



The Benefits of Cloud-Based Security

How Companies of All Sizes Can Save Money and Improve Efficiency with Cloud-Based Solutions

Tony Bradley, CISSP-ISSAP, Microsoft MVP
July, 2008



Table of Contents

Abstract..... 3

Overview of Network Security 4

 Malware 4

 Network Intrusion 4

 Security Compliance..... 5

Challenges of Traditional Security 6

 Growing Pains 6

 IT Training 6

 Spikes in Demand..... 6

 The Bottom Line..... 7

Addressing Needs with Cloud-Based Security Solutions 8

 No Capital Investment 8

 Quicker Deployment 9

 Self Maintaining 9

Meeting Evolving Security Needs 10

 Alert Logic Threat Manager 10

 Alert Logic Log Manager 11

Abstract

It is no longer acceptable for security to be an afterthought. Organizations must proactively defend their networks and their data from relentless malware attacks, attempts at unauthorized access, and other security threats. In addition, most companies fall under at least one compliance mandate such as SOX, HIPAA, GLBA, PCI DSS, or others which establish minimum acceptable security standards and spell out mandates for how organizations are required to protect their data.

The problem is that implementing security costs money. There are up front capital investments to be made in equipment and infrastructure. There are processes that need to be written and policies to be defined. In the event that there is a surge in activity, the security solutions in place may not be able to scale to meet that need. This white paper will explore how security cloud-based solutions can represent a scalable, cost effective, and efficient solution to meet security and compliance needs.

Overview of Network Security

It is virtually impossible to think of how business was accomplished before there were desktop computers and computer networks. Today, everything from the mundane to the most critical business process requires a computer to accomplish. Today, staggering amounts of information and data are transported over the network from one computer to another. Today, information that could fill a warehouse is stored on network-accessible hard drives. Today, almost every aspect of the computer and computer network feel as if they are critical elements in the business processes necessary to get the job done.

Technology is a double-edged sword though. For all of the benefits and efficiency computers and computer networks provide for organizations, it also helps thieves and attackers to access the data more easily as well. The convenience provided by networking, enabling employees to communicate with each other in the blink of an eye, share data, and access stored information quickly, also enables an attacker to reach out to each of those computers on the network or to gain unauthorized access to the data. There are a variety of threats that organizations need to be aware of and defend against. The greatest concerns or most prevalent threats include:

Malware

As technology has changed and evolved through the years, attackers have also matured in their own way. Viruses used to be written primarily by teenagers looking for little more than making a name for themselves in the hacker underworld. The goal was to wreak the most havoc or do the most damage in the shortest amount of time to gain notoriety.

Now, malware has evolved into a tool for organized crime and professional thieves. Rather than developing attacks designed to gain the most attention, viruses, worms, and other malware are designed to fly under the radar and remain undetected for as long as possible. Instead of malware that simply destroys data or overwhelms the network with more activity than it can handle, attacks are designed with profit in mind.

Network Intrusion

Unauthorized access to the network or network resources is another major concern. Previously, companies only really needed to worry about external attackers that might try to gain unauthorized access into the network. Over time, the threat has grown to include internal users that may attempt to access resources they are not authorized to access, as well as a need to monitor outbound network traffic to ensure no sensitive or classified company information is leaked in any way.

Organizations that have wireless networks implemented have additional risks to consider. It is easier to control and police data traveling along an actual wire between two points. With wireless networks the data is just there, floating in the air for anyone within range to intercept. Encrypting the wireless data can help, but there are ways to break some wireless encryption protocols and businesses need to understand the risks and how to protect against them.

Security Compliance

Another serious concern for most companies is compliance with legislative mandates and industry guidelines. With government regulations such as SOX (Sarbanes-Oxley), GLBA (Gramm-Leach-Bliley Act), and HIPAA (Health Insurance Portability and Accountability Act), or industry guidelines such as PCI DSS (Payment Card Industry Data Security Standard) or BASEL II, it is a virtual certainty that a given organization will be impacted by at least one compliance requirement.

Each of these regulations applies to a specific field or industry, but depending on the type of business in question it is possible that they may fall under multiple compliance mandates simultaneously. For example, a publicly traded financial institution must comply with SOX by virtue of being publicly traded. If the financial institution is a bank, they also must comply with BASEL II and FFIEC requirements. If they accept or process credit card transactions, they are also required to implement network and data security controls per the PCI DSS guidelines. It can be quite daunting and confusing for an administrator to comply with multiple regulations and ensure that the company remains compliant with each of them while also addressing any conflicts or overlaps between the mandates.

Challenges of Traditional Security

There are established tools and technologies to protect against most threats. Security products such as antimalware, firewalls, and even intrusion detection or prevention systems (IDS / IPS) are implemented in many companies at both the network and endpoint levels. The tools and solutions themselves are not the problem. The issue for many companies comes down to the time, money and personnel resources that must be dedicated to updating, upgrading and maintaining the tools and solutions to ensure the continued security of the network and computer assets. Scaling the security as the needs of the company grow, keeping IT personnel skills and knowledge current, and coping with surges in demand are all serious issues for security administrators to deal with.

Growing Pains

As the company grows, either through organic growth based on its own success or through mergers and acquisitions, the security infrastructure that has been developed must be able to scale to meet the needs of the organization. Expanding the capacity of the security technologies may include purchasing additional hardware such as firewall or intrusion detection appliances to protect the network perimeter. New hardware also means an increase in power consumption, as well as a greater need for cooling in the server room or data center. It may also require running power or cables and modifying the network infrastructure to accommodate the additional hardware. For software based solutions such as endpoint antimalware or firewall products, or agents that might be required for hardware based technologies, organizations must deploy, install, and maintain the software on new endpoint systems as the company grows.

IT Training

In order to ensure that security is implemented and maintained properly, the personnel tasked with administering the security products have to be properly trained. The bad guys will continue to develop new and innovative attacks, and security vendors will continue to develop new techniques for addressing those attacks. Stagnant IT skills are not an option. Providing training for IT personnel and keeping their skills current to adapt with the changes in the threat landscape and update their knowledge to reflect emerging technology trends can be one of the most expensive components of the network security budget.

Spikes in Demand

The security infrastructure can only handle so much. An organization architects its security to address normal levels of network traffic and a predicted number of users. If for any reason there is a temporary surge that exceeds the capacity of the security infrastructure it could result in a denial-of-service as the overload causes the security appliances or applications to slow to a crawl, and activity and attacks that should be logged may be missed due to the inability of the infrastructure to keep up with the spike in demand.

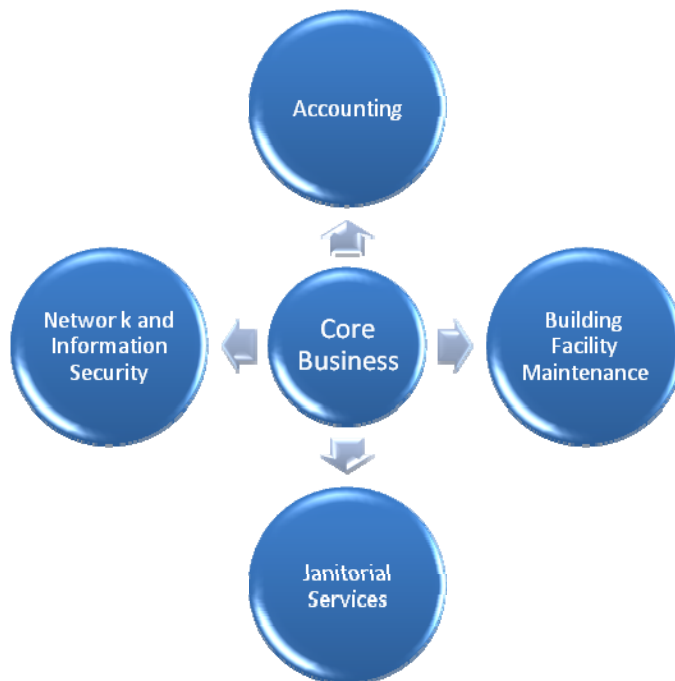
The Bottom Line

Companies need to protect their own intellectual property and data assets. They also have an ethical, and often legal, obligation to protect customer or consumer information as well. Sooner or later though, the degree to which a company protects their data comes down to money. Security is an expense which will hopefully protect the company from an even greater loss, but that type of reverse ROI (return on investment) logic is a tougher sell than investing in products or technologies which equate directly to revenue. The hardware, software and training that go into properly securing an organization and keeping it secure over time is a tough pill to swallow for many organizations which often leads to cutting corners and taking shortcuts that leave the company vulnerable.

Addressing Needs with Cloud-Based Security Solutions

There are many services required by companies that are typically outsourced. An automobile manufacturer is not in the business of keeping buildings clean, so they outsource that job to a janitorial service of some sort. A law firm does not exist to do accounting, so they typically outsource that task to an accounting firm of some sort. Generally, companies want to stay focused on the tasks and activities that generate revenue and let other entities worry about those jobs that don't generate revenue. That is also true for network and information security which is why more organizations are looking at cloud-based solutions as a viable solution for their network security needs.

Rather than having to keep up with changing trends and emerging concepts in the janitorial, accounting, or network security industries, companies can focus their attention on their own industry. Relying on a third-party that does nothing but information security ostensibly means that your network is in good hands. It becomes the job of the third-party to ensure that the tools used to protect your data keep up with the threat landscape and that the personnel entrusted with administering those tools is trained and stays current with the latest attack techniques and defensive strategies. Cloud-based security also means that your security infrastructure does not require an upfront capital investment, it can be deployed faster, and it is maintained by the provider, freeing the company to focus on its core business.



No Capital Investment

Implementing security internally requires purchasing hardware and/or software. In the IT world, capital expenditures can be substantial, and security is no exception. Rather than allocating a significant chunk

of the company budget for an upfront capital expense in hardware or software which will likely be obsolete by the time it is fully deployed and implemented, a company can engage cloud-based security to meet the security needs of the organization. The cloud-based solutions provider will ensure that the hardware and software being used are kept current without the company having to constantly upgrade and invest in the security infrastructure.

Quicker Deployment

Relying on a cloud-based security solutions provider generally means a quicker deployment time. Organizations that want to implement security on their own have to dedicate a significant amount of time and energy into understanding what is at risk, what the threats are to their environment, and what the best strategies are to protect their data. They then must go through a process to explore the options in terms of hardware and software and go through evaluations and pilot tests to determine the right tools and technologies for their needs. At that point, they still have to purchase it, deploy it, and configure it in order to protect the network. By offloading responsibility to a cloud-based security vendor most of these steps are eliminated and the protection the organization needs can be in place and protecting network assets in a fraction of the time.

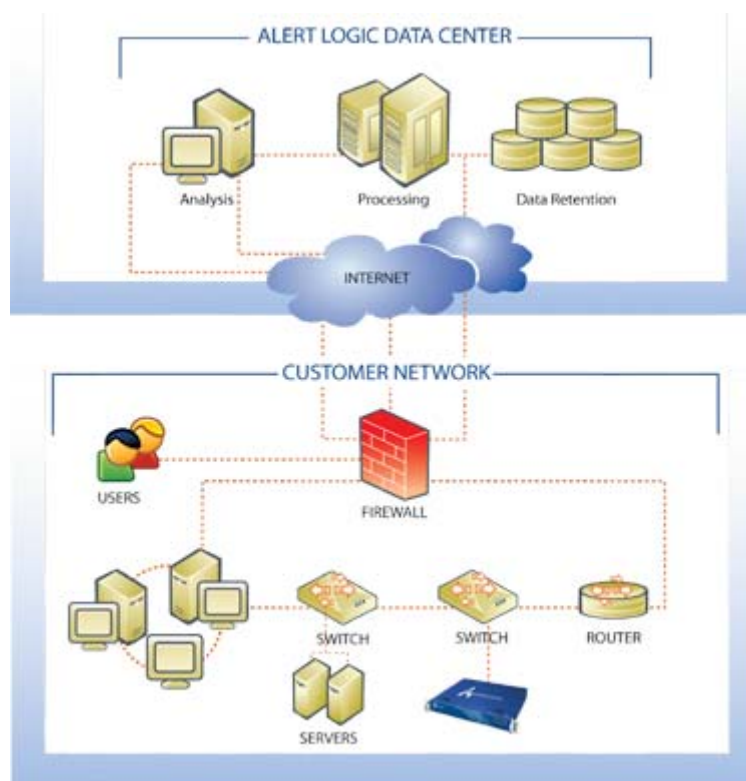
Self Maintaining

Companies that deploy and administer their own network security also have to maintain it. That means keeping hardware and software up to date. That means troubleshooting the appliances and applications when problems arise. By utilizing cloud-based security solutions, the organization can focus on their core business and let the provider worry about maintaining the security infrastructure, keeping hardware and software current, and keeping the personnel managing the security infrastructure trained and educated on the latest security threats and security strategies.

Meeting Evolving Security Needs

Alert Logic is revolutionizing the way IT compliance and security solutions are designed, delivered, and utilized. Their cloud-based security platform is designed for rapid deployment, zero maintenance, and maximum ease of ownership for customers and partners. There are two main components that make up the solution. The network appliance resides on the customer network and performs the function of collecting and forwarding log, threat, and vulnerability data to the Alert Logic data center.

The cloud-based component exists in the Alert Logic data center and takes care of securely archiving and analyzing data from the customer network, as well as all other Alert Logic customers around the globe. The cloud-based component also provides the customer a web portal where customers can view real-time feedback and historical trend information regarding their security as well as the current threat landscape around the world.



Alert Logic Threat Manager

To protect the customer network and provide a simple means of security compliance, Alert Logic developed Alert Logic Threat Manager. Threat Manager monitors network traffic and provides constant

protection against malware threats regardless of whether they originated from a VPN connection, a wireless access point, a partner network connection, or any other source.

Threat Manager provides customers with both proactive and reactive defenses by combining vulnerability management and intrusion protection in one integrated solution. Alerts from the Threat Manager are transmitted to the Alert Logic data center. The expert system hosted in the Alert Logic data center aggregates and correlates the vulnerability data and real-time threat information from all Alert Logic customers to help proactively protect against emerging threats while also eliminating false positives and identifying the valid security incidents that need attention.

As a supplement to Threat Manager, Alert Logic Active Watch monitoring service delivers an additional layer of intrusion analysis and incident response. Alert Logic's Security Analysts are monitoring customer data 24x7x365 in the Alert Logic Security Operations Center (SOC). Alert Logic Security Analysts notify customers when security incidents occur and assist in taking effective action against attacks.

Alert Logic Log Manager

Log data is as important as it is tedious. Many organizations miss critical warning signs, or lose valuable forensic evidence because they either don't properly collect and manage their log data, or they don't have personnel with the knowledge and skills to know what to do with it. Alert Logic's Log Manager is the only on-demand log management solution available.

Log Manager collects, aggregates, and then transports that information to the Alert Logic data center where the log information is processed and analyzed. The log data is securely archived in the Alert Logic data center where it can be accessed for reporting or forensic analysis. Customers can manage their log data from any web browser, while the tasks of configuration, tuning, and upgrading the logging infrastructure is handled automatically by Alert Logic.

Alert Logic is an established leader in log management, and their on-demand platform is an ideal solution for small and medium organizations, and even some enterprises, to address their security and compliance needs in an efficient and cost-effective manner. With years of experience and hundreds of satisfied customers, Alert Logic is a proven provider of cloud-based security solutions.