WHITE PAPER

Intel IoT
Intel® Security

More Confidence, Safety, and Security in the Digital World

We are addressing end-to-end IoT security by hardening devices, securing communications, and analyzing and monitoring networks while managing the complexity inherent to such systems.

The Internet of Things (IoT) has the potential to transform our world and reshape the way we interact with our environment. Millions of previously unconnected devices will soon begin to transmit data to the cloud and to each other, potentially making us even more reliant on the Internet and the technology that enhances our daily lives. Data is crucial in the Internet of Things as it enables new insights and innovations in automation. Sensors and devices are constantly sending and receiving information, which presents an opportunity for companies to transform their operations, but can also increase complexity. IoT implementations must be architected to manage the flood of data to achieve best results. Intel has the technology, expertise, and reach to bring simple and more secure IoT solutions to new industries, helping to accelerate the development and deployment of new products while enhancing security.

Security is a fundamental pillar for IoT solutions. With decades of experience in computing, Intel® Security takes a holistic view of the threat defense lifecycle, with solutions to **protect** against attack, to **detect** compromises, and to **correct** or remediate after an attack, restoring normal operations. The very nature of IoT means that any disruption can be very damaging. The Intel® IoT Platform, which includes reference architectures and a portfolio of products from Intel and our ecosystem, provides security offerings that can help system integrators create new applications that feature security as a core component for their specific industries.

The Challenges in Securing the Internet of Things

IoT systems interact with the physical world and increasingly operate critical infrastructure such as utilities and transportation. And the nature of IoT means that a security compromise could have physical consequences. This means that security solutions generally will reorder the usual considerations, focusing on delivering availability first, followed by integrity and confidentiality. IoT also presents a new set of challenges that developers and system integrators historically haven't had to deal with, including:

- A long, complex life cycle in which devices are seldom, if ever, rebooted, make continuous threat prevention imperative. Critical security updates must be delivered without disrupting uptime.
- Devices are often part of a system of systems; complex networks that need to be secured along multiple end points and communication channels.
- Internet of Things solutions often rely on devices that are mass produced in the same configurations, leaving a broad swath of systems that can be left vulnerable without proper installation and updates.

- Gateways represent a great opportunity to include legacy equipment in the IoT, but because these devices were never intended to be connected, they do not have even the most basic security protections. The gateway needs to act as a "helper" to protect the edge.
- The IoT delivers value by comprehending an end-to-end system. When thinking about a solution, we need to consider security at the device level, securing communications and protecting the cloud in order to understand the potential threats to deployments.
- IoT devices are used in different environments with vastly different risk profiles. For example, a temperature sensor might be used in a home or a nuclear reactor, each with very different device security, data protection, and encryption needs.
- Machine-to-machine communication presents a bigger challenge in terms of device identity. Security solutions have to verify the veracity of device data, device integrity, and identity while also ensuring data is protected as it travels to the cloud.

These considerations mean that companies pioneering the Internet of Things have to think differently about security. While there is no "silver bullet" to secure the IoT, there are many technologies available to protect against attack, detect compromise and correct compromised IoT systems.

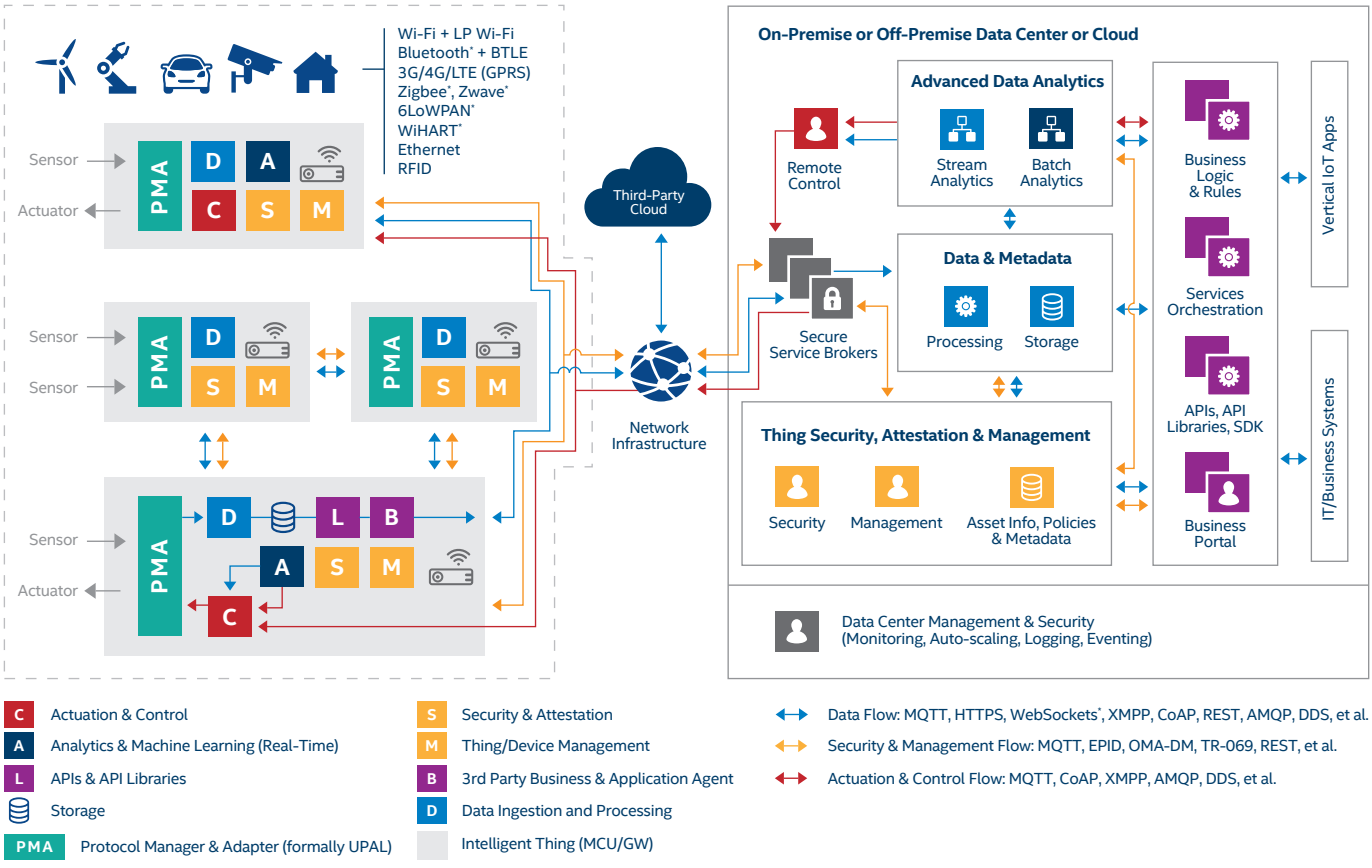
Addressing Security at All Levels

Intel Security takes a holistic approach to preserving the integrity of IoT solutions, with a strategy of delivering IoT-appropriate software products, a robust hardware foundation built into Intel® processors and SoCs, and by offering platforms for integration with third-party security solutions. Our goal is to address IoT security end-to-end by hardening devices, securing communications, and analyzing and monitoring networks while managing the complexity inherent to IoT. This means our customers can focus on creating new products that have security woven into their fabric.

While security fundamentals are consistent across the different market sectors comprehended in IoT, there is

INTEL® IOT PLATFORM

Reference Architecture for Smart and Connected Things



Security is at the center of the Intel® IoT Platform reference architectures

also a need to understand the specific risk profiles and implementation constraints for individual use cases. That allows us to tailor solutions designed for optimal cost benefit.

An example of a tailored and comprehensive offering is McAfee Enhanced Infrastructure Protection* (McAfee EIP*). McAfee EIP is a preintegration of Wind River and McAfee branded products designed to provide end-to-end security for systems with the highest protection requirements. We've made use of Wind River's virtualization and secure operating systems plus McAfee integrity control, network security, and management technologies, and configured them to take full advantage of Intel silicon-level features. McAfee EIP provides the means to harden devices, secure communications, and manage/monitor security.

Another example of a market-specific effort is the work Intel is doing in automotive security. In addition to delivering hardware security features plus Wind River and McAfee products to protect cars, we have undertaken an industry effort to learn from some of the best security researchers and to improve best practices broadly. We have established the Automotive Security Review Board and published a white paper called Automotive Security Best Practices.

Companies developing IoT products have access to McAfee Embedded Control* technology, which allows for whitelisting of software to help prevent rogue applications from running on devices. Additionally, McAfee ePolicy Orchestrator* (McAfee ePO*) software, which has been successfully helping enterprises manage hundreds of deployed devices with ease, may also be used to perform security management on IoT devices. McAfee ePO provides a platform for innovation, with more than 100 partners developing applications to address the problems facing enterprises and system integrators today. Lastly, Intel Security customers gain access to McAfee's Global Threat Intelligence* technology, which leverages information collected by 1M devices located in 120 countries to help companies defend against attacks.

Intel solutions also feature a hardened foundation, with security built into systems at the silicon level. The Intel® Data Protection Technology for Transactions solution is designed for use in retail point of sale systems. It uses a trusted execution environment in Intel silicon to separate sensitive data from the solution's software, employing whitelisting and encryption capabilities built into the hardware to enhance security of credit card information. This product is designed to facilitate secure handling of information throughout the entire chain of a connected solution, from peripheral devices to terminals, and eventually to the cloud for processing and analysis. Although this technology was initially developed for the retail industry, it can potentially be used to help secure a variety of Internet of Things solutions. As connected solutions become more common in our daily lives, consumers will want reassurance that companies are working to safeguard their personal information regardless of the setting and platform.

Another example of hardware-based security technology that is very useful to IoT is Intel® Enhanced Privacy ID technology (Intel® EPID). Intel EPID may be used for very robust device identity, which is critical for IoT. It's imperative that the IoT system be able to trust that the data it's using is coming from a known and secure device. But Intel EPID goes a step further, providing device identity without compromising privacy by offering anonymity preserving properties that allow the device to be securely identified as part of a group. An example of this could be that of a smart driver's license. A smart license could potentially identify the bearer as being in the group of people of a legal age to drink without revealing the holder's address, driver's license number or actual birthdate.

Intel Security also focuses on protecting industry innovation by building new products and platforms that make it easy for developers to better secure their Internet of Things solutions. The Intel IoT Platform gives system integrators a clear path that allows for specialization while taking care of complex security considerations. Additionally, Intel is constantly rethinking protection in order to innovate how we approach security in a rapidly changing technology environment. For example, in rethinking the concept of "trust" Intel has evolved the process of attestation into a multifaceted approach in which devices and data centers must affirm their identity to each other. With this approach in mind, Intel has developed a number of technologies that force devices to prove multiple things about them, leading to more complex systems to better safeguard data. Additionally, Intel has technology built into the silicon that only allows whitelisted software stacks to run on a device to help prevent rogue agents from infiltrating the network by hijacking trusted devices.

Conclusion

The Internet of Things has the promise of improving our lives and our world. Intel Security is committed to designing systems that build security and privacy protections into the Internet of Things.

Learn more at intel.com/iot

0216/LS/CMD/PDF Please Recycle 333916-001US