White Paper

Security for Small Business

The challenge of strong security and cost-effective compliance

Table of Contents

Small businesses today are squeezed between extremely tight IT budgets and unyielding requirements to protect sensitive information. Security and compliance seem like impossible tasks. Impossible security tasks can become an ugly reality for small businesses seeking growth and profits. Credit card sales of goods and services frequently are often the greatest source of profit for a small business. Therefore, a business model built on processing and storing sensitive customer or consumer information is a critical strategic advantage for many small businesses. Ignoring the challenges of securing sensitive information, or walking away from compliance and risk requirements, simply is not an option.

Allocating large amounts of costly and scarce resources to security and compliance is not viable for small businesses. They lack the deep pockets to pay six-figure salaries for a dedicated security staff and million-dollar budgets to purchase enterprise security solutions. Regardless, small companies must meet the same security and compliance requirements as Fortune 500 behemoths to remain in business.

There are small businesses that successfully navigate this intractable dilemma of scarce resources and inscrutable requirements. Most do it the way small businesses traditionally have competed with larger enterprises—with ingenuity in finding new ways to solve problems and agility in applying them.

Compliance and security starts with a clear understanding of the risks your business faces and elimination of all unnecessary data and duplication. Once security issues are reduced to the absolute minimum needed to sustain and grow the business, it's time to rigorously apply the risk lifecycle methodology to find the most efficient safeguards.

Spending too much on security and compliance is not as dangerous as spending too little, but both raise the risk profile of a small business. The best security is that which can be directly linked to reducing the risk to a business process, such as an e-commerce website or online distribution chain. Spending too much on security and compliance carries a high opportunity cost. Dollars available for research and development or growing new markets are siphoned off.

This white paper reviews the security and compliance challenges facing small businesses and the risk they pose to the business. It introduces the risk management model as a critical tool for understanding how to evaluate and minimize risk before spending a dime. The risk management lifecycle is presented as a useful guide for evaluating when and how to spend on security, and how much. An overview of McAfee® risk management solutions is provided to help small businesses see how a mix of products and services from an industry leader can help them achieve the elusive goal of cost-effective security and compliance supporting business strategy.

Economic and Security Challenges Facing Small Business

Companies are seeing an accelerating number of attacks on sensitive information executed by criminal gangs.

Criminals target banks because that's where the money is. Banks get robbed when the economy is good. They get robbed even more during an economic recession. The same can be said for cybercriminals targeting sensitive business and personal information. The risk of an external attack resulting in an information breach may be higher in a bad economy when budgets are most squeezed and you're least able to pay for strong protection.

Tightening security requirements and the escalating cost of security

Companies are seeing an accelerating number of attacks on sensitive information executed by criminal gangs. These gangs are international in scope, targeting businesses adopting cloud computing, new and risky mobile wireless smartphones, and social networking. The traditional internal threat posed by employees has been replaced as the chief information risk to business. External attacks from information criminals now are the most costly information risk, and the change in threat vectors leaves businesses uncertain about how to respond.[1]

1. Help Net Security, *Perceptions of Data Security At Odds With Reality*, http://www.net-security.org/secworld.php?id=9208

Government agencies overseeing privacy regulations and security standards bodies that publish regulations and standards are not ignoring the increasingly virulent threat universe. They are busy strengthening regulations.

The Payment Card Industry (PCI) Standards Council in October, 2010 issued a new edition, version 2, of the PCI Data Security Standard (PCI DSS).[2] The PCI DSS is the most widely applicable information security standard, applying to millions of merchants that accept credit cards for goods and services around the globe. Most of these are small businesses that are vulnerable to increasingly aggressive enforcement actions by card issuers.

Small businesses providing services in healthcare are directly impacted by the tougher security requirements and penalties in the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The HITECH Act of 2009 addresses electronic private healthcare information (EPHI). It raised civil and criminal penalties for HIPAA violations and extended the legal requirements for protecting EPHI directly to third-party service providers (dubbed business associates by HIPAA), making them directly liable to the Department of Health and Social Services (HSS) for civil and criminal penalties.

The many small businesses providing billing, insurance processing, pharmaceutical, lab, therapeutic, and other services to larger healthcare entities must now include specific HIPAA business associate language in their business contracts. They face the same potential HSS penalties as their customers, the owners of the EPHI.

A bevy of new and strengthened federal security regulations recently issued by the National Institute of Standards and Technology (NIST) applies to most small businesses providing services to the federal government. The NIST 800-series of computer security guidance contains many new and updated regulations with stronger requirements and more specific guidance.[3]

Attacks by information criminals and stronger regulatory requirements, combined with industry moves to social networking and the adoption of cloud and wireless computing is increasing security budgets.

The impact of more attacks by information criminals and stronger regulatory requirements, combined with industry moves to social networking and the adoption of cloud and wireless computing, is increasing security budgets. In 2010, spending on security software was forecast to be seven percent more than what was spent in 2009[4] as organizations of all sizes found themselves "ill-prepared for the major changes ahead, and potentially endangering the organizations they secure."[5]

In the heavily targeted retail banking sector, spending to strengthen online banking will reach $9.7 billion in 2015, representing a 33 percent annual growth rate.[6] Financial services spending for network security safeguards, such as VPNs, intrusion protections, and firewalls, will propel growth in the segment by 8.1 percent in 2011, from $7.5 billion to $8.2 billion. Security appliances, a low-cost architecture favored by small businesses, are a key component of the network security marketplace.[7]

The Escalating Costs of a Security Breach

The cost of a security breach continues to escalate year over year. Businesses experiencing a breach must spend on investigations, individual notifications to persons with personal information exposed, strengthened security countermeasures and programs, and, increasingly, legal fees and fines. Fines for security and privacy breaches are expected to increase with more regulatory focus on sensitive information collected from cloud applications, social networks, mobile phones, and electronic payments.[8] Then there are the intangible costs to reputation, brands, and goodwill—costs that, in some cases, can exceed the tangible costs.

2. https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0
3. http://csrc.nist.gov/publications/PubsSPs.html
4. Gartner, *Security Software Markets, Worldwide, 2009-2014, 2Q10 Update:* http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1410013
5. http://www.networkworld.com/news/2011/021811-security-departments-not-prepared-for.html?page=1
6. Ovum, http://about.datamonitor.com/media/archives/5290
7. IDC, http://www.networkworld.com/news/2011/010411-network-security.html?source=nww_rss
8. *FTC Privacy Framework:* http://www.ftc.gov/os/comments/privacyreportframework/00386-58031.pdf

A 2010 survey of 51 organizations suffering a breach found that the average total cost of an information breach continued to rise, increasing by 5 percent from 2009, from $6.8 million to $7.2 million. Malicious attacks by information criminals are by far the most expensive type of breach, costing an average of $318 per breached record in 2010. This is 90 percent more than the $167 average cost of remedying a breached record caused by internal negligence or system failures.[9] Breach costs also vary by sector with financial and healthcare costs per record being almost twice as much per breached record as in retail.

Yearly Increases in Average Breach Costs[10]

	2007	2008	2009	2010
Average Total Breach Cost	$6.3 M	$6.6 M	$6.8 M	$7.2 M
Average Cost per Breached Record	$198	$202	$204	$214

An opening salvo in the regulatory move to tougher enforcement were the first HSS civil penalties issued for HITECH and HIPAA violations in February 2011. Cignet Health of Maryland was fined $4.3 million for a multitude of HIPAA violations.[11] A pair of one-time HIPAA privacy violations resulted in Massachussetts General Hospital being fined $1 million,[12] along with Seattle-based Providence Health and Services being penalized $100,000.[13] In announcing the fines, HSS served notice of stronger future enforcement.[14]

The Federal Trade Commission (FTC) also levies fines for failure to protect consumer information. One notable example is a $2.25 million levy against the large CVS Caremark retail pharmacy chain in February 2009 for failing to implement an information security program to protect customer and patient data. CVS Caremark was found to have improperly disposed of consumer pharmacy records in commercial trash dumpsters.[15]

Rising numbers of external attacks

External breaches by criminals are precisely targeted, often leading to identity credentials stolen from a specifically targeted individual, one with access to sensitive information. The result can be a large theft of financial assets.

An example of this new type of targeted attack on small businesses is the "corporate account takeover." In 2009, authorities noticed a surge in stolen online banking credentials from malware infections aimed at small businesses.[16] With the stolen account information, criminal gangs initiated fraudulent electronic wire transfers from the victim's account to international destinations, often beyond the reach of U.S. authorities. Automated clearing house (ACH) transfers were used to send money to domestic criminal accomplices if the compromised account lacked wire transfer authority.

Fifty-six percent of small and mid-sized businesses experienced some type of banking-related fraud in 2010, with 75 percent of this coming from online sources, most prominently online account takeover. Among small businesses falling prey to bank fraud, 61 percent were victimized more than once.[17]

A dragnet in the U.S. and the U.K. rolled up one of these sophisticated international criminal gangs attacking small business bank accounts in October 2010. Authorities arrested more than 60 people connected with an Eastern European information theft ring. Indictments charged gang members with using the Zeus Trojan to steal more than $3 million from online corporate financial accounts.[18]

9. Ponemon Institute, *U.S. Cost of a Data Breach, 2010:* http://www.networkworld.com/news/2011/030811-ponemon-data-breachhtml?source=NWWNLE_nlt_daily_am_2011-03-08
10. Ponemon Institute: http://www.networkworld.com/news/2009/020209-data-breach.html
11. http://www.thegovmonitor.com/world_news/united_states/hhs-fines-cignet-health-4-3-million-for-hipaa-privacy-rule-violations-46834.html
12. http://www.healthdatamanagement.com/news/hipaa-privacy-fine-hhs-massachusetts-general-42023-1.html?ET=healthdatamanagement:e1680:188848a:&st=email
13. http://www.healthcareitnews.com/news/hhs-slaps-providence-health-100000-fine
14. Ibid
15. *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees*: www.ftc.gov/opa/2009/02/cvs.shtm
16. http://admin.nacha.org/userfiles/File/NACHA_Operations_Bulletin_-_Corporate_Account_Takeover_-_December_2_2009.pdf
17. *2011 Business Banking Trust Study*, http://www.informationweek.com/news/smb/security/229400827
18. http://uk.news.yahoo.com/16/20101001/ttc-us-officials-charge-60-in-zeus-crime-6315470.html

The widely used spear phishing attacks used in online account takeovers continue to grab headlines by using social engineeering attributes to exploit human vulnerabilities. Precisely targeted spear phishing email messages appear to come from trusted legitimate sources, such as legal counsel, corporate contracts, or market research. Company officers, managers, or employees are targeted based on information harvested by criminals.

The emails contain links to bogus websites that inject malware into the victim's browser. The malware quickly spreads inside the victim's network, seeking out systems hosting sensitive information to expose to the information criminals. The much-publicized attacks on RSA Security and Epsilon email marketing revealed in early 2011 were classic examples of spear phishing attacks.[19]

The onslaught of increasingly sophisticated targeted attacks is reflected in growing information breach statistics. A 2010 survey found that 60 percent of organizations report a "chronic and recurring loss" of sensitive information.[20] Two-thirds of large companies reported successful intrusions of their networks from external sources in 2010, up from 41 percent in 2009.[21]

More than one million small businesses and retailers were victims of some type of information theft in 2010. Physical theft or tampering with point-of-sale terminals was experienced by 37 percent, while computer viruses and malware were seen by 22 percent. Employee misuse or the internal theft of credit card data accounted for 17 percent of security incidents in small businesses.[22]

Breaches of sensitive information from internal sources are fundamentally different from information stolen in external attacks. Internal theft or loss may expose large numbers of individual records per breach, but are far more likely to be accidental than malicious. The information exposed from an internal breach may not fall into the hands of criminals capable of identity theft. The random and untargeted nature of an internal breach may not result in millions of dollars stolen from bank accounts. However, the economic damage from an internal breach can be significant due to the cost of repair and the notification of each individual victim.

Maintaining Strong Security with Reduced Budgets

Today licensed software is giving way to models increasingly en vogue among IT buyers.

The average security budget for all companies is around 5 percent of the total IT budget.[23] Some sectors, such as financial services, spend a considerably higher percentage of IT budgets on security, others less. In the current economic climate the trend in IT spending is down generally. In this era of reduced IT spending, security budgets continue to grow.[24]

Small businesses must be secure and compliant on significantly less money than a large enterprise. A classic example in how small businesses push the envelope and get more bang for their security and compliance buck is demonstrated in the early adoption of three new security and industry trends—Software-as-a-Service (SaaS), managed security services, and dedicated security appliances. Both cloud-based services and security appliances were disruptive solutions when first introduced, offering new bundles of security and compliance functionality at lower prices than previously available. They took far less time and capital to be deployed than traditional enterprise software solutions. They also were new and not well understood and initially were viewed as more risky.

Small businesses have a deep and fundamental appreciation of the linkage between managing business risk and competitiveness. They intuitively understood the agility and economic benefits of cloud-based software and security services. Small businesses became early and enthusiastic users, launching the growth in SaaS and managed security services while propelling growth to double digits. The economics caught the attention of large enterprises that fueled a second wave of growth.

19. http://www.reuters.com/article/2011/04/05/us-hackers-epsilon-idUSTRE7336DZ20110405
20. Ponemon Research-Accenture, *How Global Organizations Approach the Challenge of Protecting Sensitive Data*: https://microsite.accenture.com/dataprivacyreport/Documents/Accenture_Data_Privacy_Report.pdf
21. Amplitude Research, *Sixth Annual Enterprise IT Security Survey:* http://www.computerworld.com/s/article/9190559/Most_large_companies_hit_by_hack_attacks_survey_shows
22. http://smallbiztrends.com/2011/01/first-data-and-nrf-release-results-of-smb-data-security-study.html
23. Gartner, *Key IT Metrics Data for 2010*
24. Gartner, *Security Software Markets, Worldwide, 2009-2014, 2Q10 Update*: http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1410013

Today, traditional on-premises, licensed software "is giving way to models more increasingly en vogue among IT buyers, as CIOs continue reshaping their data center operations to embrace cost-saving technologies like the cloud and easier-to-deploy approaches like dedicated appliances."[25] Even the Federal Government is jumping on the SaaS bandwagon with a goal of using cloud computing to bost efficiency by increasing IT infrastructure utilization from 30 percent to 70 percent.[26]

The trend to increased use of SaaS, cloud-based managed security services and dedicated security appliances is expected to further accelerate and outpace licensed software until it becomes "the preferred purchasing method."[27]

Risk Management for Cost-Effective Security

Meeting tougher security requirements is not optional for any business, regardless of size. However, it is possible to have strong, effective security efficiently delivered at an acceptable cost, a fundamental requirement for small business. Making security cost effective requires following three guiding principles:

- Minimize the amount of sensitive information retained in the organization
- Practice risk management first
- Buy the appropriate level of security

Minimize the amount of sensitive information

Every piece of sensitive information processed, transmitted, or stored in your business increases risk and cost.

Every piece of sensitive information processed, transmitted, or stored in your business increases risk and cost. Many organizations have repositories of sensitive employee and customer data for internal use or to provide revenue-generating services, such as billing or insurance claims. Often this sensitive information crosses state or international boundaries for processing and storage with little management oversight.

The gathering and processing of sensitive information is exploding with the growth of consumer data from social networking, mobile devices, and cloud computing. An entirely new industry, dubbed the "tracking industry," is forming around the collection, correlation, and selling of online consumer information about finances, purchases, religion, entertainment, travel, hobbies, and other interests. The tracking industry and the potential threats of so much concentrated and correlated consumer information has attracted the interest of privacy advocates and regulators. Legislation has been introduced in Congress to protect the online privacy rights of consumers.

Minimizing the types of sensitive information processed is not always an option when the strategy of the business is to add value by processing finance, healthcare, or consumer information. Efficiencies can be gained by reducing the number of locations where sensitive information is processed or stored. Consolidating systems and locations that process and store sensitive information reduces risk and the cost of protecting sensitive information in multiple locations.

The first step in minimizing the amount of sensitive information in the organization is to identify every location it is transmitted, processed, or stored. Every piece of data must have sufficient business justification to allow its existence in that location or it should immediately become a candidate for elimination or consolidation. In addition to eliminating redundancies in the duplication and protection of sensitive information, consolidating sensitive information processing and storage locations brings economies of scale. Take advantage of the fact that the marginal cost of protecting each incremental gigabyte of sensitive information declines with volume.

A related strategy to sensitive data minimization is obfuscation. New technologies such as tokenization, or proven ones like encryption, require keys or indexes to make the information usable by humans. It can greatly reduce the cost of protecting sensitive information after consolidation. Risk is reduced because specific exemptions are allowed for breaches of encrypted information that eliminates the costly notification step.

25. Ibid
26. http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf
27. Gartner, *Security Software Markets, Worldwide, 2009-2014, 2Q10 Update*: http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1410013

The most cost-effective way to manage security and compliance starts with classic risk management.

Risk management for security and compliance

Experts across the security, compliance, and risk management spectrum agree that the most cost-effective way to manage security and compliance starts with classic risk management. It's no longer an option for business. Compliance regulations require a periodic and documented assessment of risks to sensitive information. A risk management assessment is no longer optional for businesses covered by compliance regulations.

IT risk management is an intuitive lifecycle that brings an insurance paradigm to security and compliance. It is increasingly practiced in the public and private sectors, with a track record in producing cost savings, stronger security, and better compliance.

The Risk Lifecycle for Efficient Security and Compliance

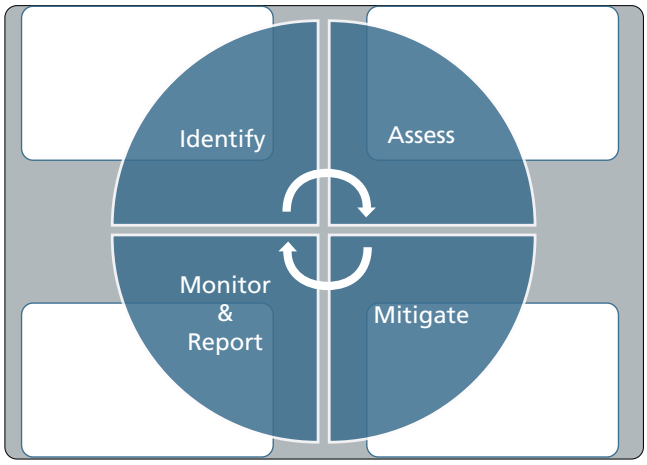

Figure 1. The IT risk management lifecycle helps small businesses achieve cost savings, stronger security, and better compliance.

Phase 1: Identify information assets

The first phase in the risk management lifecycle is to identify and catalog every internal or external location, system, application, and network your company uses to process, store, or transmit sensitive information. List the precise piece of sensitive information (Social Security numbers, cardholder names, account numbers, expiration dates, and related data) and the business justification. You also want to know the economic value of the information and the systems processing, storing, or transmitting it to use in the next step. The inventory of sensitive information catalogues your company's critical assets targeted by the threat universe.

Phase 2: Assess threats and vulnerabilities

This phase includes a three-step economic analysis: .

- Identifying and classifying threats
- Mapping the threats to vulnerabilities
- Calculating the risk in dollars

The internal and external threat universe represents all potential avenues that can limit, degrade, disrupt, or destroy your ability to do business. Threats range from natural disasters, competitive moves, legal and regulatory actions, thefts by information criminals, or your accidental or malicious acts by your trusted employees. In this first step, you categorize each threat according to the annual probability of occurrence. Not all threats are equal. Your job is to identify the likelihood of occurrence as an annual percentage of occurrence.

In step two, map each individual threat to each asset/system, facility, or business process. Not all assets will be vulnerable to each threat. For instance, Linux systems are not vulnerable to malware targeted at Microsoft Windows systems. Attach the economic value determined for each asset in Phase 1 (identifying information assets) to each vulnerable asset identified in the threat-vulnerability pairing.

In step three, determine the risk in dollars posed by each threat-vulnerability combination. The classic tool used in this step is the risk equation:

Risk = Annual Threat Probability (a percentage) x Vulnerability Impact (in dollars)

The risk equation results in a dollar value. For example, if the annual threat probability is 10 percent and the vulnerable system is valued at $1 million, the risk is $100,000.

10 Percent Annual Risk Probability x $1 Million Value of Vulnerable System = $100,000 Risk

The dollar value produced in the risk equation provides you with a spending yardstick.

Phase 3: Mitigate risk

Mitigation to remedy risks to systems begins with a budget based on the risk to each asset measured in dollars. High-priority systems will have more risk in dollar value than lower-priority systems. Risk guidance says you should not spend more to protect a system than the risk value in dollars. It is a judgment call on what period to use for applying the risk spending guidance—one year or the life of a system.

Get creative and strategic in planning mitigation. For instance, spending $10,000 from a capital budget to protect internal systems with in-house controls may only be one option. Small businesses traditionally are adept at displaying business agility. Consider alternative economic models or business processes. Moving information assets to a cloud-based SaaS provider with good security may cost far less with a monthly expense and one-time relocation fee for consulting services. If the asset is too critical or strategic to host in the cloud, perhaps costly security infrastructure can be outsourced before making more investments. Firewalls and intrusion systems are security controls that frequently can produce savings if outsourced.

Phase 4: Monitor and report

Security is a journey, not a destination. The security journey requires continuous monitoring of safeguards, critical systems and information, and new developments in the threat universe. Monitoring produces feedback information for continuous improvements to security and business processes. It can identify inefficiencies or weaknesses before they are exploited. The value of continuous monitoring has recently been elevated as requirement for federal information systems.

The security journey requires continuous monitoring of safeguards, critical systems and information, and new developments in the threat universe.

Similarly reporting is a strategic security, compliance, and risk management tool. Reports help organize information to identify areas for investment. Reports, and their source log data, are critical detective tools for forensic investigations of security incidents. Good and thorough reports on operations also provide audit evidence to help reduce the expense of a compliance audit.

McAfee Solutions—Products and Services for Strong, Cost-Effective Security and Compliance

Small businesses must secure critical information assets against high risks to meet compliance requirements and grow revenues. As an information security leader, McAfee has the broadest and deepest lineup of products and services to give small businesses cost-effective choices for managing the risk of internal and external threats.

McAfee products include a mix of software and appliance-based solutions, coupled with cloud-based services. McAfee offers small businesses options for effective security and compliance that also enhance business agility. With McAfee, small businesses get cost-effective alternatives to protect websites and email messages from malware attack, thwart malicious intrusions, secure perimeters, protect sensitive information, and manage risk policies across the company.

The best defenses against malware implement layered security with anti-spam and anti-virus defenses lodged in the cloud, at the enterprise gateway, and on the user's endpoint.

Detecting and combating malware

The best defenses to meet compliance mandates for malware protection implement layered security. Cloud-based defenses filter malware far away from your sensitive information, greatly reducing the risk of malware infections inside your network, while eliminating the cost of storing infected email messages. Endpoint filters add an additional layer of protection from email and web-borne threats and secure against local threats.

The McAfee SaaS service family

Cloud-based services provide enterprise-level protection for small businesses with no need to buy any hardware or software. McAfee SaaS Email Protection meets compliance requirements with comprehensive filtering and security from the source to the destination as an easy-to-manage cloud-based service. You enjoy complete and cost-effective control of email defenses with no backups or updates to install. Cloud-based policy controls scan outbound emails from designated sources or to specified destinations, preventing sensitive data leaks to unauthorized recipients.

Protection from malware includes monitoring a user's web browser for drive-by attacks launched from malicious websites. Malware injected from an infected website has become one of the most widely used malware attack vectors. McAfee SaaS Web Protection monitors the user's browser session for injection attacks, while McAfee SiteAdvisor® and McAfee SECURE™ reputation services assess the website's safety before you click on links embedded in a spear phishing email message, social networking sites, or in search results.

Secure email messaging

The McAfee SaaS Security family includes McAfee SaaS Email Encryption to meet compliance requirements for keeping sensitive email message content secure from source to destination. Working with McAfee SaaS Email Protection service, messages are encrypted at the source on keywords or at designated destinations. The service helps small businesses meet compliance requirements by eliminating the need to deploy and manage costly third-party PKI or certificate authorities.

McAfee SaaS Email Continuity helps small businesses meet business continuity requirements by engaging automatically upon detection of a server failure. McAfee Email Continuity offers full email functionality via a secure web browser interface, allowing email access, use, and management until normal service is restored.

McAfee SaaS Email Archiving is a cost-effective solution for small businesses with legal e-discovery requirements to produce messages and information requested in a subpoena. The cloud-based service automatically, securely, and economically stores unlimited volumes of email for future review and e-discovery. Its self-management features give users powerful search and recovery capabilities on message subject matter, originator, destination, or keyword. McAfee Email Archiving eliminates the need for costly, dedicated management staff and disaster recovery with unlimited, in-the-cloud storage.

Protecting the endpoint

McAfee SaaS Endpoint Protection meets compliance requirements for device protection from viruses, spyware, web threats, and hacker attacks but is deployed and managed via the cloud. McAfee SaaS Endpoint Protection provides a versionless solution with transparent updates, centralized deployment, and automatic and peer-to-peer upgrades—all with real-time threat protection.

McAfee Endpoint Encryption solutions use industry-leading encryption algorithms and offer multiple layers of protection that address specific risk areas. Encryption is extended to PCs, laptops, network files and folders, removable media, and USB storage devices.

Around-the-clock protection and availability

Small businesses can't afford a dedicated team of security specialists to monitor the global state of threats around the clock and provide real-time updates. McAfee provides this level of expert protection, far beyond what most organizations could provide for themselves.

Behind the services is McAfee Global Threat Intelligence™ (McAfee GTI™), a sophisticated streaming data environment that continuously monitors the real-time state of the Internet 24/7 and dynamically adds threat updates from a global network of million of sensors. McAfee GTI is supported by a dedicated global research team. Small businesses benefit, as all McAfee customers do, from the global McAfee view of the threat environment.

Summary

Small businesses must provide strong security and compliance with small budgets and fewer resources while enhancing business agility. Adopting a risk management approach for security and compliance helps small businesses identify critical risks and develop economic yardsticks to help prioritize spending.

McAfee, as a leader in risk management solutions, has the expansive and modular mix of security and compliance products, appliances, and cloud-based services that small businesses need for cost-effective choices that enhance business agility.

The broad and deep McAfee solutions help small businesses move to a risk management framework for security and compliance solutions. McAfee solutions offer layers of choices for perimeter and endpoint firewalls, host and network intrusion defenses, anti-malware, and vulnerability controls. Escalating security lifecycle costs become history as small businesses make choices based on cost and flexibility.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.
http://www.mcafee.com

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

26308wp_smb-security_0511