CONTENT PROVIDED BY

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

SPONSORED BY

thawte®

Securing the Cloud

As cloud usage rises, the number of threats also increases. Find out here how to identify and overcome threats to cloud security.

1105 MEDIA

Cloud usage is rising and so are the number of threats to the security and privacy of your organization's information.

BY JOHN K. WATERS

As cloud computing moves beyond the early-adopter stage, security and privacy concerns and the inherent risk of moving assets off-site are not just fears—they're real. Uncertainty about data security and privacy slowing the adoption of cloud computing existed before last year's revelations by Edward Snowden of covert government surveillance, but the scope accentuated skepticism, coinciding with the rise of cyber attacks from around the world.

"Edward Snowden's revelations were really a wake-up call for the industry about what the government can do with your data," says IDC analyst Al Hilwa. "And if the government can see your data, who else can? It's really not surprising that security concerns have slowed enterprise adoption."

"Edward Snowden's revelations were really a wake-up call for the industry about what the government can do with your data,"

–Al Hilwa, analyst, IDC

Those fears notwithstanding, they're unlikely to put a major dent in projected adoption of public cloud services in the coming years. Gartner Inc., for example, predicts cloud computing will constitute the bulk of new IT spending by 2016, and that nearly half of large enterprises will have hybrid cloud deployments by 2017. However, the results of a recent survey (**bit.ly/1ssDE9R**) by U.K.-based communications services provider BT Group of IT decision makers in large U.S. companies underscore a contradiction: 79 percent of respondents said they're adopting cloud storage and Web applications in their businesses, but they also report their confidence in the security of the cloud is at an all-time low.

Top Security Threats

Another major risk is the ease with which employees can and typically do bypass IT departments when using cloud services.

The lack of confidence is with good cause. The Cloud Security Alliance (CSA) has identified what its researchers believe to be the top nine cloud security threats. Data breaches top that list, dubbed "The Notorious Nine" (download: **bit.ly/1lEughf**). Also on that list are data loss, service traffic hijacking, insecure interfaces and APIs, denial-of-service attacks, malicious insiders, cloud services abuse, insufficient due diligence, and shared technology vulnerabilities. The company emphasized those risks at a three-day conference in September hosted jointly by the CSA and the International Association of Privacy Professionals (IAPP).

Not on that list, but another major risk, is the ease with which employees can and typically do bypass IT departments when using cloud services, says Jim Reavis, founder and CEO of the CSA. Today, anyone can use a credit card to spin up a virtual machine on Amazon or Microsoft Azure, set up a SharePoint instance via Office 365 or another third-party provider or by using free services such as Box, Dropbox, Google Drive or Microsoft OneDrive. Reavis points out that when people bypass IT when using these and other services, it undermines business-level security policies, processes, and best practices, making enterprises vulnerable to security breaches.

Another risk Reavis points to: the lack of knowledge by IT management of the scope of cloud usage in an organization. At the CSA Congress 2014, the group published the results of a survey (download: **bit.ly/1sm2VDq**) of U.S. companies, many of which drastically underestimated the number of cloud-based apps running

in their organizations. The report concludes, "Cloud application discovery tools and analytical tools on cloud app policy use and restrictions are crucial in the workplace, especially when it comes to sensitive data being used by these cloud applications. With sensitive data being uploaded and shared by these apps with authorized and unauthorized users, policy enforcement becomes a major role in protecting your data."

The report estimated with more than 8 billion Internet connected devices, a growing number of businesses may own data, but no longer own their infrastructure. "A few years from now, that 8 billion will become a quarter trillion," Reavis says. "If we lose ground on privacy and security today, we'll have a very hard time getting it back. That creates a mandate to embrace the tools and technologies that are emerging to manage and protect these resources."

"The perimeter has failed or is failing, given that data is now everywhere."

C.J. Radford, VP of Cloud, Vormetric Inc.

The proliferation of all those devices and the bring-your-own-device corporate culture has resulted in an enterprise that's more difficult than ever to protect–cloud or no cloud, says C.J. Radford, VP of Cloud at data security company Vormetric Inc.

"The perimeter has failed or is failing, given that data is now everywhere," Radford says. "If you're only focused on your perimeter, you're going to have a very hard time protecting your data. But that's where the enterprise has traditionally spent its money over the past 10 or 15 years–essentially, on building a bigger moat. The problem is, you can't build a moat around, well, everything."

Controlling Access

In an increasingly cloud-centric, perimeter-less world, enterprises must concentrate their security efforts on protecting the data itself, Radford says. His company partners with leading cloud vendors, including Amazon Web Services Inc., Rackspace, IBM Corp., and Microsoft, to provide data-at-rest encryption, integrated key management, privileged user access control, and security intelligence logging. Among other things, the Vormetric Key Management Key Agent software works with Microsoft SQL Server Transparent Data Encryption (SQL Server TDE) to help manage SQL encryption.

"Today, it's all about controlling data access," he says. "If you read any of the major breach reports, one of the ways the bad guys are

getting access to data is compromising privileged username and password credentials. They're doing it through social engineering, phishing and that sort of thing."

Not surprisingly, Radford is a strong advocate of data encryption, and he also recommends a bring-your-own-key (BYOK) approach. "You should never rely on the provider to manage your encryption keys," he says.

"BYOK means the provider can turn over your data in encrypted form, but it's useless without the key. The other thing it buys you is the ability to 'digitally shred' your data. We call that 'permanently securing your data.' That's why we always say, rule No. 1 in encryption is never lose your key."

The primary cloud security concern in the enterprise today is availability.

Encryption support is even showing up above the infrastructure level. Azure, Outlook.com, Office 365 and OneDrive, for example, are now supported by Transport Layer Security (TLS), Microsoft announced last summer. The encryption support covers inbound and outbound e-mail, as well as Azure ExpressRoute, which allows users to create private connections among Azure data.

Data encryption and data-centric solutions seem to be especially appealing to enterprises in the post-Snowden era, says Luther Martin, chief security architect for Voltage Security Inc.

Martin believes the primary cloud security concern in the enterprise today is availability.

"If you look at the data, in terms of frequency, most of the cloud incidents so far have been about service outages," he says. "The outages have been relatively short, but they can be terrifying, and there's not much an enterprise can do about them."

He also notes, however, that encryption keys present their own challenge—namely, keeping track of them. "Effective encryption key management is hard," he says, "and people often don't give it the consideration it deserves. I mean, if you lose a key, you've lost your data, too."

Fortunately, new technologies and approaches to the management of encryption keys are emerging. Martin points to so-called stateless key management, which enables on-demand key generation and re-generation, as an example.

Cryptographer Taher Elgamal, CTO in the security group at Salesforce.com Inc., believes security for the cloud is seriously lagging in an outdated IT model.

"We're not protecting the cloud infrastructure using the cloud," he says. "We're pushing products that were built to secure one environment–the enterprise network–to secure a very different environment–the cloud. Security would be a lot better in a cloud infrastructure."

"We're pushing products that were built to secure the enterprise network to secure a very different environment–the cloud."

– *Taher Elgamal, CTO in the security group at Salesforce.com Inc.*

Shielded Execution

And, yet, as CSA's Reavis has pointed out, demand for enterprise cloud security solutions is driving innovation. Microsoft, for example, has just taken what might prove to be a big step toward securing the enterprise cloud with a very different strategy.

In October, the company introduced the concept of "shielded execution," which protects the confidentiality and integrity of a program and its data from the platform on which it runs.

The concept was introduced in a white paper (download: **bit.ly/1ECPnY6**) presented at the 11th USENIX Symposium on Operating System Design and Implementation, along with Haven, a prototype of a system that provides this kind of security. According to the researchers, Haven "is the first system to achieve shielded execution of unmodified legacy applications, including SQL Server and Apache, on a commodity OS (Windows) and commodity hardware." The project aims to bypass the inherent risks of a hierarchical security architecture, in which the provider is trusted with full access to user data. The result, they wrote, will move us "one step closer to a true 'utility computing' model for the cloud, where the utility provides resources (processor cores, storage and networking) but has no access to user data."

And has the enterprise perimeter really disappeared? The researchers behind the CSA Software Defined Perimeter (SDP) project might beg to defer, if only slightly. They're attempting to define a multi-layer security model to protect the application infrastructure from network-based attacks. The idea is to integrate into a single framework some well-known security strategies, such as network access control, one-time passwords, and digital certificates, with new approaches, such as identity federation, device attestation, and geo-location. Only authenticated access to app infrastructures would be allowed in public and private clouds, as well as traditional datacenters.

The researchers behind the CSA Software Defined Perimeter (SDP) project are attempting to define a multi-layer security model to protect the application infrastructure from network-based attacks.

If they can pull it together, such a framework could thwart a range of attacks, including DDoS, man-in-the-middle, SQL Server compromises and APT hash theft, says Junaid Islam, co-chair of the SDP Research Group. Islam is also the co-founder and CTO of Vidder Inc., a company that offers its own SDP solution, which generates what it calls "dynamically provisioned perimeters."

"Connectivity in an SDP is based on a need-to-know model in which device posture and identity is verified before access to application infrastructure is granted," Islam explains.

The SDP Working Group sponsored a hackathon at the CSA conference, challenging developers to access a file server in a public cloud protected by the SDP from a different public cloud. The CSA says nearly 11 million attempts have been made as of mid-October. In that month's timeframe the SDP was yet to be hacked. R

John Waters is a freelance journalist based in Silicon Valley and is an editor at large for sister Web site ADTmag.com.

Cloud Security Report

Gain Control

What your organization can do to get cloud usage under some semblance of control and even turn issues into assets.

BY SCOTT BEKKER

The use of cloud computing and storage services can contain surprises for even the most security-conscious IT departments.

Take, for example, the most recent quarterly "Cloud Adoption and Risk Report" from cloud security vendor Skyhigh Networks. As part of its services, Skyhigh discovers cloud services in use by a company's employees. Using anonymized data across its customer and prospect base, Skyhigh determined that in the second quarter of this year, companies used an average of 738 discrete cloud services.

Now, bear in mind, these are companies diligent enough to already believe it's important to have a vendor check their network for rogue services. And how many cloud services were those IT departments already aware of on average?

"Thirty," says Skyhigh CEO Rajiv Gupta.

Another industry insider, Frank Cabri, has a name for the two groups of cloud apps. "Sanctioned" apps are the small set of cloud services that the IT department knows about and led the implementation for, says Cabri, vice president of marketing at Skyfence Networks Ltd. Those sanctioned services might include Microsoft Office 365 or Salesforce.com or Amazon Web Services (AWS). "Unsanctioned" apps are the ones the business groups or individual users installed without any IT involvement. They could be some of the same apps from the sanctioned list done on the sly or a free file sharing service set up to meet a departmental business need, or the Twitter, Evernote or Yahoo Mail accounts of individual users, accessed on occasion from the company network.

The highest-profile group of new cloud problems with significant implications for IT departments come from governments.

More Sideswipes

Unsanctioned–or shadow cloud services, as they've come to be called–are only one of the new classes of potential security sideswipes that IT departments face in the cloud.

The highest-profile group of new cloud problems with significant implications for IT departments come from governments, as revealed by reports based on the cache of U.S. National Security Agency (NSA) documents provided by Edward Snowden. In a blog post last December, Microsoft General Counsel Brad Smith went so far as to claim that "government snooping potentially now constitutes an 'advanced persistent threat,' alongside sophisticated malware and cyber attacks."

Organizations must now seriously consider whether data they store in the cloud would be a potential target for the NSA and other nations' signals intelligence agencies. Then there's the possibility of old-fashioned industrial espionage by foreign governments. One other risk category for data stored at a cloud services provider (CSP) is the possibility that the cloud provider will receive a government investigatory request for your organization's data. A CSP that fails to fight successfully to keep that customer data private and that can access the data often will be prohibited from informing the customer about the request or the data handoff.

Then there are the more traditional security concerns, equally present or sometimes amplified in the cloud. First, there's the issue of the

CSP's security procedures. The most recent Skyhigh scan uncovered 3,861 unique cloud services in use during the quarter. Only 9 percent of the services met the Skyhigh Enterprise Ready trademarked security standard. What that means is that many of the CSPs are themselves at risk of compromise by an attacker, putting their customers' data at risk. No matter the CSP's business practice, there's also always the possibility of rogue administrators at the CSP.

Another issue that arises from the use of personal cloud services on the company network is that many users will keep the same passwords for personal and business accounts, meaning that compromised credentials on a consumer service can lead to successful attacks into a corporate system.

"[Embracing cloud is] taking IT from the guard of the asylum inmates to the guide who says, 'Let me help you to do what you want to get done.' "

Rajiv Gupta, CEO, Skyhigh Networks

None of the alphabet soup regulatory requirements stop at the company firewall, either. Cloud data, known and unknown to the IT department, is subject to the same privacy, security, disclosure and data residency requirements as any of the corporation's other data.

Make It Work

While the cloud risks are real to data, brand and compliance, Gupta identifies another important risk for IT departments. "The further IT gets away from addressing the employee need, the less relevant IT gets in the eyes of users. That's a pretty slippery road," Gupta says.

A lot of cloud service usage arises in the organization because the service meets a need the IT department may not be filling. "What are employees trying to do? If my employees are using file-sharing services, they probably need file sharing.

What's the most enterprise-ready, lowest-risk service that I should allow my employees to use?" Gupta says.

Among Skyhigh customers who pivot to that approach of standardizing on a reliable service, Gupta says two surprising things happened. "As they communicated to employees that they understood [their needs], the use of all of the other higher-risk services dramatically went down because the employees [finally had] something to use. The second thing that happened was the employee satisfaction with the IT organization went up. It's taking IT from the guard of the asylum inmates to the guide who says, 'Let me help you to do what you want to get done.'"

"One thing organizations need to be aware of is that credential theft in many ways is becoming a new attack vector for these cloud apps. Once the bad actor has your credentials, it doesn't matter whether that data is encrypted or not."

Frank Cabri,
VP of Marketing,
Skyfence Networks Ltd.

For similar reasons, Cabri reports that Skyfence users often choose to leverage customized profiles for actions within cloud applications like Salesforce.com rather than a "hardline block" of certain actions. "Sometimes that's not the most graceful approach," he says.

"We understand that they want to get their tasks done, but it may expose security and compliance risks for the company. That's the general trend that we're riding. Companies no longer own the applications, the infrastructure or, often, even the device," Cabri points out.

The Cloud Security Toolbox

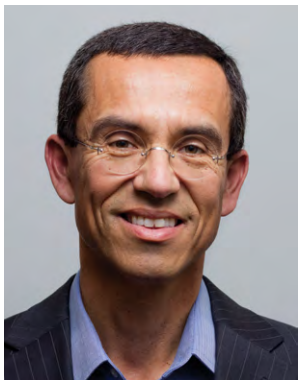
IT departments looking to strike that cloud balance between user and organizational productivity and security have a number of tools in the toolbox.

The best known is bring-your-own encryption, the kind that protects data before it gets to the CSP. "One of the top-trending inquiry topics hitting our cloud and security analysts lately are about cloud encryption for AWS and Salesforce.com," James Staten, vice president and a principal analyst at Forrester Research Inc., said in a blog post of cloud predictions for this year. "You can thank the U.S. NSA for popularizing this trend. Clients are asking for recommendations on offerings that encrypt data before it hits the cloud service and lets the enterprise control the keys."

Encryption relies on a complicated brew of technology and organizational policy, however, with many seeming solutions turning out to be "warm fuzzies" that make customers feel good, but may not protect their data. "The important thing for businesses to understand if they really want to have control over their data is that they need to do three things," says Elad Yoran, CEO of Security Growth Partners LLC and former chairman and CEO of cloud security company Vaultive Inc. "They need to ensure that their data is encrypted before it gets to the cloud provider. The second thing is that they need to have control of the encryption keys. Then they need to ensure that the data is always encrypted, meaning in use, as well as in transit and at rest."

Executed rigorously, encryption addresses a host of ills, from an IT standpoint. CSP compromised by attackers? They see only gibberish. CSP gets a National Security Letter from the FBI? The CSP can only hand over the gibberish. The FBI has to come to the customer for the key to decrypt the data. This means the customer knows it's being

targeted and can get the lawyers involved in the tried-and-true process of negotiating what gets handed over, Yoran says.



"If you look at most organizations, they don't encrypt information within their environments. If you're going to a major cloud provider and you're encrypting the information and you're keeping the keys separate, that's going to put you in a better position."

Bob West, Chief Trust Officer, CipherCloud

Encryption is no silver bullet, though, warn all the experts. "One thing organizations need to be aware of is that credential theft in many ways is becoming a new attack vector for these cloud apps. Once the bad actor has your credentials, it doesn't matter whether that data is encrypted or not," Cabri says.

Because of that, encryption must be paired with several other technologies. One is effective authentication—be i single-sign-on or two-factor authentication or some other password policy solution. On the other end is policy enforcement. "Say a user usually logs in from the Bay Area. Now they're logging in from Russia with a different end point than we've ever seen," Cabri says. "We can block access based on policy."

Auditing tools are also important and several are emerging to address the unique problems of the cloud—where a good portion of the audit trail is dark because it passes through the black box of the CSP.

A Better Risk Posture

Although an entire cluster of cloud security companies are emerging to face the challenging new security threats, their attitudes are far from gloomy about the possibility of security in the cloud.

Bob West, chief trust officer at CipherCloud, contends organizations that enter the relationship with cloud providers with their eyes open may actually be able to achieve better security than they had previously. On the one hand, vendors such as Google Inc. and Microsoft are making serious efforts to improve datacenter security, due to pressures and revelations stemming from the NSA reports.

"If you look at most organizations, they don't encrypt information within their environments," says West. "If you're going to a major cloud provider and you're encrypting the information and you're keeping the keys separate, that's going to put you in a better position. If an adversary understands your IP range, they know where the targets are. In a multi-tenant environment, that's much more difficult. I think you have a better risk posture there." R

Scott Bekker is editorial director for the 1105 Enterprise Computing Group and editor in chief of sister publication Redmond Channel Partner.

Cloud Security Report

Security Tools

The growth of employee-owned devices and use of cloud services requires advanced protection. Here are six new and emerging products worth considering.

BY CHRIS PAOLI

As the use of employee-owned devices and personal cloud services continues to rise, so does the risk of enterprise data getting into the wrong hands. Mobile device management suites are one way organizations can mitigate threats of data loss—either by a willing employee or one who's merely careless. But just as most people have multiple locks or alarm systems on their homes and buildings, IT organizations need to think the same way about protecting their data.

Fortunately, there's no shortage of technologies that can reduce the chances of your organization's data getting into the wrong hands.

Among some noteworthy new offerings worth evaluating, here are six.

1 FireHost Compliance as a Service

FireHost Inc.

If your business is in an industry that has strict data compliance requirements but lacks the staff or skills to deploy a solution, Texas-based FireHost offers what it describes as a cloud-based Compliance as a Service (CaaS). The service entrusts FireHost experts with securing your data and ensuring you're meeting such requirements as PCI and HIPAA. The service also aims to reduce the need for multiple security products.

"[FireHost CaaS] will help our customers reduce risk and avoid costs through a smaller remediation footprint."

– Kurt Hagerman, CISO, FireHost

"[FireHost CaaS] will help our customers reduce risk and avoid costs through a smaller remediation footprint and reduced technology needs," explains Kurt Hagerman, FireHost's CISO. "Because all of these services are integrated and delivered by a single provider, customers can focus on their business and leave security and compliance to full-time specialists and experts like us," he says.

The service includes incident response, forensics, security monitoring and remediation, and employs SSL encryption for all data leaving on-premises. In an attempt to alleviate concerns that come with putting all your security eggs in one third-party basket, the company has partnered with risk management firm Coalfire Systems Inc. to provide periodic, independent auditing for customers.

2 FireLayers

FireLayers Inc.

Half of all data losses are due to the use of unauthorized and malicious apps, according to 70 percent of enterprise IT pros recently surveyed by Cisco Systems Inc.

Israeli-based startup FireLayers believes it can thwart the use of these apps with its new application security gateway for apps running in the cloud that provides additional monitoring and protection. The policy-based Software-as-a-Service (SaaS) offering secures both custom and third-party cloud apps accessed by employee-owned devices. While many cloud services already offer some baked-in security, FireLayers looks to offer extended protection with support for Xtensible Access Control Markup Language (XACML), the XML-based access control policy protocol. "Cloud app providers

"Cloud app providers like Salesforce, Google, Box, SuccessFactors and others provide excellent user experiences, meet demanding performance SLAs and secure data in their clouds. But their responsibility ends there."

Doron Elgressy, President, FireLayers Inc.

like Salesforce, Google, Box, SuccessFactors and others provide excellent user experiences, meet demanding performance SLAs and secure data in their clouds," says FireLayers President Doron Elgressy. "But their responsibility ends there." Elgressy says an application security gateway closes that gap by providing security controls of cloud application usage at a granular level.

The FireLayers app security includes a central dashboard that lets administrators extend policies, manage permissions and approve specific access. It also shows known threats and can employ rules to counter them and provides reporting tools to assess and outline specific weaknesses.

3 StorageGRID Webscale

NetApp Inc.

In order to keep data secure, organizations must know where their data is stored. NetApp StorageGRID Webscale provides monitoring tools that lets IT track the physical movement of data. This storage management tool tracks large amounts of uncategorized data and keep it constant with the same security levels extended to confidential enterprise data.

It supports the Amazon Web Services Simple Storage Service (S3) and implements automatic encryption and access control capabilities, and aims to limit the threat of an unauthorized access or data leak.

The company is currently testing the next version of StorageGRID Webscale in its early adopter program, which includes geo-distributed erasure coding, a process in which data is fragmented and encoded with redundant data pieces and stored over multiple datacenters, ensuring that if there is a breach, data will stay protected. The company plans to release it in 2015.

4 Keyless SSL

CloudFlare Inc.

CloudFlare has made a name for itself over the past few years giving Web sites hosted in its service protection from distributed denial-of-service (DDoS) attacks. Recently, the company has come up with a solution for those enterprises not wanting to hand over SSL encryption keys to cloud providers in its Keyless SSL solution.

Developed by cryptographers and system engineers at CloudFlare, its Keyless SSL feature allows companies to allow their encrypted data to travel through the CloudFlare network without handing over the keys to the data. How it works is that SSL certificates are signed and verified on-premises by the enterprise's private keys before ever leaving. This allows CloudFlare to move and secure clients' data without ever having access to private encryption keys.

This technology could be a welcome anecdote now that online data breaches of major retailers, banks and other companies are becoming routine events. Want to harden your Web site from attack, but don't want to put the keys in the hands of a third party? CloudFlare has figured out a possible solution. While Keyless SSL is currently only offered through the CloudFlare Web protection service, look for similar approaches to start popping up from competing cloud security firms.

Whether you're keeping your enterprise files in a public cloud, an on-premises private cloud or in a hybrid deployment, the service you choose can make a difference when it comes to ensuring your organization's data is secure.

5 SharePlan for Enterprises

Code 42 Software Inc.

Whether you're keeping your enterprise files in a public cloud, an on-premises private cloud or in a hybrid deployment, the service you choose can make a difference when it comes to ensuring your organization's data is secure. SharePlan for Enterprises from Code 42 looks to keep your documents secure—and encrypted—while allowing for easy employee access to data, whether they're on-premises or in the cloud.

SharePlan for Enterprises syncs files across all user devices, notably Windows, Android, Mac OS X or iOS, while providin IT with a window into where and by whom the files are being accessed.

For those looking to keep their files on-premises, SharePlan lets IT run the SharePoint appliances within their own hardware configurations, allowing for full control of the service. Or, for those who prefer outside monitoring of their private cloud, or those running a hybrid solution, the Code 42 SharePlan can also be customized with around-the-clock monitoring and support.

To keep documents safe, files are automatically encrypted with AES 256-bit keys in transit and at rest. Accessing the data can only be done by those with the correct PIN to randomly generated, expiring links. It also supports two-factor authentication. And looking to close a huge hole in data leakage—lost or stolen employee devices—IT can remotely wipe any device running the SharePlan app.

What's the advantage of going with a paid service like SharePlan over rival cheap and cost-effective cloud storage services such as Dropbox or Google Docs for storage and user collaboration? Unlike personal document storage services that may be used by employees, IT has total control and insight of enterprise data at all times.

6 Windows 10

Microsoft

Yes, this belongs in the mix, too. As the cloud embodies everything Microsoft does, its flagship Windows OS is no exception. The next version–Windows 10–slated for release in mid-2015, will do its part to offer improved cloud security. Microsoft last month released the Windows 10 Technical Preview for testing.

As the cloud embodies everything Microsoft does, its flagship Windows OS is no exception.

While Microsoft relies on the BitLocker encryption service to keep data secure on devices, Windows 10 promises to improve security when data is in transit or stored elsewhere using container technology to separate data from the OS.

"With Windows 10 we are able to provide an additional layer of protection using containers and data separation at the application and file level–enabling protection that follows the data wherever it goes," said Jim Alkove, Microsoft Windows enterprise program management team lead, in a blog post. "Whether the data moves from a tablet or PC to a USB drive, e-mail or the cloud–it maintains the same level of protection."

Alkove said this approach will bring data protection to the "file level," and won't need any new actions from end users to gain the new security capabilities.

Chris Paoli is a Web producer for the 1105 Enterprise Computing Group. Reach him at cpaoli@1105media.com.
