Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 6

SaaS Security: The Sensible Solution

By Becky Bracken

It's a natural evolution, really. Now that we've unlocked the key to flinging data all over the place — from the cloud to mobile devices and back again — the next question, naturally, is how to keep that data secure while it's being flung far and wide.

Particularly in North America, the mobile-enabled workforce is taking shape. It's also what's driving the BYOD frenzy. Almost every job can be made that much easier with a mobile handheld computer — and everyone has their own brand of choice. Businesses understand that employees armed with smartphones are productive, happier and cost less to manage.

Frost & Sullivan's survey of 300 mobile and wireless decision makers revealed that while 35 percent of businesses have deployed MWFM applications, many have delayed adoption because they lack the in-house expertise to deploy. SaaS, or Security as a Service, solutions allow in-house IT departments to focus on business- and industry-specific tasks.

The question is one of security. Keeping business data in the cloud and offering many employees access to that data demands thoughtful security considerations. Security as a Service is shaping up to be an attractive solution for enterprises today to easily and cheaply solve their individual — and constantly emerging — security issues.

Infonetics reports that the mobile segment of the security client market jumped an astounding 76 percent in 2011, and predicts continued double-digit growth through 2016, five times faster than the desktop segment. Mobile security is driving the market, and the industry is turning its attention to creating the solutions.

"Coming off the spike in 2011, the perennially strong desktop-security client segment is slowing as companies turn their attention to mobile and cloud-based security solutions," noted Jeff Wilson, principal analyst for security at Infonetics Research. "More and more consumers and enterprises are using smartphones and tablets in place of traditional desktops and laptops, fueling an increase in mobile malware and the need for mobile-specific security products. As a result we expect mobile solutions to grow to over a third of the total security-client software market by 2016."

Major mobile carriers are working to meet the changing demand for mobile SaaS solutions, and rushing to partner with SaaS providers to offer customers a mobile app for smartphones to protect against malware. Verizon worked with McAfee and Asurion to develop Verizon Mobile Security, a new app for Android 2.1 and higher that protects against malware and other threats.

SaaS Comes to Play

Industry analysts and their numbers might not all agree, but the impressive growth opportunity in the SaaS market is an easy call. Gartner predicts SaaS-based delivery will see steady growth through 2015, and that global revenue will reach $22.1 billion.

"Customers are starting to buy and deploy integrated security solutions — including firewalls with mail and gateway antivirus, IPS, DLP, mobile device security, and application control — instead of standalone solutions, which is driving up the overall network-security market

but weighing down on sales of standalone content-security gateways," said Jeff Wilson. "Security as a Service and hosted security services are outgrowing product markets, and until recently, standalone content-security product sales were outgrowing integrated appliance sales."

Revenue for SaaS content-security gateways is up more than 50 percent year-over-year and is forecast by Wilson to grow 23 percent from 2011 to 2016. "Any serious player in the content-security market who doesn't currently have an SaaS offering is missing out on the fastest-growing segment," he said.

Cisco is the leader in the SaaS segment and has a strong content-security offering, including their IronPort Hosted Email Security and Cisco ScanSafe Web Security cloud services, which promise to cut spam by 99 percent. McAfee, Websense and Symantec are also leaders in the content-security sector.

SaaS offerings are also attractive for enterprise because they are easily scalable for specific vertical markets. In the case of the medical industry, which is currently undergoing a multi-trillion-dollar digital and communications revolution, service providers see a real opportunity to dive headlong into the healthcare security vertical. Verizon has just released a cloud security portfolio for the healthcare industry that is designed to meet U.S. federal Health Insurance Portability and Accountability Act (HIPAA) requirements for safeguarding electronic protected health information (ePHI).

SaaS Goes Vertical

Verizon is one of the first top-tier providers to offer these specialized services, which will include the secure storing of ePHI in its Terremark data centers. With the cloud, healthcare professionals can collaborate, share patient information in near real-time and store large volumes of data for electronic health records and radiology images. In addition healthcare organizations can centralize their data so they can operate more efficiently.

Available immediately, the new portfolio offers Verizon clients in the healthcare, insurance, pharmaceutical, and supporting industries a full range of public and private cloud services that meet applicable physical, administrative and technical security controls under HIPAA.

"Today's healthcare provider is faced with the enormous and costly burden of protecting personal health information for patients," said Dr. Peter Tippett, chief medical officer and vice president of Verizon's health IT practice. "To address this need, we are bringing to market a suite of cloud services that enables healthcare providers to secure patient data while offloading the burden of building and managing their own data centers. By enabling a connected healthcare system, we intend to transform U.S. healthcare delivery."

Frost & Sullivan's survey of 300 mobile and wireless decision makers revealed that while 35 percent of businesses have deployed MWFM applications, many have delayed adoption because they lack the in-house expertise to deploy.

SaaS Limitations

But there are limitations to SaaS offerings. First, there are regulatory concerns: some banking and financial-services regulations require that banking information remain in a specific location, making cloud storage and security a complicated issue. Second, Gartner's survey of IT decision makers found that most enterprises are comfortable with SaaS solutions for sensitive data, but not what they call "mission-critical" data.

"These results make sense, given that sharing data with a partner almost certainly means that one or more of its employees will be accessing the data, while in an SaaS scenario the data is typically only accessible to the primary customer," said Jay Heiser, research vice president at Gartner. "This year we asked about both data availability and data confidentiality policies. Survey respondents indicated 10 percent less willingness to place mission-critical data into an SaaS offering than to place sensitive data into it. They were even less willing to place mission-critical data into outsourced data centers, with over one-third of respondents saying that they do not allow it."

Security as a Service remains one of the strongest and hottest segments in the ComIT space. Smart offerings will continue to carefully consider the specific security needs of a given vertical market, and, even more importantly, the risk-management mindset of an organization. As the entire economy digitizes, scalable, affordable security will continue to be a need. SaaS is poised to be a one-size-fits-most solution that will help business IT managers sleep a little easier.