SEPTEMBER 2012

By: Jared Weiner – *Analyst*
With: Chris Rommel – *Vice President*

CASE STUDY | McAfee & Xerox

A Partnership for Extending Endpoint Protection to Intelligent Devices

VDC research

The Situation

The proliferation of intelligent, connected devices has brought countless conveniences to today's workplace. The benefits of intelligent devices are widespread, and include features such as mobile access and email-based (and driverless) printing. However, these conveniences come with considerable risk. As more and more connected devices enter the enterprise with each receiving, storing, and/or communicating potentially sensitive corporate, customer, or personal data, hackers and other criminal entities are becoming increasingly interested. A wide range of devices, including peripherals and office equipment, have become the targets of malicious attacks, with hackers able to identify and exploit the vulnerabilities they have discovered within these products.

These vulnerabilities exist for several reasons. First, OEMs who make office equipment historically have not focused on security, despite the increasing connectivity requirements of their devices. In many cases this may be due to benign neglect or a perceived lack of risk. As such, connected office equipment has not provided IT managers with the same level of security and system management capabilities typically found in traditional PCs or servers.

Many enterprises using connected office equipment also have not acknowledged the risks inherent in deploying unprotected (or under-protected) devices. Even for those organizations that have recognized these risks, many have struggled to implement security technologies due to the challenges associated with security management across the many disparate types and brands of office equipment in use.

As a result, any built-in security within connected office equipment – devices such as printers, copiers, fax machines, and multi-function printers (MFPs) – is not typically integrated with broader enterprise security tools. Office equipment security strategies have been inconsistent, often isolated, and generally not connected with broader enterprise security policies. Consequently, malicious entities may not only be able to gain access to data stored on or communicated by the device itself, but may also be able to use a printer or MFP as an access point to attack the entire network infrastructure.

These issues are combining to create a perfect storm: a large and growing number of machines with access to sensitive data, connectivity with enterprise networks, and limited security capabilities. Considering the volume and nature of the sensitive data either on the network or the device itself (credit card numbers, customer and employee records, company financials, and even intellectual property) a security breach in this formerly innocuous area now has the potential to be extremely costly. The repercussions of such breaches range from financial losses to legal consequences and potentially irreparable reputation damage.

Unfortunately, a costly breach is possible. Sensitive data is often stored on a network left vulnerable to attack or failure due to a weak endpoint easily turned into a point of access. With security threats on the rise, there has been a growing desire to improve not only the management of embedded devices in the enterprises, but also the security policies associated with them.

Office equipment security strategies have been inconsistent, often isolated, and generally not connected with broader enterprise security policies.

The Solution

Xerox executives examined these mounting threats and concluded that it was time to combine security technology and office equipment. After evaluating the multitude of potential partners in the security solutions market, Xerox was drawn to the McAfee brand, track record in embedded (McAfee technology is widely used in a variety of devices, such as ATMs, point-of-sale, medical, and industrial control system devices), and position as a global leader in security technology. Also attractive was McAfee's relationship with Intel, by whom it was acquired in early 2011. Intel, through initiatives such as Intel Virtualization Technology and Intel Trusted Execution Technology, has also shown an ambitious long-term vision and integrated product roadmap to improve embedded device security. Ultimately, Xerox recognized the opportunity to establish a new standard in secure office equipment through the strategic alliance (and combined brand recognition) of well-respected market leaders.

After conducting a collaborative assessment and an evaluation of various device profiles, McAfee and Xerox decided to redefine the model for office equipment protection, specifically around MFPs. MFPs, while embedded devices with both multiple users and multiple administrators, in fact have many properties (network protocol stacks, encryption, web server connections, etc.) more typically associated with more advanced IT systems. However, MFPs are much more diverse than typical PCs, particularly with regard to the underlying OS and other internal components. As such, traditional PC and server security controls are not optimized for MFPs. The team's solution was to establish a new paradigm for MFP security; one that doesn't rely solely on PC/server security controls while also fitting with the low deployment and maintenance costs required for embedded devices.

Ultimately, the McAfee/Xerox partnership came to revolve around the integration of McAfee Embedded Control technology and McAfee ePolicy Orchestrator (ePO) security management software within Xerox devices.

McAfee Embedded Control, based on technology obtained through McAfee's 2009 acquisition of Solidcore Systems, helps to protect devices from malware infections and other forms of attack through the formation and management of whitelists. A whitelist defines the list of files that are permitted to implement software changes and blocks everything else, thus helping to reduce change-related outages and other compliance violations. A blacklist, conversely, requires a user to be aware of all potential threats, which is an overwhelming challenge, given the ever-changing nature of viruses, spyware, and other malicious software. Furthermore, the blacklist paradigm is simply harder to deploy in embedded systems given the diverse hardware and OS combinations inherent in these devices.

Through the use of ePO, Xerox intends to ease the integration of its products with its customers' enterprise infrastructure, thus increasing visibility, operational efficiencies, and providing additional layers of data protection. The result will be twofold: devices that are more securely connected to back-end networks, and the implementation of more consistent, integrated, enterprise-wide security policies.

The Impact

While this is certainly a compelling solution in its own right, VDC expects the impact of the McAfee/Xerox relationship to run much deeper. Through this partnership, Xerox has clearly demonstrated its commitment to being the leader in office equipment security – a commitment that VDC expects will soon become an industry standard. Until that time, however, Xerox's security initiative becomes an important competitive differentiator.

A commitment to office equipment security will become the industry standard.

By leading the charge, Xerox has claimed the first-mover advantage, both from a security policy and vulnerability protection perspective. As such, the company will have a tremendous opportunity to seize market share from its competitors, whose customers may already be in search of more robust security features. Furthermore, we believe Xerox will also have the opportunity to increase its revenue opportunity over the long run by incorporating this technology in new lines of devices as a standard feature.

Of course, this partnership benefits McAfee as well, particularly as the company aims to broaden its footprint in embedded. By collaborating with a leading OEM in another industry-specific implementation of its solutions for device security, McAfee has strengthened its reputation as a leading vendor of embedded security solutions. VDC believes that the success of Xerox's implementation of McAfee products will result in similar relationships between McAfee and leading OEMs within a variety of other embedded verticals.

Recommendations

To OEMs, security solution vendors, and enterprises across the business world, VDC offers a number of recommendations in light of the McAfee/Xerox partnership.

Security Policy & Intrusion Protection Must IncludeAll Network Endpoints

No longer can organizations ensure the security of their sensitive data solely through PC- and server-based security initiatives. Threats to embedded systems are all too real, and becoming more serious by the day. OEMs and enterprises alike can no longer afford a *"head-in-the-sand"* attitude toward device security. Xerox recognized the importance of proactively addressing security and worked with McAfee to develop a full-scale security approach. If OEMs (or their customers) fail to properly address device security until there is a costly breach, it is already too late!

No longer can organizations ensure the security of their sensitive data solely through PC and server-based security initiatives.

The McAfee/Xerox Model Should be Embraced Across All Embedded Verticals

Despite the heterogeneity that defines the embedded device industry as a whole, the basic tenets of the McAfee/Xerox relationship – collaboration and joint implementation – are applicable across a wide range of vertical market segments. The key, of course, is identifying specific pain-points and developing a tailored solution to address those concerns. The potential business models around these new security features (positioned as fundamentally required for general protection or as premium add-ons for targeted protection) are also applicable across most industry segments. While embedded security has broad applications, VDC expects that consumer electronics, medical devices, and military/aerospace applications present the best near-term opportunities.

OEMs Must Carefully Evaluate Their Specific Device Security Needs

Security can (and should) be addressed at each stage during the device development process and in any number of places within the device stack itself. In addition to solutions such as McAfee's, available software technologies that can help OEMs satisfy security requirements within their devices include automated test and verification tools, embedded hypervisors, and real-time/embedded operating systems. VDC recommends that OEMs evaluate all of the available options before moving forward with a security plan. However, the planning and evaluation phase does not stop there. Even after Xerox had selected McAfee as its strategic partner, the two companies had first identified more than 20 potential areas that could be addressed before homing in on critical areas to be the target of this initial integration. We believe this deliberate approach is essential to the efficient and effective implementation of a robust security policy.

OEMs Should Focus on Security Scalability

While evaluating the aforementioned security technologies, VDC recommends that OEMs develop a comprehensive plan for all relevant current and future product lines. However, this should be a scalable plan where different security-focused technologies are implemented in different stages so as to not overwhelm the design and development process. Specifically, we recommend that critical security features are implemented first, with additional security-related functionality added in subsequent iterations of the device or related software. Of course, the threat analysis and assessment of relevant product lines is the key part of this equation. As such, VDC also recommends that third-parties be consulted (as Xerox did with McAfee) if in-house security expertise is insufficient to effectively serve these needs.

Contact:
Mike Collette
Vice President, Sales & Enterprise Accounts
508.653.9000 x112
info@vdcresearch.com

VDC research

VDC Research Group (VDC) provides market research and advisory services to the world's top technology executives. Our clients rely on us to provide actionable insights to support their most important strategic decisions. The firm is organized around four practices, each with its own focused area of coverage including: automatic identification and data collection, embedded hardware, embedded software and enterprise mobility.

For more information about this research product, please contact:

VDC Research Group, Inc. | 679 Worcester Road | Suite 2 | Natick, MA 01760