IoT Device Security and Privacy for Thermal Scanners

With more businesses implementing thermal scanners and touchless check-in tools as part of their overall reopening strategy, you may be considering implementing one in your workplace. Using intelligent sensors and software automation, these solutions can save your organization time and provide an additional layer of safety to your workplace.

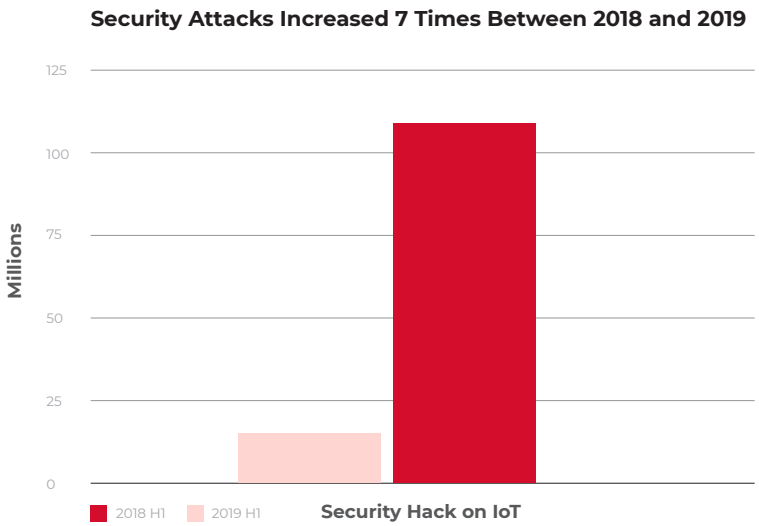
In considering the right solution for your workplace, you'll want to ensure both the safety of your staff and the security of your organizational data. These IoT devices have cameras and sensors that can capture sensitive information, and they often sit on the same network that your other workplace systems run on. As more white-labeled scanners enter the market from unknown manufacturers, it is important to not only understand how these solutions work, but it is also critical to consider how these devices were designed, by whom and what they're doing with your data.

In this white paper, we provide you with a framework for evaluating workplace IoT devices across five critical categories: **1. Data Security**, **2. Data Access and Permissioning**, **3. Privacy**, **4. Security Maintenance** and **5. Physical Security**.

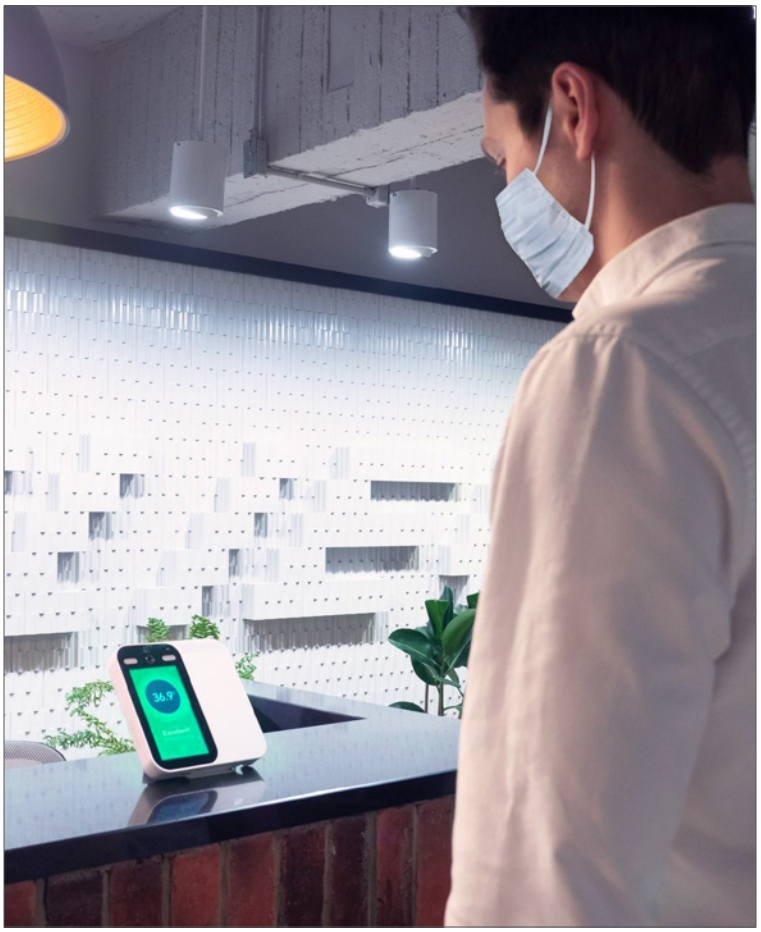
Data Security

Data security refers to the process of protecting data from corruption and from unauthorized access throughout its lifecycle. A recent study[1], conducted by security firm Kaspersky, of almost 5,000 companies in 23 countries reveals the depth of the risks associated with IoT systems.

Of the 3,050 companies with IoT systems in use, over a quarter (28%) faced attacks targeting their connected devices in 2019. In total, Kaspersky noted that 105 million attacks against IoT devices were reported in just the first half of 2019—an increase of 7 times over the same period in 2018. Even though IoT devices can pose a security risk, they perform essential functions that businesses increasingly rely on.



Given their interoperability with and access to business networks, IoT devices can be attractive targets for hackers and the consequences for businesses can be significant. To mitigate risk, there are three main considerations when choosing a device:



1. **The device itself.** Who manufacturers it and to what degree have they prioritized data security? Rather than just a feature, security should be central to the design of the overall device. "Security does not just happen. It needs to be designed in from day one," writes industry expert Chris Hickman.[2]

2. **Encryption**. Data can be at risk whether it's at rest or in transit, and it's crucial that it be properly secured in both states. For data at rest, files should be encrypted before they are stored in addition to the storage drive itself, if possible. For data in transit, files should be encrypted beforehand and an encrypted connection (HTTPS, SSL, FTPS) should be used to transfer them.

3. **Network security**. The IoT network should be secured in such a way that potential security breaches would not compromise the entire business network. Many gateways only protect the IoT devices connected to them rather than the actual gateway, meaning that a gateway breach can result in the deactivation of security technologies. Ensure that your organization conducts regular network security reviews, with special attention paid to IoT networking.

For organizations that want to dive deeper into ensuring holistic IoT security, the IoT Technology Stack below[3] outlines the steps to take to ensure your organization is protected.

Device Hardware
- Physical tampering
- Open ports

Device Software
- Identity management
- Anomaly detection
- Firewall
- Safe Boot
- Data encryption at rest and during transfer
- Patches

Communication
- Encryption
- Secure networks (VPN, private networks)
- Secure access to the network (i.e., Wi-Fi drive-by)

Cloud Platform
- Best practice in IT security
- Secure hosting
- Patches
- Encryption
- Identity management
- User management - right people, right permissions
- API authentication and authorization
- Multiple layers of authentiction for critical items

Cloud Applications
- Authentication & authorization
- Secure hosting

Data Access and Permissioning

Cloud portals make it convenient to access your IoT data but with that data access comes the risk of exposing data to the wrong eyes. When considering employee data across various office locations and departments, it is critical to have multiple levels of data access so that the information is only available to authorized personnel.

Account-based data access and permissioning are key to ensuring the security of your network. Many organizations have networks and devices with incorrectly configured permissions, rendering sensitive data vulnerable to exposure. A recent report from security firm Varonis[4] found that 18.9% of companies with an excess of 1 million folders have 100,000 of them accessible to every employee in the organization—many of which have full editing permissions. "Depending on the OS and device, there can be dozens of individual granular permissions, along with inheritance issues and group membership considerations that can add up to permission mistakes," writes security expert Roger Grimes[5]. He ranks improper permissioning as the fourth biggest cybersecurity risk to companies, after social engineering[6], unpatched software and passwords.

Experts like Grimes suggest integrating permission and access audits into your regular network security reviews. In terms of IoT devices specifically, access and permissions should be easily customizable so that super administrators can set them for every level of user across the organization. For example, location-specific administrators with a certain level of access can oversee permissioning at each specific office, while individual users can only access their own data.

When evaluating your IoT solution's cloud platform, make sure you spend enough time understanding its capabilities on data access and permissioning.

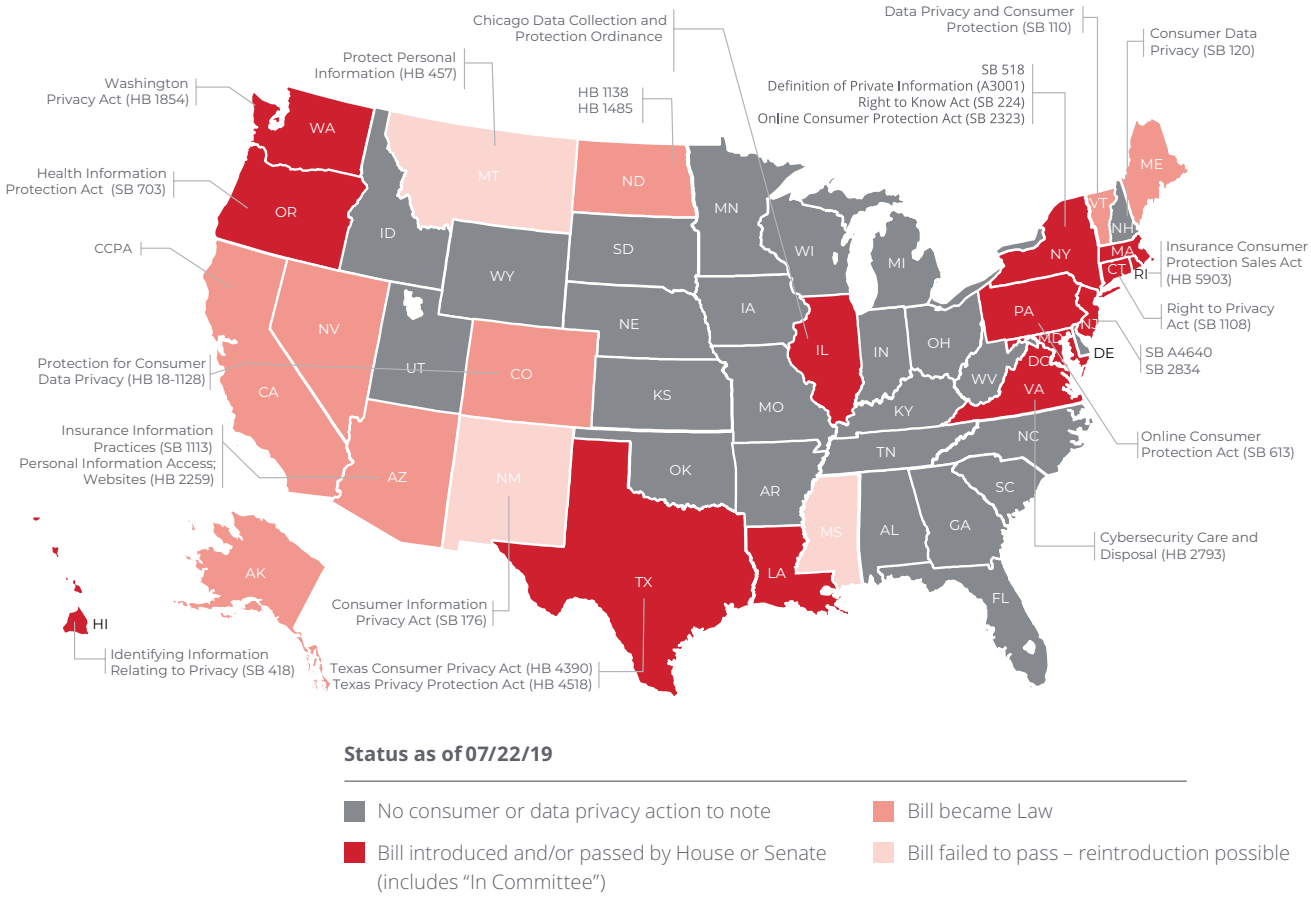
Privacy

Protecting individual privacy has never been more important, both from the viewpoint of employees and guests as well as from a regulatory standpoint. In the years following the passage of GDPR in Europe, more comprehensive laws pertaining to the collection, storage and sharing of personally identifiable data have been popping up across the United States—most notably the passage of the California Consumer Privacy Act (CCPA) in 2018.

These new laws require businesses to better understand their data collection and sharing practices and to implement reasonable security measures to protect any personal information contained therein. They also impose new obligations around data quality, completeness and governance. As a result, many businesses are in the process of reviewing which types of data they collect, how it's retained and for how long.

They are also reviewing their data sharing practices in cases where third parties, vendors or service providers also have access. According to Kaspersky Research, 36% of organizations give third parties access to their IoT systems. Not only does this increase the possibility of a data breach, but it also poses a compliance risk.

Similar legislative initiative to the CCPA across the United States[7]



To maintain compliance with data privacy laws, businesses should select a solution and provider that protects sensitive information and ensures that any data retention is managed in a compliant manner. It's important to understand the type and source of personally identifiable data being collected, used and retained, and to have a system in place to respond to customer requests around deletion. Companies should also maintain a comprehensive inventory of their third-party relationships and understand which types of data are being shared as part of these relationships.

To protect your organization and employees, ask your provider about their compliance with CCPA, GDPR and other privacy laws relevant to your workplace.

Security Upgrades

Regular software and firmware updates are key to maintaining overall system security. The Kaspersky study[1] shows that 86% of organizations have vulnerable or obsolete software, which is a common cause of security breaches and distributed denial-of-service (DDoS) attacks. Once vulnerabilities are exposed, the provider should patch the software or firmware in question as quickly as possible and make it simple for you to incorporate the patch.

Keeping software up to date is particularly important for IoT devices, notes industry expert Bruce Schneier. "Many of the embedded networked systems in these devices that will pervade our lives don't have engineering teams on hand to write patches and may well last far longer than the companies that are supposed to keep the software safe from criminals," he writes. "Some of them don't even have the ability to be patched[8]."

It's important to ensure that whichever provider you choose is responsive when it comes to patching vulnerabilities. Recently, a backdoor was discovered in DblTek branded devices by IT security firm Trustwave that enables a remote attacker to access root privileges. The researchers alerted the manufacturer, who responded by trying to make the backdoor more hidden rather than closing it. According to IT security researcher Zach Lanier, this is not an isolated incident. "Network devices from manufacturers all over the world have fallen prey to attackers time and time again—often by way of backdoor services and accounts," he says. "These backdoors are often present under the guise of providing 'remote administration' or 'support', but occasionally for more nefarious purposes[9]."

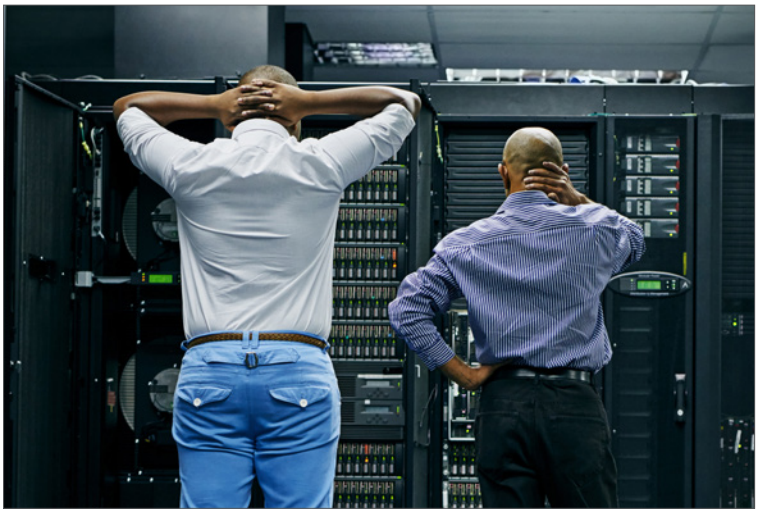
It is vital to select a device that is easy to update (or uses over-the-air updates), as delaying critical software or firmware updates can be detrimental to overall system security. Before installing an IoT system, ensure you have a clear understanding of how the company keeps its software and firmware up to date and your role in that process (if any). It's also important to ensure that secure code signing processes are used to validate the signature of updates, so that only trusted code is executed on the device.

Physical Security

One of the most important, but often overlooked, considerations in evaluating IoT is physical security. Physical security involves vulnerabilities that come from a malicious actor being in close proximity to the device. That risk can come from security backdoors installed during the manufacturing process or from hackers gaining physical access to your active device.

With global security risks on the rise, especially from foreign sources, the most critical question is whether an IoT device is made by a trusted manufacturer. You should ask potential solutions providers:

- Who actually manufactures your device?
- Do you have full control of the components and firmware of the device?
- Do you have access and control of the manufacturing and quality control process?



It is important that the device be difficult to tamper with and free of any potential backdoors to your business network. The risk associated with backdoors is increasing. Last year, Microsoft reported that it had delivered almost 1,400 security notifications to companies whose IoT devices had been targeted or compromised by hackers over a 12-month period. "When an actor gains access to a network via an IoT device, they will often sniff out other unsecure devices to provide them with broader access to the network and will target higher-privileged accounts in order to obtain deeper network access," notes law firm K&L Gates LLP[3].

When evaluating an IoT device, it's important to understand the mechanism used to determine and flag root access, or unauthorized tampering with the device. Does the manufacturer have an established process by which vulnerabilities can be reported and quickly corrected? What type of cybersecurity process or auditing does the device have? Make sure you are able to review internally and fully understand the details before you make your final decision. In conclusion, it's important to consider both the security of your data and the safety of your employees when evaluating a potential IoT solution. Threats to network security, data privacy and physical security are ever-present, and maintaining employee and customer trust as an organization is paramount.

The LivMote Solution

LivMote offers industry-leading security and privacy controls and is highly customizable in order to meet your organization's needs. LivMote's main points of differentiation are:

Data Security	■ Runs on best-in-class data security standards, with AES-256 encryption of data at rest and HTTPS/TLS 1.2 encryption over Port 443 for data in transit. ■ Cloud platform is built on Azure, Microsoft's cloud computing service, which is purpose-built for deploying and hosting secure IoT solutions. All data in transit through Azure's infrastructure is automatically encrypted to ensure data confidentiality and integrity. ■ Does not rely on facial recognition and does not capture face geometry. The system only captures a rectangular bounding box for face positioning, to ensure reading accuracy and we never store that information.
Account Access and Permissioning	■ LivMote's ScreenMeIn™ platform offers multiple levels of account security and data access permissions to ensure data does not get into the wrong hands. ■ Platform data access can be given for a single location, department or across the whole organization.
Data Privacy and Management	■ LivMote allows you to manage what data is collected and for how long, including the option to collect no data whatsoever. ■ Its platform and services have undergone third-party privacy and security audits and work with CCPA and GDPR regulations.
Security Upgrades	■ Performs regular over-the-air (OTA) upgrades to system applications, firmware and security. ■ Enterprise OTA process allows nearly immediate vulnerability patches. ■ Every firmware and system app that is updated through our OTA server is verified using a secure code signing process, indicating that the file is the one that was originally uploaded and is not malicious.
Physical Security	■ Designed in California and manufactured in Taiwan by Foxconn, the world's leading electronics manufacturer. ■ Protective security mount prevents unauthorized removal and has a built-in tamper detection mechanism to detect root access.

Sources

1. Kaspersky Lab, Benefits and challenges of IoT in business, 2020
2. Security Boulevard, Key Considerations for IoT Security by Design, April 2020
3. ScreenMeIn, IoT Device Security and Privacy for Thermal Scanners, August 2020
4. Varonis, 107 Must-Know Data Breach Statistics for 2020, April 2020
5. CSO, Check your access control permissions before hackers do, April 2019
6. CSO, Social engineering explained: How criminals exploit human behavior, September 2019
7. Deloitte, Data privacy as a strategic priority, 2019
8. Schneier on Security, Ransomware and the Internet of Things, March 2017
9. Internet of Business, Security researchers find backdoor in Chinese IoT devices, 2017

Final product design and user interface are subject to change.