TERSO SOLUTIONS, INC.

2019

CHOOSING AN INVENTORY MANAGEMENT SYSTEM YOUR IT DEPARTMENT WILL LOVE

INTRODUCTION

While considering new inventory management solutions, you have probably seen several that use Internet of Things (IOT) devices connected to cloud-based platforms. These solutions are appealing because they facilitate the storage and communication of inventory information from various devices (or things) to your company's internal (or enterprise) network using internet connections. By using this approach, many more devices and geographical locations can be interconnected more efficiently than compared to what older on-premise technologies could do. The setup allows you to access applications and services without investing more in computer hardware, software and personnel, while increasing interconnectivity and improving productivity.
Saving money. Making global connections. Becoming more efficient. The benefits are undeniable. However, cloud-based systems rely on internet connections and outside servers and IT departments know that those connections and servers may not have the same level of protections as your institution's more traditional enterprise network systems. When it comes to the selection of a final inventory management platform, your IT department will look deeply into the measures your selections have taken to mitigate security risks within the cloud-based system. To make the IT review process go more smoothly and avoid delays in implementing the inventory management system, narrow your options to those that are likely to pass the IT review.

How do you narrow down the cloud-based inventory management options to those your IT department will accept, while getting the features your team needs? This paper will address some of those IT concerns to help you make a more informed decision...without requiring you to become a security guru.

WHAT'S IMPORTANT TO IT?

What are the most dangerous parts of an airline flight? Is it when you are soaring 547mph at 35,000 feet? No. Somewhat counterintuitively it is at takeoff and landing. Data is similar. When it is cruising along inside a system, or on an encrypted connection, it is relatively safe. It is the points of change, when the data is leaving one system or entering another where your system is most vulnerable.

As a result, IT will focus mostly on:

1. How the connection initiates
2. How the connection is secured
3. How data is being received and controlled

Below is a simple version of a cloud system to identify the vulnerable points within a typical service. Figure 1 denotes the main areas to consider in your review:

1. The devices (or things) attached to the cloud. This might be a medical-grade freezer, a storage locker, or a single sensor. It might be tablets or other mobile devices. These items can store information and act as connecting points to the cloud.

2. The communications among all elements within the cloud-based network. In other words, how does the data move; what triggers that move; and how and where is the data stored?

3. The cloud itself. That nebulous collection of servers acts as a repository containing certain programs and company information for use across all connections and devices.

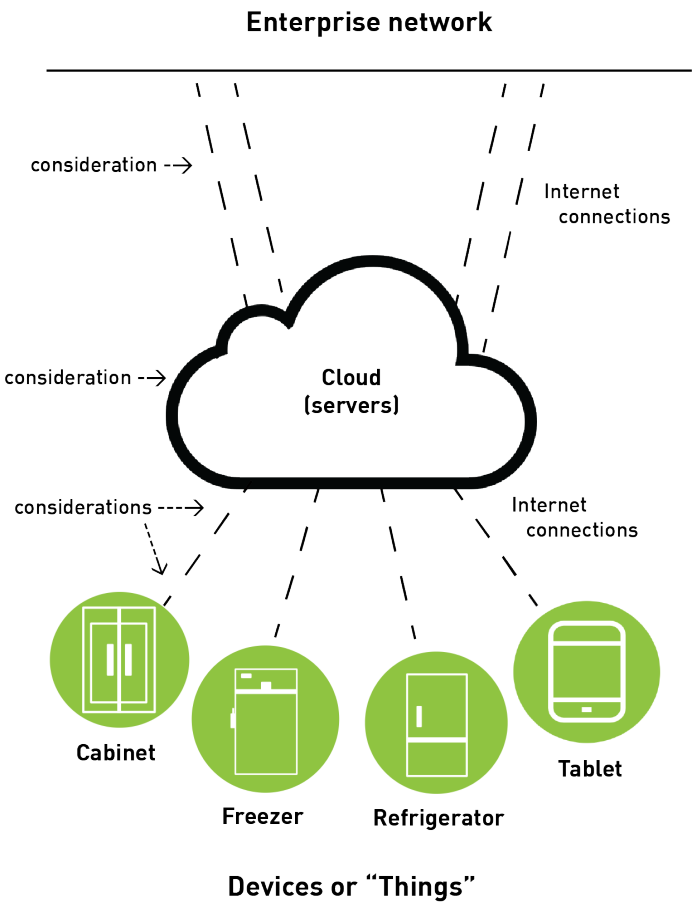

Figure 1.
Areas of consideration within a typical cloud-based application. Areas of change are of most importance to IT. These include how connections are initiated and secured and how the data is received and controlled.

The security considerations at these points are primarily addressed through two approaches: encryption and authentication protocols. These two approaches must be used in combination to address the various security points of concern, and multiple types of each may be used within a cloud-based inventory management system.

WHAT ENCRYPTION AND AUTHENTICATION METHODS AS WELL AS OTHER FEATURES SHOULD I LOOK FOR?

A first area to focus on is how the system is accessed. Looking at user-level access, there are IT personnel who use the tools in the cloud to manage your system and the users who access the IoT devices connected to the system. There are also non-technical users accessing this data in their day-to-day work through a dashboard or other interface. Access for either type of user should be controlled by strong, unique access keys or passwords. It might also be useful for the system to have the ability to set a hierarchy of access levels (i.e., permission sets) so that users can only access the data they need, and no more. This concept is often known as the principle of least privilege. On the device end, user access should similarly be controlled. The ability to define permission sets (e.g., one person can access only a subset of freezers) can be important, and in some situations, may be required. Typical controlled access to devices usually relies on key cards, passwords, and/or biometrics.

Cloud-based systems use internet connections to transport data from a device through the cloud network. A preferred cloud-based inventory management system should connect via https, which provides an additional level of data encryption over the standard internet connection (The difference in how HTTP and HTTPS communicate data is shown in figure 2.). This is the same security element you look for when ordering from an online vendor. Just as you don't want to give credit card information over an unsecure internet connection, likewise you don't want your sensitive inventory information traveling over internet lines that are not https. Not all https is created equal, websites that take security seriously will be using TLS 1.2 or higher, as older forms of https are not secure against a determined hacker.

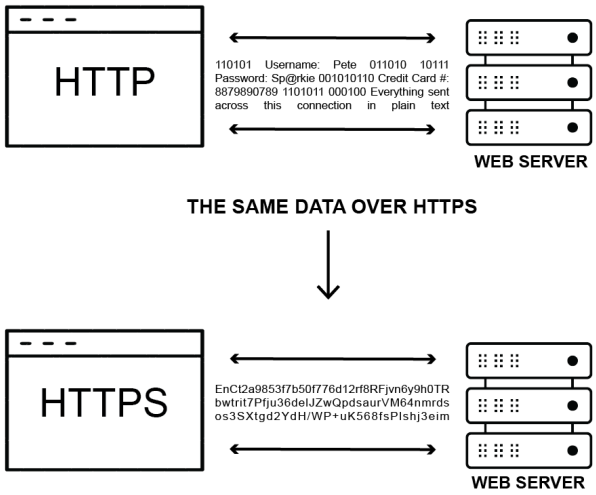

Figure 2.
The difference between how information is communicated from a data encrypted site versus a non-secured site.

Next, learn how communications between devices and the cloud are initiated. The preferred initiation is one-way, with the device initiating communication with the cloud servers. Your IT department will not want the cloud initiating communication to the device. It is also good that once the communication is initiated, it remains open (versus locked) because the system will work more seamlessly and be faster than if the device always has to initiate a connection. To achieve this real-time interaction, look for IoT devices that utilize

websocket protocols.

With communications always open, you might wonder if that would increase security concerns. With websocket technology, the device-cloud connection is open under "terms". These terms are authentication protocols that alert the cloud servers and the devices when one or the other is compromised. Think of these authentication protocols as a pass phrase you have with a bank, where both entities need to know it before a service or exchange of information can happen. If the device tries to share a wrong pass phrase, the system will view that device as compromised and immediately disconnect it from the system. For a cloud-based system, authentication methods can include strong "hashed and salted" passwords that are exchanged between a device and the cloud, for example, a very long access key (hashed) with a device serial number attached for further identification (salted). Other, more complicated authentication methods might use certificates to verify device identification within the cloud. If the authentication measures are done properly, they can apply to large numbers of varied device types, enabling your IoT solution to scale securely.

The actual transmission of data within cloud-based inventory management systems can be triggered using time or events. Time triggers might collect the device data hourly or daily, for example, whereas event-triggered data transmission will be more real-time. A storage door opening could be an event trigger that sends the data (what was removed and by whom) through the cloud. With regards to security, event-based triggers would provide more immediate awareness of a breach over time-based models. Lastly, the cloud should be considered. When evaluating a system, you need to understand the type and volume of company-specific information that is stored in the cloud. It is important that the data stored is minimal, and what information is stored cannot be easily leveraged by outsiders to get into your other systems and devices. For example, a device name or serial number stored in the cloud should not be a big issue. However, your customer's billing data is better stored at the enterprise network levels, not in the cloud. Figure 3 provides an example of a cloud-based platform that includes the encryption and authentication measures to look for when choosing an inventory management system.

The cloud itself should be encrypted for protection. In addition, your institution's information within the cloud should be encrypted because the space is shared with other companies and institutions. Encryption is complex and there are multiple types. Don't be fooled by companies touting high bit encryption counts. It may surprise you to learn 2048-bit RSA encryption is widely considered inferior to 256-bit AES encryption. Luckily most systems use 256-bit AES encryption, so just knowing that this (or an equivalent) is being used should give you peace of mind. That level of encryption is considered unbreakable in our lifetimes, even if decryption was attempted by the world's fastest supercomputer.

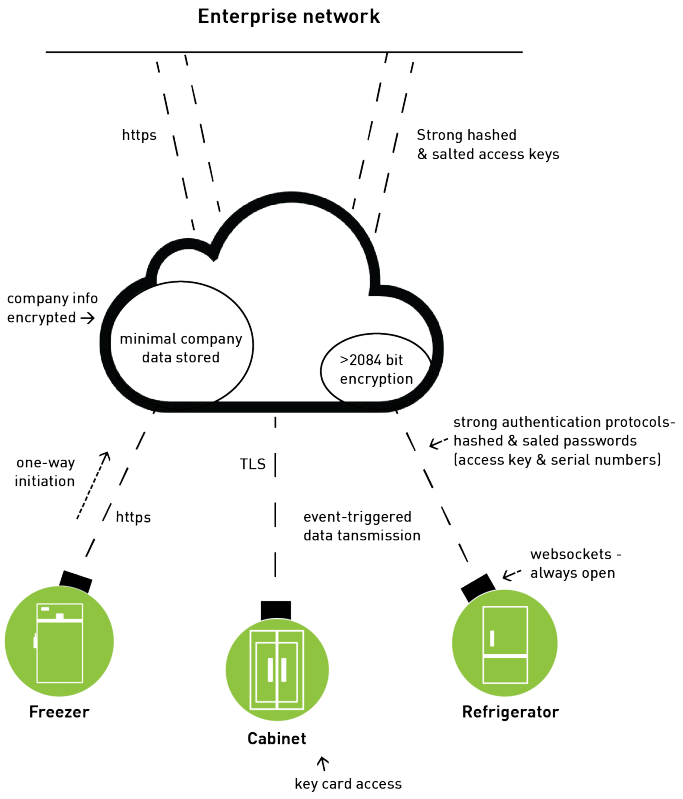

Figure 3.
Examples of the various features, encryption and authentication measures of a cloud-based inventory system. The Jetstream inventory management system from Terso Solutions features many different encryption and authentication measures as well as other features that mitigate the security concerns that might be associated with a cloud-based platform.

Another cloud consideration is the cloud service provider's reputation. Do they have a record of updating for security purposes? Are they a validated environment that is regularly tested for potential security breaches? A lot of people can set up a cloud application—you want those that have demonstrated credibility in managing the system and its security. Also look for a service provider that will partner with you because the best security will be achieved from both the service provider and your own IT team working together.

SUMMARY

You do not need to become a security guru to select an inventory management system that offers the best security protections. Simply having a basic understanding of how the devices connect to the cloud, how those connections are secured and how data is managed over the cloud system should help you make smarter choices. Knowing to ask how the data is secured at every step of the journey from physical device, to cloud, to your systems will help you find a partner that your IT team will love.

We know about building security into IoT and cloud applications, because that's what we do every day. Terso Solutions offers the end-to-end security you deserve from an inventory management solution. From our IoT devices deployed across the globe, to our AWS-hosted cloud servers, from our Jetstream API to any inventory management solution, we ensure that security is built in at every layer and connection point.

ABOUT THE AUTHORS

Travis Phillips is the Technical Architect and Taylor Leick is the Software Product Manager at Terso Solutions, Inc., the leading provider of automated inventory management solutions for tracking high-value medical and scientific products in healthcare and life science. The Terso line focuses on RAIN RFID cabinets, refrigerators, freezers (-20°C to -80°C), smart rooms, and cloud-based solutions that deliver improved productivity and cost efficiencies.