Solution Brief

KIOSK and Intel Security Offer the Enhanced Security Suite

Building greater security, compliance, and trust into every self-service interaction.

Kiosks offer consumers the ultimate convenience while driving significant self-service cost savings to deployers. To make customers' lives easier, these devices may live beyond corporate network perimeters on the front lines of the new cyberattack environment. As attacks on connected devices continue, smart businesses are seeking a proactive approach to self-service security that will protect their customers and their brands. Fortunately, there is a proven way to fortify these devices with advanced security and compliance protection—even for devices already in service.

The Combined Expertise of Two Market Leaders

Intel Security offers an unmatched portfolio of security technologies and a 30-year history of securing the world's most demanding digital environments. As the world's leading custom self-service solution provider, KIOSK Information Systems (KIOSK) has a 20-year track record of providing complete solution services across the most dominant self-service vertical markets. KIOSK understands the need to ensure trust, confidence, and compliance for every transaction that occurs on the devices it designs and manufactures. That's why KIOSK has chosen Intel Security, the leader in embedded security protection, to address this critical need.

Enhancing Security in an Insecure World

Intel and KIOSK Information Systems have introduced the first-of-its-kind Enhanced Security Suite to add advanced security and compliance protection to self-service devices. This optional enhancement secures and differentiates your self-service platform while addressing today's most pressing customer issues.

Ensure device integrity with change control enforcement

Every self-service appliance—from bill payment and ticketing systems to healthcare and banking kiosks—share a common need: the device must remain available, and the system must run with unfailing integrity.

The Enhanced Security Suite at a Glance

- Prevent unauthorized access by applications and code, making the devices malware and tamper-resistant.
- Ensure that only authorized software is permitted to execute on the device using dynamic whitelisting.
- Minimize performance impact with a low-overhead solution that requires marginal use of the device's CPU resources.
- Comply with security standards, such as PCI-DSS, HIPAA, and other industry-specific mandates.
- Control support costs, patching updates, system downtime, and management throughout your devices' entire lifecycle.

KIOSK Information Systems

intel Security

The Enhanced Security Suite includes McAfee® Embedded Control software, which maintains the integrity of self-service systems by only allowing authorized code to run and authorized changes to be made. This small-footprint, low-overhead solution creates a dynamic whitelist of authorized code on the embedded system. Unlike antivirus protection, whitelisting provides complete malware protection without the need for signature updates. Once the whitelist is created and enabled, the system is locked down to the authorized baseline—no program or code outside the authorized set can run, and no unauthorized changes can be made. This unique whitelisting solution allows self-service device operators to:

- Control what software is installed to help maintain a consistent state.
- Reduce patching frequency to minimize outages and reduce support costs.
- Enforce software change policy to attain more control.
- Monitor file integrity.

Antivirus + Whitelisting = Better Protection

In addition to antivirus protection, which detects and remediates malware from the system, the Enhanced Security Suite benefits from whitelisting, which prevents malware or any unauthorized files from executing. Running antivirus and whitelisting together provides layered security protection for systems with ample computing resources.

Smart Prevention Simplifies Compliance

Maintaining regulatory compliance in self-services device environments can be an arduous task. The Enhanced Security Suite addresses many requirements in sections one, three, five, six, 10, and 11 in PCI-DSS 3.0, as well as specific HIPAA requirements for administrative safeguards, technical safeguards, and physical safeguards.

As many kiosks require credit card transactions and increasingly sophisticated services, regulators are stepping up compliance requirements. The Enhanced Security Suite removes much of this complexity with proven solutions that address the most difficult-to-satisfy qualified security assessors (QSA) requirements and help make your devices compliant and audit-ready.

The Enhanced Security Suite provides proactive, low-administrative protection that satisfies section five of PCI DSS 3.0. This modular suite allows individual protections to be activated as needed. For example, some QSA auditors insist that antivirus protection must supplement whitelisting. For those situations, Intel Security offers industry-leading virus-scanning capabilities that scan and block viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage device availability. This antivirus technology scans faster, uses less memory, requires fewer CPU cycles, and protects users better than any other anti-malware product on the market. In fact, NSS Labs gave the solution the highest overall exploit protection score of any vendor tested.

Stateful firewall protection

Self-service devices typically connect via the Internet. As such, these systems require protection from Internet intrusion. With the Enhanced Security Suite, you control applications that can access self-service devices to stop network-borne attacks and downtime. You can deploy and manage firewall policies based on location to deliver complete protection and compliance with regulatory rules.

- Gain deployment flexibility, allowing security integration during the manufacturing process or with existing devices in the field.
- Simplify compliance audits and reporting using dashboards, reports, and a tamperproof system of record.

Audit and policy compliance

The Enhanced Security Suite provides dashboards and reports that help you meet compliance requirements. These reports and dashboards are generated through the McAfee® ePolicy Orchestrator® (McAfee ePO™) console, which provides a web-based user interface for users and administrators. The solution delivers integrated, closed-loop, real-time compliance and audit, complete with a tamperproof system of record for the authorized activity and unauthorized attempts.

Bringing Peace of Mind to Convenience

Today's self-service device operators face unprecedented challenges of security, device management, and compliance regulations. Forward-thinking device operators are seizing this opportunity by adding advanced security capabilities into their devices. To learn more about the Enhanced Security Suite, talk to your KIOSK representative today.

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee, the McAfee logo, ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2015 McAfee, Inc.
61950brf_kiosk-enhanced-sec-suite_0515

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com