McAfee
Together is power.

Protecting the Internet of Things

The Internet of Things (IoT) is an exploding market that could herald the "next Industrial Revolution."[1] IoT devices are becoming more pervasive. From fitness wearables and retail point-of-sale systems to medical devices and robotics on the factory floor, IoT devices are being used by nearly everyone everywhere. It's estimated that connected devices that fall into the IoT category will reach 20.8 billion by 2020.[2] IoT has become increasingly important to device manufacturers as customers are demanding products that can be connected to the internet.

While IoT devices are becoming commonplace in almost all areas of our lives, the potential risks associated with them are formidable. In large part, this is because native, built-in security is based on the simplicity of these devices and generally doesn't take into account the larger infrastructure and connectivity picture. Because these devices generally do not have the benefit of private networks, exposure to advanced cyberthreats can be significant. IoT device manufacturers are eager to find better ways to secure their IoT products before they hit the market. As part of its open, connected approach to security, McAfee is committed to helping IoT device manufacturers provide security at every level: the device, the connection, and the cloud.

IoT Security Challenges

At this point, it's too early to adequately answer the question of how cybercriminals will profit from hacking into, or taking advantage of IoT devices. The **McAfee® Labs Threat Predictions for 2017** suggests that this will become clearer over the next four years and that we can expect a proliferation of financially motived attacks in the IoT realm. In addition, we can expect that IoT devices used at critical infrastructure sites, such as nuclear power plants and electrical grids, will be become cyberwarfare targets.

Here are some of the trends predicted by experts at McAfee Labs:

- Ransomware, which has become a growing threat across the board, is expected to become more prevalent on IoT devices. Such threats are already appearing in healthcare and the power distribution sector.
- We are likely to see hactivisim and, potentially, nation-state attacks migrating to IoT devices. By commandeering connected IoT devices, these groups may attempt to make political statements through dramatic acts like altering voting machines or opening the valves of a dam.
- IoT devices, by nature, will further diminish consumer privacy, requiring manufacturers to provide explicit agreements, opt-ins, and possibly compensation for using or sharing data without authorization.
- With weak or non-existent security controls in place, network-connected IoT devices will serve as convenient attack vectors into control, information, and surveillance systems. Additionally, rather than focusing their efforts on single devices, hackers will attempt to access the control plane, which will enable them to scale up and attack entire communities of devices. Similarly, aggregation points, where data is collected from multiple devices, will be an attractive opportunity for large-scale data theft.

2016 saw one of the biggest distributed denial-of-service (DoS) attacks in the history of the internet. The attack was launched by taking over connected devices like surveillance cameras, routers, and DVRs.3 In light of recent events like this, IoT device manufacturers can't afford to make security an afterthought. Security must be built into the design of the device at every layer: the hardware, software layer, network connections, data in transit, and application data. To provide a secure user experience, new IoT security architecture must:

- Guarantee authentication without jeopardizing individual privacy
- Address key issues such as integrity assurance/functionality, trustworthiness, accountability, privacy, and roles/responsibilities
- Protect new IoT devices and custom interfaces while supporting IoT-connected devices that use legacy systems
- Support resource-constrained devices with smaller CPUs and scarce memory
- Function seamlessly across devices, networks, the cloud, and data centers
- Address today's risks while adjusting for the security challenges of tomorrow

Strengthen the Threat Defense Lifecycle for IoT Device Manufacturers

The open, connected McAfee security ecosystem enables IoT device manufacturers to detect, protect, and correct threats faster, and to automate their defense with fewer resources. The ability to share threat intelligence between McAfee and third-party products helps IoT device manufacturers build products with stronger security that can more rapidly adapt to the changing threat landscape. McAfee solutions both accelerate time to market for IoT device manufacturers and strengthen the threat defense lifecycle for their customers by:

- Delivering pre-tested, ready-to-deploy application and hardware combinations
- Providing a connected architecture that enables products to learn from each other and act as one when responding to security threats
- Solving IT and cloud services challenges in connecting next-generation systems to new and future services

Protection at Every Level

Truly effective IoT security needs to span three levels of the technology architecture: the device itself, the connection, and the cloud.

- IoT device manufacturers must protect the device and user identities, ensure device integrity, and protect operational and personal data on every device. Each device should guarantee authentication without jeopardizing individual privacy and have the ability to automatically self-assess and resolve any situation.
- When it comes to the connection, manufacturers need to ensure secure applications, traffic, and data security in transit through every type of wired and wireless network connection.
- The cloud component must deliver the necessary trust for data centers and multitenant public cloud environments to unleash powerful IoT services and analytics while protecting data and ensuring privacy.

Proven technologies from the McAfee solution portfolio can help IoT device manufacturers take advantage of rapidly growing IoT market opportunities. IoT device manufacturers can build in comprehensive security with the help of McAfee by:

- Locking down a device's original software configuration through dynamic whitelisting to reduce the overall cost of post-sale operation
- Reducing service and support issues to increase customer satisfaction
- Strengthening device security by preventing unauthorized code from executing on a managed device
- Embracing future use case scenarios through a vast array of easily deployed security capabilities
- Providing integrated central security management, reporting, monitoring, and analytics for global insight and proactive device control

Devices	Features	Benefits
Application and change control		
McAfee Embedded Control	▪ Safeguards applications and binaries at the kernel level from malware and zero-day exploits ▪ Dynamic whitelisting allows only authorized code to run ▪ Permits only authorized changes ▪ Monitors, prevents, and logs unexpected, unauthorized changes and attempts ▪ Integrates with Intel IoT Gateway	▪ Protects embedded systems—such as point-of-service terminals, ATMs, and medical imaging systems—from malware and zero-day attacks ▪ Change control reduces support and field maintenance costs related to security problems ▪ Meets PCI compliance requirements
McAfee Integrity Control	▪ Dynamic whitelisting trust model ensures that only trusted applications run on fixed-function devices, such as point-of-service (POS) systems, automated teller machines (ATMs), and kiosks ▪ Blocks unauthorized and malicious applications ▪ Provides continuous change detection and prevents unauthorized changes	▪ Increases control over fixed-function systems ▪ Reduces customer risk ▪ Dynamic whitelisting lowers cost of ownership ▪ Improves service availability ▪ Helps IoT device manufacturers meet and sustain PCI DSS compliance
Data security		
McAfee Endpoint Encryption	▪ Protects data on removable media, such as USB flash drives ▪ Controls the specific file types and folders to encrypt or block ▪ Encrypts files to cloud storage services such as Box, Dropbox, Google Drive, and Microsoft OneDrive	▪ Policy-based, scalable encryption protects vPaluable user data ▪ Automatic, always-on encryption—even when data travels across devices ▪ Transparent to the user
McAfee Device Control	▪ Prevents data from exfiltration via removable devices: USB drives, tablets, Bluetooth devices, CDs, and DVDs ▪ Comprehensive device management controls and policy enforcement to allow or block data copied to removable media ▪ Complete visibility through reports generated by the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console	▪ Unparalleled data protection ▪ Simplified management ▪ Enables IoT device manufacturers to prove compliance

Devices	Features	Benefits
Content security		
McAfee Embedded software development kits (SDK)	▪ Antivirus SDK safeguards systems and files from viruses and other security risks It detects and removes malware, and configures antivirus policies to manage quarantined items ▪ McAfee Global Threat Intelligence (McAfee GTI) SDK provides IoT device manufacturers' products with access to threat intelligence data (web/URL filtering) gathered by a global network of 100 million sensors and correlation capabilities of more than 350 researchers	▪ IoT devices can identify and block a wide range of threats, including targeted attacks using unknown malware with no catalogued signature ▪ Protect IoT devices with the same security intelligence used by the majority of McAfee products
Hardware-assisted security		
McAfee Endpoint Security	▪ Machine-learning behavior classification detects zero-day threats in near real time—enabling actionable threat intelligence and automatically evolving behavior classification to identify future attacks ▪ Closes the gap from encounter to containment from days to milliseconds with the help of threat intelligence gathered from multiple sources ▪ Intelligent, adaptive scanning capability monitors, prioritizes, and escalates, as warranted by suspicious applications, processes, and behaviors ▪ Defends against ransomware and greyware, and secures "patient zero" ▪ Protects, detects, and corrects malware faster with a new anti-malware engine that is efficient across multiple devices and operating systems ▪ Ensures safe browsing with web protection and filtering for endpoints ▪ Integrated firewall uses reputation scores to protect endpoints from botnets, DDoS, APTs, and suspicious web connections ▪ Actionable threat forensics help with understanding threats and reacting more quickly	▪ Collaborative, advanced threat defenses and visibility into advanced threats help automate and speed response times ▪ Real-time intelligence sharing with multiple endpoint defense technologies provides better protection against targeted attacks and zero-day threats ▪ High performance, with minimal impact on user productivity ▪ Stronger forensic data helps IoT device manufacturers harden security policies
Connections		
Network security		
McAfee Advanced Threat Defense	▪ Innovative, layered approach to detection of stealthy, zero-day malware provides the strongest advanced malware security protection on the market ▪ Tight integration with McAfee network defenses enables instant sharing of threat information across the environment, enhancing protection and investigation ▪ Flexible, centralized deployment options support all types of networks	▪ Closes the gap from encounter to containment and protection across the entire IoT network
McAfee Network Security Platform	▪ Next-generation intrusion prevention system (IPS) employs layered signature-less technologies to identify malicious traffic and defend against never-before-seen threats ▪ Combines real-time McAfee Global Threat Intelligence (McAfee GTI) feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks ▪ Provides advanced threat prevention and application awareness in a single security decision engine ▪ Scales to speeds of more than 40 Gbps with a single device to meet the needs of demanding networks ▪ Integration with McAfee ePO software incorporates device details, user information, endpoint security posture, vulnerability assessments, and other rich information to help IoT device manufacturers understand threat severity and business risk factors	▪ Unmatched protection against advanced threats ▪ High performance and high availability ▪ Intelligent security management ▪ Visibility into applications, users, and devices

Devices	Features	Benefits
Web security		
McAfee Web Protection	▪ Layered threat detection technologies offer the most advanced protection from zero-day threats and malicious attacks ▪ Combines features of McAfee Web Gateway appliance with McAfee Web Gateway cloud service into a single subscription ▪ Number one-rated McAfee Gateway Anti-Malware Engine provides proactive behavioral analysis that inspects content in real time ▪ McAfee GTI powers web reputation and categorization, which assign a risk score that administrators can use to apply "permit" or "deny" access policies ▪ McAfee Client Proxy protects and controls web access for mobile users ▪ Deployment options: on premises, in the cloud, or hybrid ▪ McAfee ePO software and McAfee Content Security Reporter work together to provide detailed information on web usage to help with policy enforcement and compliance	▪ Advanced, top-rated protection against web-borne threats ▪ Controls for mobile devices and users help IoT device manufacturers provide more robust security for their connected products ▪ Flexible deployment options and high availability ▪ Simplifies compliance
McAfee Global Threat Intelligence	▪ Extracts threat intelligence from millions of global sensors on customer-deployed McAfee endpoint, web, and network products ▪ Aggregates threat intelligence from multiple Cyber Threat Alliance partners and public sources ▪ Integrated with numerous McAfee security solutions	▪ Provides timely threat intelligence to protect IoT device users from both known and emerging cyberthreats ▪ Enables McAfee products to work together, based on the same robust, near real-time threat data ▪ Closes the threat window and reduces probability of attack
Intel Intelligent Gateway for IoT	▪ Enables seamless interconnectivity of industrial infrastructure devices and enables secure data flow between devices and the cloud ▪ Ensures that federated data generated by devices and systems can travel securely and safely from the edge to the cloud and back—without replacing existing infrastructure	▪ Allows IoT devices to securely access and make use of valuable data previously hidden in non-connected legacy systems ▪ Enables building of scalable solutions with standards-based interfaces to securely connect and aggregate data from the edge to the cloud
The Cloud		
Host intrusion prevention		
McAfee Host IPS for Servers	▪ Enforces broad intrusion prevention system and zero-day threat protection across the network, applications, and execution ▪ Defends servers that house vital information assets from data loss ▪ Integrates with McAfee Global Threat Intelligence to protect servers against advanced threats (botnets, distributed denial-of- service, and emerging malicious traffic) before attacks occur ▪ Specialized protection for web and database servers ▪ Vulnerability shielding automatically updates signatures to protect endpoints against attacks resulting from exploited vulnerabilities ▪ Protect and manage servers with the McAfee ePO console and simplify compliance with easy-to-use reporting and forensics	▪ Maintains uptime and business continuity for mission-critical servers, which is essential for critical infrastructures ▪ Simplifies patching to close the window of vulnerability and lower operational costs ▪ Saves time and cuts costs with centralized management

Devices	Features	Benefits
Database security		
McAfee Database Activity Monitoring	▪ Provides visibility to external threats, insider threats, and threats within the database ▪ Prevents intrusion by terminating sessions that violate security policy ▪ Enables customization of policy to meet industry regulations ▪ Logs access to sensitive data, including all transactions, providing a reliable audit trail	▪ Helps IoT device manufacturers protect their most valuable and sensitive data from external threats and malicious insiders ▪ Stops attacks before they do harm, thereby minimizing risk and liability ▪ Easy to deploy on most IT infrastructures, including the cloud and virtualized environments

McAfee Data Center Security Suite for Databases	▪ Combines multiple McAfee technologies to protect against today's advanced, stealthy threats that target business-critical databases:
	  ▪ McAfee Vulnerability Manager for Databases automatically discovers databases and vulnerabilities
	  ▪ McAfee Database Activity Monitoring offers complete visibility into database activity, including privileged users
	  ▪ McAfee Virtual Patching for Databases protects against breaches prior to applying vendor patch updates
	▪ Customization enables automatic discovery, monitoring, and security management for databases
	▪ Detects and protects in real time, with no database downtime
		▪ Provides IoT device manufacturers with an extra measure of protection for sensitive user data stored in databases
		▪ Makes it easier to demonstrate compliance

Security information and event management		
McAfee Enterprise Security Manager	▪ Advanced SIEM solutions deliver real-time understanding of the world outside through threat data and reputation feeds and views of internal systems, data, risks, and activities ▪ Prioritized and actionable real-time and historical information speeds time to detection, protection, and correction ▪ Advanced analytics and data enriched with contextual information enable better understanding of threats and make triage more accurate ▪ Information is heavily indexed, normalized, and correlated to detect a wider range of risks and threats ▪ Embedded compliance framework simplifies compliance	▪ Provides critical threat information in minutes, not hours, to allow informed risk-based decisions faster ▪ Optimizes and streamlines security operations, with a centralized view of security posture, compliance, and events that require investigation
Centralized Management		
McAfee ePolicy Orchestrator	▪ Single-pane-of-glass security console provides centralized security management, visibility, and reporting for IoT device manufacturers ▪ Provides real-time event monitoring, automated reporting, alerting, analytics, and customizable dashboards	▪ Enables manufacturers to deploy software and automatically manage configurations and policies, all from one centralized location ▪ Automation capabilities help streamline management tasks, resulting in reduced operational costs and increased efficiencies

Use Cases

Medical devices

From electrocardiograms to glucometers to healthcare mobile apps, the demand for networked IoT devices in the medical setting is exploding. Healthcare organizations typically use Wi-Fi, Bluetooth, ANT+, and the cloud to enable connectivity for these devices. While IoT presents an opportunity to deliver patient care more effectively and efficiently, it also potentially exposes healthcare organizations to compromise. In 2015, there were 253 healthcare breaches, representing a combined loss of 112 million records.

Challenges:

Medical device manufacturers need to:

- Secure their products against the constant threat of internal and external data breaches, ransomware, and other advanced attacks
- Ensure their products conform to strict regulatory compliance mandates dictated by the Health Insurance Portability and Accountability Act (HIPAA) and the requirements for medical devices issued by the US Food and Drug Administration (FDA)

Solution: McAfee Medical Suite

- **McAfee Complete Data Protection Suite:** This solution helps medical device manufacturers protect against data theft by automatically encrypting medical files and folders on the fly for mobile storage devices and cloud storage.
- **McAfee Application Control:** An intelligent and adaptive whitelisting solution efficiently and automatically blocks unauthorized applications and executables—including Java apps, ActiveX controls, scripts, and specialty code—on servers, corporate desktops, and fixed-function medical devices without labor-intensive signature updates or application list management. It also leverages McAfee GTI for global reputation threat intelligence on files and applications, real-time behavioral analytics, and automatic immunization of endpoints, including medical devices, from new malware.
- **McAfee Device Control:** Monitors and specifies what data can be transferred from PCs and laptops to removable media, such as USB drives, Apple iPods, Bluetooth devices, and recordable CDs and DVDs. It also provides comprehensive device management capabilities to control and allow or block copying of certain types of data to removable storage devices. This helps maintain compliance without hindering the flow of vital patient information in a clinical environment.
- **McAfee ePO software:** All of these technologies are fully integrated with the McAfee ePO management console, which provides convenient, single-pane-of-glass visibility and management and customizable reporting for compliance accountability.

Retail (POS/ATM)

In the retail business, security issues, such as breaches and unscheduled downtime, can impact customer confidence and the bottom line. Point-of-sale (POS) systems, kiosks, ATMs, and other embedded systems are all attack vectors. In addition, compliance with federal regulations make creating a retail device secure much more daunting. There are cost-effective, quick-to-deploy software solutions that resolve software security, change control, and compliance issues for the lifetime of retail systems.

Challenges:

Retail device manufacturers need to:

- Maintain the integrity of their POS or ATM systems to reflect the "gold standard."
- Defend against known and zero-day security threats, which are the main causes of in-field breakage or unavailability. Antivirus, which degrades performance on these systems, is insufficient.
- Simplify compliance auditing. Currently, this is a cumbersome process with ineffective results.
- Secure ageing systems. The product lifespan of retail systems can be 10 years or more, making it difficult to defend against the constant barrage of threats to these older systems.
- Find a more efficient way to perform patching and updates, reduce urgency of patching, and ensure that only authorized changes are made. Often, this requires having a technician on the scene, which can be costly and time-consuming.

Solutions

- **McAfee Embedded Control:** This small-footprint, low-overhead solution provides essential "deploy-and-forget" security for POS and ATM systems, which can be integrated into devices by IoT device manufacturers. It converts vulnerable embedded systems that are built on commercial operating systems into black boxes, so that they operate much like closed proprietary operating systems. McAfee Embedded Control prevents the execution of any unauthorized program that's on a disk or is injected into memory and prevents unauthorized changes. Through dynamic whitelisting, only authorized code is allowed to run. It also integrates with Intel IoT Gateway, which enables connectivity between new IoT systems and legacy systems. Through IoT Gateway, security solutions can be applied across the board.
- **McAfee Integrity Control:** Blocks unapproved changes and unauthorized applications that may be malicious and may compromise the security of POS and ATM systems. Out-of-policy changes that are attempted are blocked, and files and directories are checked regularly to ensure their integrity. Compliance is made easier, as administrators have complete and continuous visibility to all changes, including applications used to make the change. McAfee Integrity Control is transparent to the user and has minimal impact on IoT device performance.

- **McAfee ePO software:** Provides complete, centralized visibility and management of IoT devices. McAfee ePO software also generates reports produced by McAfee Integrity Control to help IoT device manufacturers meet audit and compliance requirements. These are fully accessible via a web-based interface.

Factory floor/industrial applications

- Industrial controls systems (ICS) are essential to the effective management of every type of distributed control system. They need to run uninterrupted and unimpeded. However, these systems are not isolated and air-gapped like they were in the past. They are now connected to internal and external IP networks and corporate IT infrastructures. As a result, these systems are more vulnerable to hackers and more sensitive to the implementation of security technologies, increasing the probability of service interruption. At times, ICS systems are linked to unauthorized devices in the plant and the field. Industrial control systems are high-value targets for theft-of-service attacks and extortion, with potentially devastating consequences for production and distribution processes.

Challenges:

Industrial control manufacturers need to improve security because:

- Embedded devices in this environment lack adequate security to protect against complex threats
- Many legacy systems are unpatchable.
- Typically, ICS systems have poor password protection.
- Malware injections in this environment often begin with less critical network segments and quickly migrate to more mission-critical segments, thereby potentially jeopardizing the entire IoT production and distribution.
- Human machine interfaces (HMI) and databases have few security controls, modems often have open ports, and wireless communications are not adequately secured.

Solutions:

- **McAfee Embedded Control:** Ensures that sensors and fixed function IoT devices are locked down. McAfee Embedded Control can be deployed in the master image before IoT devices are deployed or shipped. Unauthorized changes by hackers, rogue employees, or well-meaning employees are blocked. The product allows IoT device manufacturers to create an application whitelist specifically for the system. Unauthorized programs are not allowed to run, and the need for patching is reduced. Change control capabilities allow only authorized changes.
- **McAfee Integrity Control:** Combines dynamic whitelisting and change control technology to ensure that only trusted applications run on fixed-function devices. IoT device manufacturers can control the "who, how, when, and what" of changes to mitigate malicious or accidental system modification. Dynamic whitelisting also prevents execution of unauthorized

code and malware, even in memory. Whitelisting—which consists of a list of known, good applications and processes—is advantageous, because it requires fewer updates and has a smaller footprint than blacklisting, which constantly requires updates to protect against the growing list of malicious executables.

- **McAfee ePO software:** This single-pane-of-glass management console provides full visibility of security events to any device. McAfee ePO software is integrated with the McAfee Enterprise Security Manager SIEM solution, which provides crucial threat information, swiftly shrinking the time to protection and remediation for IoT devices.

Learn More

Find out how McAfee products and solutions can help you create a more secure IoT experience for your customers. Visit: **https://www.mcafee.com/embedded**.

1. http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10
2. http://www.gartner.com/newsroom/id/3165317
3, http://diginomica.com/2016/10/05/a-massive-iot-security-breach-hits-the-web-how-should-enterprises-respond/

McAfee Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com