McAfee
An Intel Company

Stay Safe While You Grow Your Business

The right combination of protection for SMBs

In the world of cybercrime and cybersecurity, there is one thing that is consistent—the threat landscape changes constantly. Cybercriminals are now focusing their attention on small and mid-sized businesses (SMBs), because they are easier targets than large, multinational corporations. What's behind this trend? The pursuit, capture, prosecution, and incarceration of the perpetrators of high-profile breaches have caught the attention of hackers. Hackers have come to realize that they are better off pursuing a larger number of low-profile targets than making front page news with breaches of high-profile organizations.

Businesses of all sizes have sensitive information that is valuable to cybercriminals and that must be protected. But SMBs also grapple with the costs of supporting the robust security framework required to keep the bad guys out. These businesses are feeling pressure from all angles: increased attention from cybercriminals; growth of sensitive information that must be protected; and the costs associated with security.

While these elements create a thorny problem, there is a solution: cloud-based security Software-as-a-Service (SaaS). Security SaaS suites can deliver full-strength protection at an affordable price. Cloud-based solutions are capable of delivering the kind of comprehensive, managed protection currently associated with more expensive solutions, but at a fraction of the cost.

Shifting Targets, Smaller Strikes

High-profile arrests and convictions of cybercriminals attacking global financial companies have become front page news. According to the *Verizon 2011 Data Breach Investigations Report,* "Numerous smaller strikes on hotels, restaurants, and retailers represent a lower-risk alternative."

At the same time, the employee and customer information maintained within SMBs is becoming a more valuable commodity. Boutique hotels, personal financial services, law offices, department stores, medical billing services, building contractors, and similar organizations have information that can be collected by cybercriminals and sold or used in other destructive ways.

In some ways, the stakes for SMBs are even higher than for a large corporation. A successful attack can quickly result in loss of community trust and customer goodwill. These attributes are built over a period of years and can be lost due to a single event—and this can have long-term negative implications for an SMB unless that trust can be quickly re-established.

While the potential damage is apparent, some of the data in the *Verizon 2011 Data Breach Investigations Report* should raise additional red flags when it comes to security breaches. The 2011 report shows that 90 percent of attacks were initiated from outside of the target organization, reflecting a significant increase from the previous year. Perhaps even more noteworthy is that these attacks were not considered particularly difficult to pull off. Hacking, email, and web/Internet interactions were the most common routes of attack, with hacking comprising more than 80 percent of reported attacks. Hacking attacks through the backdoor of command and control channels on the network or through guessing common or default credentials can be successfully defended by carefully monitoring endpoints, eliminating phishing emails, testing web applications, stopping malware before it enters the network, and ensuring that essential controls are in

place. In addition to the inbound threats, SMBs are concerned about how to gain control over data exiting their organizations. The two biggest security issues SMBs face on a daily basis is adherence to regulatory compliance and secure transmission of sensitive data, documents, or personally identifiable information.

Comprehensive, Scalable, Effective Solutions

The traditional enterprise approach to security is to buy dedicated hardware, acquire the licenses of multiple tools, and set policy standards for email, Internet, and web usage. For growing businesses, however, spending this kind of time, process, and money is not a reasonable option. You need an affordable, scalable, and effective solution that allows you to conduct your business under an umbrella of protection—covering all attack routes, adjusting automatically as your business grows and maintaining up-to-the-minute technological currency.

Fortunately, the cloud offers scalability of service, automatically using only the resources required to meet the demand. Security is provided as a service to users who simply subscribe, use it immediately, and holistically monitor the status of their systems. Attacks are automatically defended and the business alerted to their nature and source. These security services provide the effectiveness of global company security within a small company budget.

McAfee Cloud-Based SaaS for SMBs

A complete security framework contains firewall protection to protect against hackers; email security to protect against phishing and viruses; regulatory compliance libraries and encryption to identify and secure sensitive data; email continuity to ensure always-on email service; and web filtering to protect against spyware, malware, and the abuse of web privileges. These services, including transparent updates, instant access, and security management, are all incorporated into McAfee® Security SaaS suites.

- *McAfee SaaS Endpoint Protection Suite*—Defends the devices on your network on all attack routes
- *McAfee SaaS Endpoint and Email Protection Suite*—Adds protection from malicious email content before it enters the network, email continuity to ensure uninterrupted access to email, and client-side web category filtering
- *McAfee SaaS Total Protection™ Suite*—Adds email encryption and pre-built compliance libraries to protect sensitive data and meet compliance requirements, and cloud-based web filtering for antivirus, antimalware, and category filtering to ensure unwanted content never makes it into the network

These cloud-based services transparently and automatically scale to the needs of your business immediately, with little or no ongoing maintenance or extra costs. They all provide comprehensive reporting and 24/7 technical support.

McAfee Products	McAfee SaaS Endpoint Protection	McAfee SaaS Endpoint and Email	McAfee SaaS Total Protection
McAfee SecurityCenter, for centralized visibility through an online management console	•	•	•
Desktop and file server antivirus and antispyware scan and block out malware	•	•	•
Desktop firewall blocks hackers and intrusions	•	•	•
Web security scans web traffic for malware, enabling safe surfing	•	•	•
Web filtering blocks unwanted websites and web content		•	•
Email server protection scans for viruses and spam in-house		•	•
Email scanning stops malicious spam and phishing in the cloud, and email continuity provides protection during any planned or unplanned email server outages		•	•
Pre-built compliance libraries and email encryption to identify and secure emails containing sensitive data			•
Web Protection filters all web traffic prior to the malware entering the network and enforces corporate web usage policies			•

How Safe Is Your Company?

McAfee cloud-based SaaS products allow SMBs to maintain the same levels of defense as global institutions at a fraction of the total cost. To help determine the protection you need, assess your current security strategy, and tailor your solution, use the McAfee Solution Advisor.

McAfee provides affordable, comprehensive security that meets your company's needs, now and in the future. Growing your business is your priority. Protecting it is ours.

Next Steps

For more information, visit www.mcafee.com/smb, or contact your local McAfee representative.

Free 30-Day Trial

Experience the value of McAfee SaaS Security solutions with a free 30-day trial.

Visit www.mcafee.com/SMB.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

44802brf_saas-smb_0412_fnl_ASD