors that transmit data to a central location.

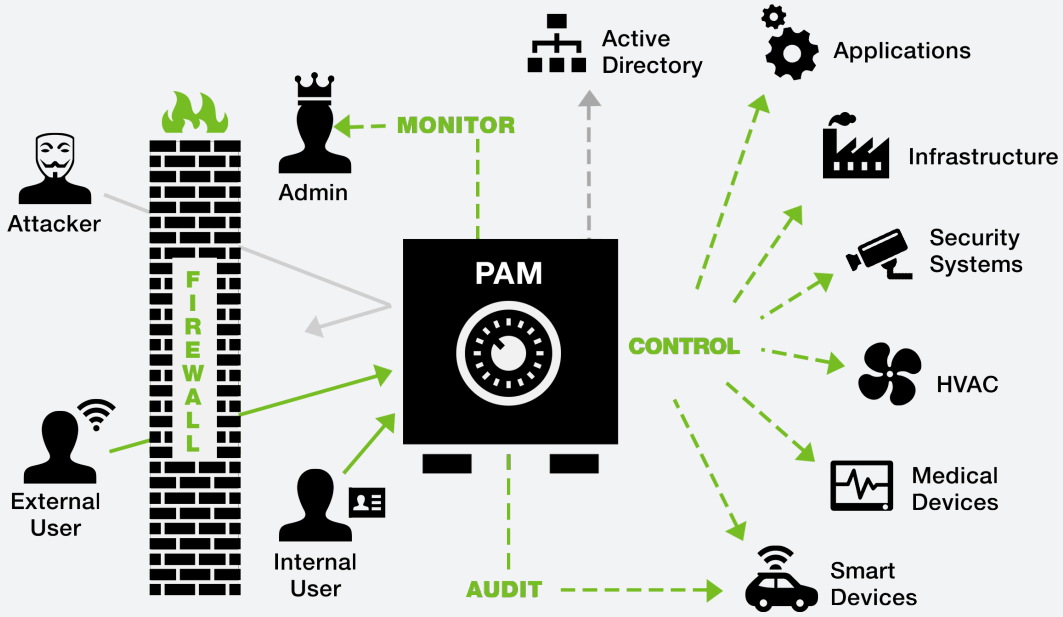
A recent study of C-level executives and business leaders, funded by IBM and ARM, found that a majority (73%) of executives said the Internet of Things has had at least some impact on business, with one in five saying it has had a major impact. The number one impact is the sparking of a new wave of innovation thanks to data that provides better insights. Yet two of the major obstacles cited by businesses in adopting IoT technologies include the cost and concerns about cyber security and privacy.

A new Verizon Data Breach Digest 2017 reported that, "Today, the IoT is not confined within an organization's typical control boundary, as the connected infrastructure has moved far beyond those control lines. These devices exist virtually everywhere, are available anytime, and are on a variety of platforms. This must prompt organizations to think about IoT threat modeling in a manner that incorporates security and privacy by design."

## THREATS TO INTERNET OF THINGS DEVICES TAKE CENTER STAGE

Devices connected through the Internet of Things pose a significant risk to enterprises and governments alike. In fact, analyst firm Forrester predicts a large-scale IoT security breach will occur in 2017. The most likely targets for such an attack include transportation fleet management, security and surveillance applications in government, inventory and warehouse management applications in retail, and industrial asset management in manufacturing. [2]

***IoT threats represent one of the most significant enterprise risks to our industrial infrastructure, since it involves enormous data or financial loss, including the real possibility of damage to property, the environment, and harm to humans.***




Protect and secure IoT privileged credentials by securing them in a Privileged Account Management vault to increase security as well as, automate control, auditing and monitoring.

IoT devices typically do not exhibit the same security controls compared with those protecting the rest of the enterprise network. For example; industrial control systems are often expected to be maintained for many years before being replaced or updated—some with a lifecycle of 15 or more years.

In the past, many devices and software used to manage our nation's critical infrastructures have been air-gapped and isolated from the public internet or physically segregated from corporate networks. In practice this meant that security measures were usually sacrificed for performance. With the advent of Big Data Analytics and the Internet of Things, however, previously isolated systems are becoming increasingly exposed to threats from Internet connections. Cyber criminals and attackers are increasingly exploiting the weaker security associated with IoT devices to compromise them and use them as launching platforms to gain unauthorized access to network systems.

As a result, IoT software frequently remains unpatched, usernames and passwords configured by the manufacturer are left unchanged, and traffic involved in managing these devices usually unencrypted.

## TO PROPERLY SECURE IOT REQUIRES EFFECTIVE CREDENTIAL MANAGEMENT

Many industrial organizations and enterprise networks rely on NIST or NERC-CIP guidelines to establish best practices to protect their infrastructures from unauthorized access. A major component of all these guidelines focuses on Credential Management.

The Industrial Internet Consortium (IIC) states that "if the credential management process is not correctly implemented and adhered to, then the results of the endpoint authentication may not provide the level of trust desired."[3]

In the industrial sector, the use of trusted devices is critical to maintaining proper security. Credential management control ensures that organizations are able to generate authorized credentials, securely store them, renew and rotate those credentials on schedule and on-demand, revoke credentials and their access when no longer needed, and maintain an audit trail record of usage activity.

To help assure proper security, the IIC has published a Security Framework for protecting devices associated with IoT. This security framework lists the top five characteristics that most affect the trust decisions of an IIoT (Industrial Internet of Things) deployment. They are: security, safety, reliability, resilience, and privacy. The IIC recommendations around the security characteristic are clear.

According to the Industrial Internet Consortium on Industrial Internet of Things (IIoT) Security, "IIoT system security should rely on automation as much as possible, but people must be able to interact with the security implementation to monitor status, review analytics, make decisions when needed, and plan modifications and improvements."[3]

> Any IoT device that has an interface will have a password protecting the interface that allows it to be configured…Plus, any Bluetooth capable device like wearables will use a PIN for a passcode." [1]

## AUTOMATE CREDENTIAL SECURITY IN IOT ENVIRONMENTS

With the exponential growth of IoT devices today, enterprises need a security strategy to protect their most valuable and sensitive information against hacker exploitation or abuse of malicious insiders.

One crucial way to minimize IoT security risks is to automate your privileged account password management with solutions that will help you:

- Create a comprehensive IoT privileged password management plan for accountability
- Adopt IoT and Privileged Account Management and security best practices across your enterprise.

To enable deployment and enforcement of the IIC "security characteristics," automated Privileged Password management solutions from Thycotic can help you secure IoT devices simply and effectively.

Delivering end-to-end, automated Privileged Account Management protection, Thycotic Secret Server provides an additional layer of security to help control, monitor and secure IoT devices. Secret Server enables your IT staff to readily authenticate all connected IoT devices on your network and protect them from unauthorized access. As a highly extensible and customizable password security solution, Secret Server allows IT and security administrators to easily manage and secure privileged account access, including remote devices (SSH, Telnet, etc.) containing administrative account privilege passwords.

> Stolen credentials may allow attackers to control physical infrastructure remotely and facilitate attacks on many of the vendor's customers simultaneously."
>
> **-Industrial Internet Consortium on Industrial Internet of Things (IIoT) Security**

Secret Server provides automated capabilities to discover privileged accounts and schedule the rotation of privileged account passwords. In addition, Secret Server's Privileged Behavior Analytics delivers a powerful platform that detects unusual behavior of privileged accounts – an early warning signs of insider threats or privileged account compromise. Today, most IoT devices can be managed directly from Secret Server using Session Launching to ensure all access to devices is logged for audit requirements, recording who has accessed which device, when, and with what level of access permissions.

To learn more about how Thycotic Secret Server can help you secure vulnerable Internet of Things devices in your enterprise, visit our website at www.thycotic.com or contact us at sales@thycotic.com

### References

(1) "The World Will Need to Protect 300 Billion Passwords By 2020," Research Report by Cybersecurity Ventures and Thycotic Jan. 2017
(2) "Large-scale IoT Security Breach Coming in 2017: Forrester" https://internetofbusiness.com/iot-security-breach-2017-forrester/
(3) "Industrial Internet of Things Volume G4 Security Framework" https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf