CDW PEOPLE WHO GET IT

SECURITY IN THE CLOUD

With the right SaaS security solutions, small businesses can gain enterprise-class safeguards at an affordable price.

Executive Summary

Being small is no protection against cybertheft. In fact, a 2012 Verizon Communications analysis of several hacking studies found that 72 percent of data breaches worldwide the previous year occurred at companies with 100 or fewer employees — a 63 percent increase from the previous year.

Fortunately, small organizations have a security option that can give them protections once enjoyed mainly by large enterprises — at a friendly cost. Software as a service (SaaS) security solutions can deliver a host of safeguards via the cloud, which means that some (or possibly even all) of the responsibility for launching and maintaining security controls can be placed in the hands of a third-party cloud provider.

SaaS-based providers are likely to have a deep bench of security experts. Small- and medium-sized businesses (SMBs) utilizing these services can be more secure than they would if they managed these tools themselves.

Cloud-based security is available at an affordable, predictable cost. Small companies pay set monthly fees, typically calculated on a per-user basis. The service-based approach has the advantage of both eliminating the upfront capital expenses an SMB would shoulder for the hardware and software of in-house solutions and insulating the enterprise from the later costs of routine maintenance and repairs, which can unexpectedly siphon off human and financial resources.

TWEET THIS!

Table of Contents

The Situation

Cybecriminals see smaller organizations as attractive and lucrative targets. As a result, they are devoting more resources to cracking their security barriers. But why all the interest in SMBs?

First, there are significant riches to plunder in the form of financial accounts, customer information and intellectual capital. Putting the bounty in dollar terms, the Ponemon Institute estimates this year that the average data breach costs organizations $194 per record.

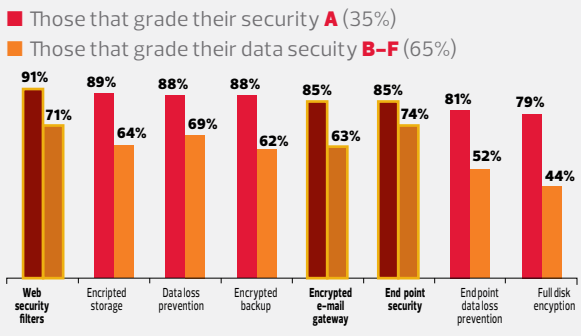
Second, getting at sensitive information may be easier when the target is an SMB. After all, these organizations typically have small IT staffs that can't focus entirely on security issues. In addition, SMBs often don't have resident security experts who keep up with the latest threats and security best practices.

With this in mind, it's easy to understand why the security controls offered in a software as a service solution are gaining traction with SMBs. SaaS, which delivers applications and services hosted in a service provider's IT infrastructure, has long been the most mature and widely used cloud option for small organizations. With SaaS, small businesses don't have to own the application or the supporting servers, operating systems, storage resources or network gear.

SMBs with limited budgets and IT staffs are among the biggest beneficiaries of this model. One reason is that SaaS pays off for them from a capital expense viewpoint. For example, a 2011 CDW Tracking Poll found that 21 percent of small businesses have adopted cloud computing and that 76 percent of this group has successfully reduced the cost of applications moved to the cloud. Savings averaged 24 percent, according to the poll.

Cloud Security Measures Play Big Role in Data Security

CDW's 2012 *Data Loss Prevention Straw Poll* revealed that **cloud-based security measures** are playing a growing role in overall data loss prevention efforts by organizations.



Solid Growth Curve

Revenues for SaaS-based security gateways grew more than 50 percent since late 2011, according to Infonetics Research.

The trend isn't likely to change anytime soon. Infonetics is forecasting a 23 percent compound annual growth rate for the category from 2011 to 2016. Security as a service is "a real bright spot," says Jeff Wilson, principal analyst for security at the international marketing and research company.

Initially, small businesses gravitated to running general business applications in the cloud, including web mail, conferencing programs and document collaboration tools. Now there's a move toward more business-critical resources being run by SaaS providers, and security is among the top choices. This option moves some or all responsibility for launching and maintaining an organization's security controls to a third-party cloud provider. In practice, a small organization may choose a complete hand off of all security functions to the SaaS partner or opt for a hybrid approach that mixes on-premises and cloud-based resources to optimize existing technology investments, yet also take advantage of a provider's specific security expertise.

There is a lot for small companies to like about a SaaS-based approach to security. Under the right circumstances, SaaS-based security can make an SMB more secure than in-house strategies. Assuming that careful evaluation has identified a service provider with solid security credentials, it can relieve a small company's IT staff of the nearly impossible burden of staying ahead of the latest security threats and abreast of relevant technology innovations and policy best practices. Security specialists have dedicated resources for assuring that policies are implemented effectively, including unwavering diligence in keeping security patches up to date.

The costs of cloud-based security options have the benefit of being predictable. Small companies pay set monthly fees, typically calculated on a per-user basis, to keep their IT infrastructure protected from hackers, data thieves and unscrupulous or careless insiders. In addition to eliminating upfront capital expenses, the SaaS security model insulates SMBs from the need for and unexpected expense of routine maintenance and repairs, which can unexpectedly sap both human and financial resources.

Although it's tempting to think of "security as a service" as a single entity, IT managers know that bolstering

security requires more than a simple, turnkey solution. No matter their size, enterprises must protect themselves from a broad range of threats. IT administrators need both a clear understanding of the security tools available and the role each plays to be able to fully evaluate SaaS-based providers and negotiate a service-level agreement (SLA) that will provide the necessary protection.

Rather than simply settling on a generic SaaS package that may or may not provide adequate safeguards, IT managers should investigate a security solution — or a combination of them — supported by these 10 building blocks. Together, these can help mitigate the risks of the biggest current vulnerabilities faced to keep vital IT resources safer.

Even though cyberthieves are ready to exploit any vulnerability without regard to the size of the intended victim, SMBs that have the right tools and practices in place can be as well protected as large enterprises, without breaking the IT budget.

Building Block #1: Security Assessments

The first step in bolstering security is simple: Perform an assessment to determine the current state of the protections in place, identify any gaps and formulate a plan to better safeguard the organization.

Whether an SMB has the advantage of in-house security expertise or not, it's often best to hire a third-party auditor to perform the assessment. A fresh set of eyes and penetration testing tools may uncover gaps that insiders inadvertently miss. When choosing an assessor, the key is to make sure its audits are guided by formal industry standards, such as ISO/IEC 27001, NIST Special Publication 800-115 and benchmarks from the Center for Internet Security.

Expect auditors to follow a series of steps to gauge vulnerabilities, including analyzing the configuration settings of hardware and applications, looking for security holes in the network infrastructure and performing penetration testing to determine how difficult it is for outsiders to access internal resources.

The result of the analysis and probing should be a comprehensive report that provides an overall rating of the organization's risk posture, with details about where gaps exist and how to remediate them as well as a roadmap for how to incorporate new security technologies and policies for better protection.

Building Block #2: Identity and Access Management

Even the most trusted employees in a small enterprise don't need access to every application or piece of information to do their jobs. To control how people or application processes can tap into any resource, SMBs need identity and access management systems. These safeguards are prime tools for protecting against insider threats — whether employees intentionally try to probe unauthorized areas or do so by accident. With the right systems in place, IT administrators can control access and also easily manage authorizations, so that authorities can centrally provision and deprovision accounts when new employees arrive or the responsibilities of existing staff members change.

Effective identity and access management solutions provide granular controls. For example, a member of the human resources department may be authorized to log on to the organization's main personnel database, but access controls could limit this user to viewing the salary and benefits information about workers who are paid hourly, not that of senior salaried officers.

Cloud-based identity and access management solutions can act as a central clearinghouse to manage authorizations for both on-premises resources and those running in public or private clouds. This "single sign-on" approach can be especially useful for managing mobile workers who need secure access to all of the same data and applications their office-bound counterparts use. Self-service capabilities, such as tools to help employees reset passwords, reduce the demands on security administrators for routine tasks.

Note that identity and access management solutions are vulnerable to identity theft if they only rely on user names and passwords to authorize individuals. SMBs may decide that these basic controls are sufficient for securing systems and applications that hold nonsensitive data. But to control access to proprietary data and highly sensitive personal information, IT administrators should look for management solutions that require multifactor authentication. For example, to access employee medical records, a multifactor approach could require entering a user ID and password in addition to swiping a security badge.

The solutions also should automatically log the activities of individual users as they navigate enterprise resources and create summary reports. This will help security

managers spot repeated attempts to access unauthorized information as well as provide forensics data if a breach does occur.

For growing companies, scalability is a key criterion to consider when evaluating service providers. Identity and access management solutions act as hubs to essential resources, so they must be able to accommodate a customer's current volume of logins and have room to grow if volume increases suddenly because of a significant expansion of the organization.

Building Block #3: Web Security

It's a fact of the interconnected world of the web that hackers, social engineers and stealthy malware are only a click away. This means that cyberthieves don't necessarily have to target a particular potential victim with a new attack. Instead, hackers can just wait for web surfers to come to them, whether they are attracted by a legitimate website that has been infected with a virus or by a site designed to be a cybertrap.

One solution to avert such threats is to employ content filters that run entirely in a cloud, or use cloud-based services to augment the on-premises secure web gateways used to watch over Internet traffic. With cloud-based filtering solutions, organizations can have additional insulation from cybercriminals by arranging for all web traffic to funnel through proxy servers managed by the SaaS provider.

After an employee clicks on a website, the content filter steps in to closely examine the data packets of all information that streams in through firewalls or proxy servers. The filters analyze the traffic using profile information created to screen for known viruses, spyware, spam and any other content the organization considers inappropriate. The filters also can use blacklists created by IT managers to automatically block web connections to sites known to pass on keyloggers or other malicious programs.

In a report earlier this year on secure web gateways, technology research firm Gartner noted that most organizations still rely on on-premises solutions. It added, however, that the market for SaaS-based solutions in this category is expanding rapidly, with growth rates expected to hit 35 percent this year. Gartner also noted that the category is subdividing into separate solutions optimized for SMBs and larger enterprises. SMB options are typically designed to be easy to use and economical, although they may lack some of the more advanced features found in enterprise applications, the report explained.

Look for solutions that provide web application firewalls, which scan traffic as it flows to and from web servers and client devices. These specialized firewalls guard against infected applications and help mitigate such major threats as SQL injections, which insert malicious code into strings that are passed to a SQL server. The script allows cyberthieves to vandalize and replace web pages, steal private data such as credit card information and manipulate databases. Such attacks have the potential to compromise thousands of records. Small organizations are also at risk from cross-site scripting (XSS), which uses malware to redirect people from legitimate websites to infected destinations.

Another key capability for securing web traffic is flexibility in setting filtering parameters and blacklists. Some products let administrators set detailed parameters about the time of day traffic to specific sites can be blocked. Advanced gateways also employ analytics to study end-user behavior and public-threat data to bolster the screening process. Solutions should have the ability to gather and summarize data about web traffic and malware encounters. These summaries can help administrators identify emerging problems and determine if there are any problem websites that need to be added to the current blacklist.

Building Block #4: E-mail Security

Closely related to web security are systems for securing e-mail communications. The two are linked because embedded URLs that send unsuspecting employees to nefarious sites are one of the oldest and biggest vulnerabilities in e-mails. As cybercriminals become more sophisticated, it isn't enough to simply warn staff members to avoid clicking on links or opening attachments in e-mail messages received from unknown sources. So-called "spear phishing" attacks are becoming ingenious enough to convince almost anyone that an infected message originated from a trusted party.

Fortunately, IT managers have advanced ways of reducing the risks that an e-mail will introduce viruses, rootkits and other problems into the organization's system. A new generation of cloud-based screening gateways focuses on e-mails and instant messages to block problem code as it enters the enterprise's system. Some of these solutions are so plugged into the latest virus databases that they update their definitions almost constantly during the day. This doesn't block so-called "zero day" viruses, which use newly developed code that initially flies under the radar of security systems. But they are effective in guarding

Mixed Feelings

The SMB Threat Awareness Poll, conducted in 2011 by security vendor Symantec, found that executives at small- and medium-sized businesses are security savvy. They understand the threats that exist in the world today, including the latest vulnerabilities that result from the use of smartphones and other new mobile devices.

Forty-six percent of the poll respondents said a targeted attack would cause a revenue loss and 20 percent said it would drive customers away. But half of the SMBs surveyed said they think their own organizations aren't in danger and that large enterprises face the biggest security risks.

against the latest vulnerabilities. Some e-mail security solutions include data encryption to provide an additional layer of protection against sensitive data being hijacked.

Look for e-mail security solutions that apply their controls at both ends of the messaging stream — to both inbound and outbound e-mail. This two-way protection keeps viruses and infected attachments from burrowing into internal systems while also blocking unencrypted information from leaving the organization.

As with other security solutions, the best options for e-mail security help IT administrators understand their threat profile with relevant data, such as the timing and sources of incoming and outgoing messages.

Building Block #5: Data Encryption

Using advanced algorithms to scramble data into incomprehensible bits and bytes can be one of the best ways to protect information while it is sitting in storage systems or moving across the network. Only authorized personnel with the proper decoding keys have the necessary tools to unscramble the code and make the data meaningful.

The latest options include full-disk encryption, which lets organizations establish policies to automatically keep all data under lock and encryption key. The rise of ubiquitous mobility is also a factor. Many commercial and public-sector organizations now require their notebook hard drives to be encrypted so that a lost or stolen device doesn't provide data thieves with a trove of valuable information. For the same reason, prudent enterprises routinely encrypt data as it is being saved to portable thumb drives. In some cases, encryption may even be required for regulatory compliance, depending on the industry sector and the type of information involved.

Individual cloud-based service providers should have advanced encryption policies in place and should be willing to discuss these safeguards with prospective clients. In addition, providers may list data scrambling among their service offerings, with capabilities that include automatic encryption of all communications between clients and the cloud providers. These services also may be equipped to combine encryption with virtual private networks (VPNs) to provide two layers of security when employees log on to the enterprise's network from the field or a home office.

Cloud-based encryption services also relieve IT administrators of some substantial management duties, which can range from overseeing the encryption/decryption processes themselves to creating security certificates and exchanging keys with trusted parties.

As with other security measures, however, IT managers must find the right balance between encryption safeguards and productivity. Encryption solutions levy a performance overhead for scrambling and unscrambling data, so cloud-based provider SLAs should include performance guarantees to ensure against bottlenecks.

Building Block #6: Network Security

Cloud-based network security services help IT managers protect today's complex communications pipelines. The necessary components include user identification tools and access controls, plus technologies for monitoring usage patterns. The heavily virtualized nature of cloud environments requires network security solutions that work as effectively with virtual machines as with physical hardware.

Deep-packet inspection is one of the most important capabilities that a network security solution can offer. It allows the security system to look beyond the address headings on data packets to understand the actual content being transported across the communications pipelines. Deep-packet inspection can be an early warning system about malicious code and other threats ready to lodge themselves into internal resources.

When an inspection uncovers problem code, the best network security solutions go beyond just issuing a warning to network administrators. Using preset criteria, the applications can block incoming software or, to mitigate insider threats, keep sensitive data from being saved to an unauthorized server or moved to an e-mail gateway. For example, SMBs can set the filters to home in on bank account numbers and apply special rules for where they are allowed to travel across the network.

To keep a close watch on their networks, administrators may choose to see real-time, daily or weekly summaries about traffic patterns, volumes and suspicious activities. But too much scrutiny can cause its own problems. Administrators might introduce delays in network performance if the security system is set to constantly analyze activities. The cloud-based solution should offer a range of oversight options that includes summary views of standard network segments and closer inspections of areas devoted to mission-critical systems.

In addition to deep-packet analyses, network security gateways should provide traditional firewalls as well as web application firewalls, the latter for network layer protection against SQL injections and other SQL Server Express (SSX) attacks. The ability to set up VPNs easily will help secure communications with mobile and remote staff members.

Other must-have features include tools for identifying the signatures of hackers associated with denial-of-service (DoS) attacks. The controls should extend to distributed denial-of-service (DDoS) vulnerabilities, which rely on a large number of systems at various locations to overload a target destination. The solution should also support the Internet Engineering Task Force's Domain Name System Security Extensions (DNSSEC), which address the inability of the DNS to authenticate domain names.

Building Block #7: Data Loss Prevention

Data loss prevention (DLP) systems help organizations monitor and manage critical information within their environments. With DLP solutions, SMBs can protect themselves against insider security breaches, whether the catalyst is malicious intent or an unintended deviation from security policies. The result can be just as damaging either way: loss or exposure of intellectual property, customer information and personnel records.

To be effective, DLP solutions must apply a variety of safeguards, including those that protect data at rest in a database or storage array.

Depending on the criticality of the information, IT managers can set the DLP solution to sound an alert or block an attempt when someone tries to copy or move sensitive data to a portable storage device, such as a DVD or USB thumb drive.

DLP capabilities also can scan local and network hard drives for critical data residing in unauthorized locations and vulnerable to being stolen or viewed by someone without the proper clearances.

Human Factors

SaaS-based security offers a number of advantages to help small organizations better protect themselves from cyberthieves and insider threats.

Even so, the cloud services address only half of the vulnerability protection puzzle. Just as important as the technology components are the policies and training that guide an organization's staff members to follow security best practices. This includes using and regularly changing strong passwords and being wise to the latest social engineering tricks.

In addition, DLP solutions can turn their attention to the network traffic of an enterprise to analyze files within the flow. IT administrators can choose to see reports or set up automatic roadblocks when the DLP system finds security policy breakdowns. For example, a company that does not allow unencrypted Social Security numbers to travel across the local area network could rely on a DLP solution to take action.

Some DLP solutions can home in on particular areas of the organization rather than looking at the entire network. This segment-specific approach is often integrated with an antispam gateway to help identify data leakages, such as might be created by e-mail attachments.

There are solutions that employ both endpoint protection and network-based components, with the benefit being that IT managers can enforce security policies centrally through two integrated solutions. This simplifies the task of deploying DLP capabilities across the enterprise.

Content-aware services are a feature of some DLP products. Content-aware detection integrates the scanning of outbound traffic with content discovery, such as identifying stored credit card numbers, personal information or sensitive data in unauthorized parts of the network. To be effective, content-aware DLP tools must scrutinize all types of traffic leaving the network, including e-mail, web traffic, file transfers and instant messages. By contrast, content-neutral products apply controls without regard to the information itself. One example of this would be a tool that blocks all downloads to thumb drives. In practice, both content-aware and content-neutral loss protection occur in endpoint protection and network-based products.

DLP technologies provide an important ancillary benefit: Their controls and monitoring tools help organizations demonstrate compliance with any regulations relevant to their particular market segment.

Building Block #8: Intrusion Detection and Prevention

Intrusion detection and intrusion prevention systems (IDS and IPS) use statistical analysis to spot security problems. One approach looks for known signatures associated with cybercriminals. Another IDS/IPS variation watches for anomalies in how people use and access IT resources. For example, if a database holding sensitive financial data is accessed at 3 a.m., it could trigger action by an IDS or IPS.

Whether looking for signatures or anomalies, these solutions react according to rules set up by system administrators. They may be set to log suspicious traffic or events, to send an alert to the appropriate administrator, or to take more decision action and actually block the activity.

Some IDS/IPS solutions are host-based, meaning they focus on a single resource and keep watch for any sign of intrusion in that particular area. Network-based solutions look at the entirety of network traffic or at all communications flowing over a particular segment. In the age of mobile applications, a third option is growing in importance: wireless IDS/IPS, which concentrates on wireless protocols. Depending on its security needs, an enterprise may need to mix and match these options to keep data safe.

Widespread use of virtualization and cloud environments is adding new wrinkles to how organizations configure and manage these solutions. Because of these new complexities, some smaller organizations are turning to the third-party expertise of SaaS providers, which can offer intrusion controls used by large enterprises without straining IT resources.

Building Block #9: Security Information and Event Management

Like some IDS/IPS solutions, security information event management (SIEM) systems also take a statistical approach to IT security. They scour the event logs to identify which documents, databases, applications and storage systems each employee is accessing and what particular data a user may be interacting with. If the SIEM solution notices unusual behavior, it can alert administrators as well as record the activity for later reporting and analysis.

Without an effective SIEM solution, SMBs either risk missing out on early signs of problems or must assign staff to constantly monitor traffic patterns and make snap judgments about what activities warrant an alert or a more substantial response.

SIEM systems often play an important oversight role with other security solutions by collecting and consolidating data from DLP, networking monitoring, IDS/IPS and event logs. This gives IT administrators a central location for viewing the security status of the entire organization. With this cross section of information in a central location, IT managers can incorporate settings for the types of anomalies to watch for and the thresholds for when alerts should be issued.

SIEM systems, however, aren't typically turnkey solutions. They require a period of fine-tuning by the end user or the cloud-based provider to avoid information overload and false positives as well as letting significant threats fly under the radar. Experts say most organizations need perhaps a week or two of running the systems under real-world conditions to finalize the settings. Baselines can be established by first determining average levels of bandwidth utilization, typical traffic patterns and other benchmarks for activities seen during normal operations.

IT managers appear to think the efforts pay off. SIEM continues to attract new users, according to Gartner: Last year, the market increased from $987 million to $1.1 billion, achieving a growth rate of 15 percent, the researcher says.

In its Magic Quadrant for Security Information and Event Management report for 2012, Gartner advises IT managers to evaluate potential SIEM solutions using four main questions:

1. Can you collect information and analyze events from the full range of host systems, security devices and network devices, and then combine that with information for users, assets and data?
2. Does the solution provide long-term event and context data and analysis?
3. Are there predefined functions that can be lightly customized to meet company-specific requirements?
4. Is the solution easy to deploy and maintain?

Building Block #10: Business Continuity and Disaster Recovery

Even the best security may not fully protect against today's most sophisticated hacking techniques, such as zero-day viruses. So, in addition to building solid defenses that protect mission-critical data, documents, web traffic and e-mail systems, organizations also need to develop contingency plans. The goal is to keep the enterprise

running when breaches occur or return its operations to normal as quickly as possible if vital data or systems are destroyed.

Cloud-based services are attractive for business continuity (BC) and disaster recovery (DR) strategies because they offer a wide range of benefits that reduce cost and complexity. They promise a quick way to set up distant backup sites for replicating data, especially for systems with relatively low volumes of information that can travel efficiently over wide area network (WAN) connections. Cost savings is another potential benefit. With cloud-based BC and DR, organizations typically pay less for the applications and underlying infrastructure because of multitenancy models that spread costs among many customers.

Another big financial advantage with cloud-based business continuity and disaster recovery is that IT managers don't have to make the business case for investing in redundant systems. Although a crisis might justify the cost of such backup resources, during normal times they are more like costly insurance policies that don't deliver value for day-to-day activities.

Cloud services, though, also can present some trade-offs. One is performance challenges. Inherent latency in WANs hinders response times when backing up or restoring large volumes of data. This means that when evaluating potential service providers, IT managers should determine whether the provider candidate has sufficient bandwidth to support all of its clients. The danger is that in a wide-scale natural or human-caused disaster, most customers of a cloud-based service will be trying to access their data at the same time, straining network capacity.

To ensure availability of critical applications and data that the SMB absolutely can't be without, IT managers should consider paying a premium for service that provides priority access to the cloud when demand is high. Another tack is to divide business among multiple service providers to avoid all-or-nothing scenarios. A third option is going with a hybrid cloud model, in which the organization keeps its most critical data within the bounds of a private cloud but also takes advantage of low-overhead public clouds for less valuable or archival information.

Any strategy that embraces using public clouds needs a solid SLA. Focus on guarantees about uptime rates as well as policies covering data replication and security to keep data available and safe from cyberthieves or from other customers of the cloud. And clearly spell out what financial penalties and other remediation steps will come into play if the service provider fails to meet the terms of the contract.