Securing the Internet of Things

OEM capabilities assure trust, integrity, accountability, and privacy.

The number of Internet-connected smart devices is growing at a rapid pace. According to Gartner, the Internet of Things (IoT) “will grow to 26 billion units installed in 2020, representing an almost 30-fold increase from 0.9 billion in 2009.”¹ The IoT is already transforming industries and opening the way to new business models focused on monetizing the explosion of services based on continuous access to real-time data and analytics. The IoT is unprecedented in scope and scale, and securing it is extremely critical. With more than three decades of experience delivering comprehensive security and control solutions, McAfee, part of Intel Security, is committed to ensuring that the IoT and those who use it achieve the full value of interconnected systems and knowledge.

A New Security Architecture for the Next Big Thing

Intelligent Internet-connected devices control everything from home security to national security, personal health and fitness to lifesaving medical devices, and biometric-sensing airport kiosks to aerospace manufacturing and air traffic control systems. Innovation abounds as creative uses for connected devices, applications, and data continue to emerge. However, the Internet-connected intelligent devices that run and manage our world (often with little or no human intervention) no longer benefit from the “air gaps” created by secure private networks. As these and other IoT systems flood the Internet, they must be protected from malware, hacking, spyware, and performance-corrupting activity.

We understand the transformative power of the IoT and are committed to helping OEMs ensure the security of these interconnected systems. We are working in close partnership with leaders in computing innovation and embedded operating systems to create a security architecture that:

- Addresses the expanded requirements for trust, solution integrity, accountability, and privacy that span every layer of the IoT: devices, connections, the cloud, and data centers.
- Unleashes the power of IoT by providing long-term assured functionality and other core security capabilities for the vast array of current and future IoT uses cases.
- Delivers innovation and confidence through the security expertise and technological prowess of McAfee, the world’s largest dedicated security company; Wind River, an embedded computing leader for over 30 years, delivering OS software to more than a billion products worldwide; and Intel, a world leader in computing innovation.

IoT Architectural Challenges

Given the diversity and scale of the IoT, new 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 the 85% of 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 unknown security challenges and use cases of tomorrow.
Securing the Internet of Things

Designed for the Internet of Things
To accelerate IoT innovation and ensure continued acceptance, device-to-device computing must become more secure in the face of increasing security challenges. McAfee® security architecture—built into Intel® Security products—protects OEM device integrity to ensure devices perform as intended without corruption and ensure data security regardless of location. This protection spans a broad range of systems, from resource-constrained embedded systems to next-generation intelligent devices and traditional computing environments. All existing and future systems must be interoperable, manageable, and secure, while adhering to industry standards.

Unleash the Power of the IoT
Innovative OEMs are already benefiting from the power of the IoT by transforming entire industries—from energy and healthcare to retail, manufacturing, and transportation. However, today's successes have only scratched the surface. According to Gartner Research, "IoT product and service suppliers will generate incremental revenue exceeding $300 billion, mostly in services, in 2020. The result will be $1.9 trillion in global economic value-add through sales into diverse end markets." The McKinsey Global Institute concurs, predicting IoT will have the broadest economic impact of all disruptive technologies, potentially in the area of $36 trillion in operating costs.

To participate in this incredible opportunity, OEMs must maintain the highest possible levels of confidence, integrity, and assured functionality with intelligent devices that include integrated self-monitoring and self-healing capabilities. Equally important, they must be able to accommodate changing business models and unforeseen use cases over the extended lifespan of devices that typically last more than 10 years. To enable these capabilities and accelerate OEM time to market/time to money, we do the following:

- Deliver pre-tested, ready-to-deploy application and hardware combinations.
- Provide a connected architecture that enables products to learn from each other and respond collectively to security threats.
- Solve information technology and cloud services challenges in connecting both legacy and next-generation systems to new and future services.

Innovate with Confidence
Security is our only business. With more than three decades of experience developing comprehensive solutions for the most demanding digital environments, we are uniquely qualified to provide the performance-grade capabilities needed to support the complexity and massive scale of the IoT. Only Intel Security brings these capabilities to OEMs and solution providers seeking to build long-term strategic partnerships:

- **Breadth of portfolio**—Our extensive portfolio spans both on-premises and cloud-based endpoint security, network security, and risk and compliance solutions.

- **Research and development**—Because security isn’t about designing for today’s threats, but a never-ending responsibility to defeat future threats as well. We have made a long-term commitment to research and development innovation focused on the security of the IoT.

- **Industry collaboration from trusted leaders**—Intel Security works closely with Intel, Wind River, and other industry leaders to build and continually enhance the secure platform for today and the future.

---

"Machine-to-machine connected devices have increased 300% over the past five years.”
—McKinsey Global Institute
Vertical market experience—We have extensive experience meeting the critical infrastructure needs in demanding vertical markets such as transportation, national defense, industrial automation/control, and medical imaging systems. We have a long track record of protecting devices and data from the endpoint to the server to the cloud across multiple environments.

Supplier stability—McAfee and Intel deliver proven solutions with the long lifecycle support required by OEMs and developers.

Security Connected for the Internet of Things
As the world’s leading dedicated security company, we provide today’s most comprehensive security portfolio to address the complex issues and scalability of the IoT. This portfolio helps OEMs deliver interoperable solutions that span every level of the IoT, from devices and connections to the cloud.

Devices
Application and change control
- **McAfee Embedded Control**—Self-sustaining device integrity is essential to ensuring system availability while minimizing ongoing support and maintenance costs. McAfee Embedded Control provides industry-leading whitelisting, change control, and memory protection to lock down any IoT device while still allowing essential updates.
- **McAfee Integrity Control**—Many IoT devices will still require monitoring, management, and tight policy enforcement. This solution offers all of the advantages of McAfee Embedded Control plus tight integration with McAfee ePolicy Orchestrator® (McAfee ePO™) software. McAfee ePO console integration streamlines administration of distributed devices, helps automate security policy control, and simplifies compliance reporting.

Data security
- **McAfee Endpoint Encryption**—IoT devices will increasingly share sensitive customer data, analytics, and real-time operational control information. This solution provides protection and strong access-control of all data during capture, transit, and storage.
- **McAfee Device Control**—IoT applications interact with new device and media types. McAfee Device Control prevents unauthorized use of removable media to protect sensitive data on any IoT device.

Content security
- **McAfee Embedded Reputation software development kit (SDK)**—IoT devices and applications must understand the reputation of every device, web address, and user they interact with. The McAfee Embedded Reputation SDK allows OEM devices and software to benefit from real-time McAfee Global Threat Intelligence data.

Virus protection and remediation
- **McAfee Embedded AntiVirus**—IoT systems require comprehensive protection against malware, spyware, and viruses. This solution brings highly acclaimed McAfee antivirus protection to any embedded system.

Hardware-assisted security
- **McAfee Deep Command**—Securing the IoT requires new levels of hardware-assistance that extend beyond operating systems by leveraging chip-level security capabilities. McAfee Deep Command allows remote remediation and encryption management beyond the operating system.

McAfee Solutions Provide Effective Protection at Every Level
Device Level:
Protect 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.

Connection Level:
Ensure secure application, traffic, and data security in transit through every type of wired and wireless network connection. A new class of intelligent gateway solutions, developed by McAfee, Intel, and Wind River, offers secure interoperability with legacy systems while providing common interfaces and seamless communication between devices and the cloud, enabling secure connectivity between a “systems of systems.”

Cloud Level:
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.
Business Brief

Connections

Network security

- **McAfee Advanced Threat Defense**—IoT systems and software will continue to morph into new “things.” So will malware. McAfee Advanced Threat Defense provides advanced detection for stealthy, zero-day malware. The solution finds advanced malware and integrates with McAfee network security solutions to freeze the threat.

- **Network Security Platform**—The explosion of “things” connecting to the Internet makes intrusion prevention an essential capability. McAfee Network Security Platform discovers and blocks sophisticated threats. It moves beyond mere pattern matching to defend against stealthy attacks with extreme accuracy and scales to speeds of more than 80 Gbps.

- **McAfee Next Generation Firewall**—The IoT will dramatically increase traffic crossing the perimeter of every enterprise. Enterprise-scale availability, manageability, and performance will be key capabilities for every firewall moving forward, as will deployment flexibility and anti-evasion security effectiveness. McAfee Next Generation Firewall sets the standard in all of these areas.

Web security

- **McAfee Content Security Suite**—Web-connected content will grow exponentially as new devices and services connect to the IoT. This suite bundles McAfee Web Protection, McAfee Email Protection, McAfee Network Data Loss Prevention Prevent, and McAfee Device Control into a single-suite purchase to protect users and data from inbound and outbound threats.

- **McAfee Web Protection**—The IoT requires a layered security approach. This solution combines numerous threat technologies to provide in-depth web security. From opening content and scanning active elements in real time to comprehensive signature-based coverage and web reputation, McAfee Web Protection provides optimal security and performance.

- **McAfee Global Threat Intelligence (McAfee GTI)**—In a world where everything is connected, threats evolve and spread very quickly. McAfee GTI is a comprehensive, cloud-based threat intelligence service that protects against cyberthreats. McAfee GTI offers the broadest threat data, most robust data correlation, and most complete product integration in the industry. It works in real time, 24 hours a day, and discovers and protects against evolving threats on an ongoing basis.

- **Intel Intelligent Gateway for IoT**—The IoT must allow secure, automated interconnectivity between both emerging and legacy devices and systems. A new class of intelligent gateways from Intel provides integrated and pre-validated hardware and software from McAfee and the Wind River Intelligent Device Platform that allows users to securely aggregate, filter, and share data among the IoT’s system of systems.

The Cloud

*Host intrusion prevention*

- **McAfee Host Intrusion Prevention for Server**—Embedding integrated intrusion prevention systems capabilities into IoT devices provides proactive protection against zero-day threats, including immediate alert notification, when necessary.

*Database security*

- **McAfee Database Activity Monitoring**—Vast amounts of data must be stored and analyzed to leverage the full value of the IoT. McAfee Database Activity Monitoring protects valuable data by monitoring activity on each database server and terminating malicious behavior in real time.

Why OEMs Embed McAfee Security in Their Solutions

We offer tangible benefits to OEMs looking to embrace rapidly evolving IoT opportunities 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.
• McAfee Data Center Security Suite—The IoT makes databases in the cloud even more valuable targets that must remain secure and compliant. This suite combines McAfee Database Activity Monitoring with McAfee Vulnerability Manager for Databases to extend visibility into database security posture, with detailed risk assessments across more than 2,700 vulnerability checks and expert remediation recommendations.

Application and change control

• McAfee Embedded Control—Trust, integrity, accountability, and privacy are serious concerns in cloud and shared data center environments. In the age of the IoT, these issues are magnified. Embedding device integrity into IoT systems using McAfee Embedded Control can enforce and validate trust using industry-leading whitelisting, change control, and memory protection to lock down systems and applications in multitenant environments.

• McAfee Integrity Control—As IoT systems multiply, keeping them up to date and compliant will be growing challenges, especially in multitenant cloud environments. McAfee Integrity Control leverages the McAfee ePO console to provide visibility and control of software installed on IoT devices. This combined solution can also eliminate the need for patching by providing compensating control for audit environments, greatly reducing support costs.

Security information and event management (SIEM)

• McAfee Enterprise Security Manager—Interdependent IoT systems produce billions of events that must be monitored and quickly correlated to detect abnormal activity. This leading SIEM solution provides intelligent situational awareness, response, and reporting for a complete picture of security activity.

Centralized Management for the IoT and Traditional IT Systems

McAfee ePO software provides a single security management and reporting console for the entire McAfee security solution portfolio, spanning embedded devices, laptops, workstations, and servers. This powerful web-based console helps you easily deploy software and automatically manage configurations and policies from a single location. It also lets you monitor events and generate reports automatically. McAfee ePO software provides monitoring, reporting, alerting, analytics, and customizable dashboards, along with process automation capabilities that streamline routine management tasks.

Learn More

New IoT opportunities present themselves every day as innovative applications, use cases, and ecosystems emerge. Make certain your devices have security, trust, and manageability built in from the start to thrive in these new markets. Contact a sales representative for in-depth insights into the exciting solutions architecture and security capabilities offered by McAfee, Intel, and Wind River.

2. Ibid.