netmagic®
An NTT Communications Company

WHITEPAPER

Delivering the Security Promise

Cloud based security services

Demands placed on the IT function within organizations have never been higher. Business risks are increasing as companies embrace the Internet for efficiency, sharing sensitive information with employees, customers, and partners using public networks. Tighter security to prevent data breaches and ensure constant information access, however, often conflicts with staffing and budget limitations. Managed security services have become a simple, cost effective solution as companies expand workforce mobility and remote access to their networks, increasing the need for 24/7 monitoring.

Who should read this whitepaper?

CSO, CISOs, Managers, Compliance Officers, Heads of Security, CIOs, and Project Managers faced with the challenge of managing enterprise security. This can include mail security; compliance; IT risk; and the monitoring, identification, and remediation of security incidents and events.

Managed security services will be the fastest-growing segment of the managed services arena, expanding at a compound annual growth rate of nearly 20% over the next few years, according to Gartner.

As the threat landscape continues to evolve and grow all the more complex, Cloud-based security solutions offered by MSSPs will find more acceptability. With the recent technological developments, security applications delivered as cloud-based services through an MSSP offer an innovative platform to manage security threats vis-à-vis premise-based solutions that still have their advantages - depending on an organization's requirements.

Security technologies including firewalls, network and host intrusion detection, and prevention systems have created a tremendous volume of information which can be valuable provided the information gathered by the various security devices are co-related. Handling this enormous amount of data puts a lot of pressure on the IT staff and makes security problems all the more challenging. As a result, organizations that currently resort to managing security in-house are looking for alternatives. The options available for these organizations are either increasing the size of the in-house security team, or outsourcing all or some security management to a managed security services provider (MSSP).

MSSPs offer high-availability security operations centers (SOCs) to provide remote management and monitoring of security devices and events. These centers provide 24x7 services thereby enabling organizations which outsource, to reduce the number of operational security personnel an enterprise must hire, train, and retain in order to maintain an acceptable security posture.

With the recent technological developments, security applications delivered as cloud-based services through an MSSP offer an innovative platform to manage security threats vis-à-vis premise-based solutions that still have their advantages - depending on an organization's requirements. However, several key factors should be considered when deciding between on-premise and cloud-based security. These include an organization's readiness to outsource its security function and the capability of its IT staff to manage a premise-based solution. Organizations with unique requirements may require specialized security solutions. Cloud-based security solutions find a greater appeal with small and medium size organizations as without the need to purchase and deploy equipment; these can be implemented much more quickly. Cloud-based security solutions charge a monthly subscription fee and eliminate the capital expenditures required for premise-based solutions.

As the threat landscape continues to evolve and grow all the more complex, Cloud-based security solutions offered by MSSPs will find more acceptability by organizations whether large or small. The underlying reason being that any large-scale security infrastructure program can take a long time to deliver ROI and bring measureable benefits to the organization as compared to the investments made.

IT Security Challenges

Cyber crime has evolved from one off hacking incidents to a full-scale criminal activity in the modern world. Modern day hackers and malicious code generators create threats that have the potential of seriously damaging the health and business of an organization. Threats generated by such malicious entities include:

Viruses/Malware/Spyware:
These can be transmitted through infected emails, URLs, downloaded data and so on. The purpose of these attacks range from productivity loss to stealing data

Spam:
These are bulk emails sent out to numerous people with the aim of tricking them for monetary gains. Spam mail often carries viruses too.

Distributed Denial of Service (DDoS):
This form of cyber terrorism is fast gaining pace and popularity as a means of extortion and profiteering as DoS can bring the entire business operation to a standstill, causing huge losses.

Data Theft / data leakage:
This is yet another method employed by internet criminals to make quick money. Confidential data like addresses, social security numbers, account details etc. are 'stolen' from otherwise secured databases and supplied to entities seeking to mass contact people without solicitation, often to spammers.

Botnets:
While sophisticated hackers do not attack directly, unsuspecting organizations are caught off-guard if their IT infrastructure is used as a channel to attack the final target. Such instances of IT assets becoming part of a botnet can create significant legal liability for the organization.

The threat landscape continues to evolve and become more complex

According to the Global Internet Security Threat Report (ISTR), cyber-criminals have become increasingly professional and commercial in the development, distribution, and use of malicious code and services. While cyber-crime continues to be driven by the motive of financial gain, cyber-criminals are now using more professional attack methods, tools, and strategies to conduct malicious activity. Based on the data collected in the report, the current security threat landscape is predominantly characterized by the following:

- Malicious activity has become Web-based
- Attackers are targeting end users instead of computers.
- The underground economy is becoming consolidated and mature
- Attackers and attack activity are adapting rapidly

In addition to malware, Distributed Denial of Service (DDoS) attacks are bringing mission-critical systems and business operations to a standstill. These attacks lead to loss of revenue opportunities, decrease in productivity and damage business reputations for organizations. It has been observed that over the past few years, DDoS attacks have grown in frequency and are carried out for a specific purpose such as extortion, market manipulation and cyber terrorism.

Large-scale data breaches have become all the more prevalent. According to an article in Forbes in 2008, the number of personal records that hackers exposed, such as Social Security numbers, medical records and credit card information had skyrocketed to 220 million. This represents the largest collection of lost data on record.

Organizations falling victim to such attacks find it difficult to bring applications and operations back on track and require extensive cleanup of the entire IT infrastructure, applications and processes. While large organizations have the scale and scope to have expert security services being operated in-house, most companies, especially small to mid-sized organizations, face several challenges like:

Set up/ Running Costs: SMBs generally cannot afford an in-house IT security set up. In addition to the massive expenditure on purchase of infrastructure which includes software, hardware and personnel, there is also the cost and administrative liabilities of running an in-house security service.

Efficient Threat Management: Prevention, detection and elimination of threats is what IT security is ultimately about. New threats are being generated round the clock across the globe and take less than a day to have a worldwide impact. This leaves organizations with barely any time to detect such threats and take preventive measures. Also, a robust set up is required to comprehensively cover all aspects of IT across the organization. It takes an expert MSSP to provide such levels of IT security.

Data Security: Personnel handling IT security have access to all of the data of the organization, including the most confidential. Not being bound by non-disclosure contracts or standards of governance, the risk of data leaks and thefts can be high.

Organizations also have to face the repercussions of brand damage. In addition to the financial losses incurred in fines and legal costs to fight lawsuits and pay out huge settlements, companies have to deal with the loss of customers and plunging market shares.

Why is it difficult to manage security in-house – some common hurdles

With customers and other stakeholders accessing critical product and service data via open networks such as the internet, organizations must ensure the integrity of the information conveyed. Failure to do so can jeopardize their reputation and brand equity. Organizations face a number of barriers when trying to manage effective security programs in-house. Some of these are as listed below:

Organizations falling victim to cyber attacks find it difficult to bring applications and operations back on track and require extensive cleanup of the entire IT infrastructure, applications and processes.

Security A Core Requirement But Not A Core Competence

Managing information security requires constant vigilance and strict accountability for every change in the state of network and systems connected to it. Organizations often lack the necessary skills to manage this daunting task.

Need To Find, Hire And Retain Security Staff

Owing to the strong market demand for information security professionals, organizations find it extremely expensive and difficult to retain them. The high attrition rate reduces a company's ability to effectively safeguard its valuable information assets.

Security Staff Overloaded With Daily Operations

Security staff often lacks time, expertise and technical resources to provide effective enterprise-wide monitoring and management on a 24X7X365 basis.

Need To Develop A Framework For Identification And Escalation Of Security Incidents

Determining what constitutes a security incident may be a difficult task. Traffic that looks regular may be malicious when correlated with other security information. With low margins for errors, developing a framework that can be consistently and quickly executed may be difficult for organizations.

Managing huge amount of data generated by security products

Protecting corporate information assets on a 24X7X365 basis from malicious attacks means that security experts must analyze disparate data from various security devices such as firewalls and intrusion detection systems (IDSs). Consolidating this data for viewing and correlating may be difficult as software tools to consolidate this data lack the ability to aggregate meaningful information.

Growth in sophistication and volatility of threats

The threat landscape has undergone a tremendous change – from a large scale pandemic threat to quieter and targeted attacks engineered by cyber criminals. These attacks spread slowly to avoid detection and can cause havoc before security controls are put in place.

Proactive Intelligence

Setting up an in-house Security operation Center (SOC) may be a difficult task for most organizations. More so, these organizations may not be aware of emerging threats and vulnerabilities.

Cost-effective security on a 24X7 basis

Increased demands for business continuity coupled with availability demands from customers and business partners is making many organizations look for cost effective security protection on a 24X7X365 basis. However the cost of building and staffing a SOC is too high for most of them regardless of the size of the security architecture being managed.

The cost of managing security in-house

To build upgrade maintain operate, and control IT security systems, any in-house security management program needs personnel and supporting hardware, software and equipment. These in-house programs require huge cash outlays in the form of:

Large-scale data breaches have become all the more prevalent. According to an article in Forbes in 2008, the number of personal records that hackers exposed, such as Social Security numbers, medical records and credit card information had skyrocketed to 220 million. This represents the largest collection of lost data on record.

Hardware and Software Costs

For in-house security management, organizations have to incur the cost of all hardware and software in addition to associated maintenance and support costs. This includes servers, PCs and peripheral equipment, as well as all associated operating systems, databases, applications, and security software.

To support security operations additional hardware and software may be required. This may include system and network management tools, fault management systems, help desk systems, and correlation technology. Additional costs may be incurred for integration and customizing the software as per the IT environment and these maybe several times the cost of the software purchased.

Maintenance Costs

The total cost of ownership of the software and equipment will also include the maintenance fees charged by the provider. This again leads to an increase in the overall cost for having an in-house security program.

Certification and Attestation Costs

In order to make security programs more effective and comply with industry regulations, many SOCs are becoming ISO7799 or ISO27001 compliant. Other regulations that need to be adhered to include Sarbanes Oxley, MiFID or Basel II (necessary for environmental audits). While these certifications are difficult to obtain, the real challenge comes from the fact that all processes essential for day-to-day operations have to be developed accordingly, which increases the cost of operation.

Staffing and Training Costs

To staff a true 24x7x365 SOC requires a minimum of seven full-time employees. While IT departments, network groups or even security teams may have the talent/expertise, they rarely have the ‘current and well-practiced’ skill set that is required to execute real-time or even batched security event analysis on the millions of events that are generated from their environment on a daily basis to find the one or two true security incidents.

Building and maintaining a SOC

Most organizations find it too expensive to build or lease an SOC because the cost can exceed $10 million USD in capital expenditures. They also have to consider the need for power, HVAC, and fire suppression systems. In addition, a disaster recovery plan that would take into account the creation of a failover facility should be taken into account.

Therefore, organizations that choose to work with a MSSP benefit from these significant investments as well as the expertise of trusting their business to security experts.

Cloud based security service – the emerging option for Managed Security Services

Cloud computing provides several advantages vis-à-vis on-premise security software and systems for delivery information security. Cloud-based security services also known as managed security or hosted security or security software as a service provides security functionality over the Internet. Here, the customer does not own the security applications but subscribes to a complete solution delivered remotely. In a cloud based delivery model, the customer need not purchase hardware/software licenses. There are no associated maintenance fees. The cloud delivery model helps in reducing the security complexity. Organizations gain access to sophisticated security technology and up-to-the-minute security intelligence without the capital expense, overhead and management responsibility associated with on-premise solutions.

Cloud-based security services help organizations to carry out their routine security activities more efficiently and cost-effectively by utilizing technology and infrastructure provided by a trusted third party or an MSSP.

So what are these services?

Cloud based security services include managed services and technology and security intelligence to integrate security with existing business processes, prevent malicious attacks against an organization, prevent misuse, and address key stakeholder demands. Cloud-based security services help organizations to carry out their routine security activities more efficiently and cost-effectively by utilizing technology and infrastructure provided by a trusted third party or an MSSP. Inturn, a cloud based security solution enables organizations to reduce the underlying costs and take advantage of a flexible pricing based on usage. The complete onus for the application functionality, deployment, performance and maintenance, is taken by the MSSP or cloud based security provider, thus, freeing the client's resources from these cumbersome activities.

Cloud-based security services offer the following benefits over traditional on premise security deployments:

- No expensive, on premise security hardware to purchase, install and maintain
- No stand-alone software to constantly update and patch
- Rapid deployment and self-service through a web-based portal
- Ability to scale and expand security coverage quickly, without investing in additional infrastructure
- Flexible, service-oriented pricing and service level agreements

As traditional security services involve huge capital outlays for deployment, personnel, and maintenance, Cloud-based services reduce these expenses and provide an ideal delivery method for many external security functions, including:

- Vulnerability scanning and testing
- Web/URL filtering
- Security event management
- Security log management
- Email security

In addition, cloud-based security services provide up to date security intelligence and analytics so that organizations have the latest technology required to counter any malicious attack. Z

Who benefits from Cloud based security services?

Advanced security technologies can only be implemented by large organizations that have the requisite budget and expertise to implement, monitor and manage advanced security solutions. Smaller and medium sized organizations may find it difficult to implement such advanced security solutions due to budget constraints and absence of skilled resources to manage them.

As compared to large scale on premise security applications, cloud security solutions require negligible up-front capital investment and deployment costs. Additionally, delivery model based on the cloud lowers an organization's operating costs. Cloud security services also help in enabling a customer's limited operational resources towards more strategic initiatives that drive real business value. Consequently, compared to traditional, on premise security implementations, organizations leveraging the cloud spend less time managing systems, troubleshooting technical problems, and responding to the most recent security threat.

Cloud security services help organizations to scale for growth, staff changes and shifts in business focus. Additionally, it speeds time to protection, reduces demands on internal resources, enhances profitability and increases focus on operational excellence.

Not only a cloud-based delivery model transforms an organization's approach to security but it also makes security decisions more strategic. The cloud model aligns security technology with constantly evolving business requirements. Offering a centralized view of security, it provides integrated security intelligence so that customers can make better educated business decisions about how to reduce risk.

A cloud based delivery model provides a consolidated view (360 degree view) of the security posture across the organization. This way, business enterprises can keep a track of the number of remediation tasks assigned and completed, the number of vulnerabilities reduced, and the cost savings associated with cleaner traffic and more efficient use of bandwidth.

The flexibility and robustness of a cloud security services portal improves regulatory compliance efforts by organizations. The information on incidents i.e., vulnerabilities, security events, log files, etc. is captured and maintained for auditing and investigation purposes. The cloud-based delivery model leverages existing technology investments such as routers, application servers and security software. Cloud security services help organizations to scale for growth, staff changes and shifts in business focus. Additionally, it speeds time to protection, reduces demands on internal resources, enhances profitability and increases focus on operational excellence.

How to select a cloud-based security service provider?

An efficient MSSP will possess the right combination of service delivery experience, managed services, technology, and security intelligence. Cloud security services should be delivered by security-focused providers who are experts in this domain and offer:

- Proven expertise in delivering security via the Internet
- A central portal where customers can view their security posture real-time
- A complete managed security services platform including device management and cloud-based security services
- A comprehensive suite of security solutions to protect the entire IT infrastructure
- Real-time, proactive security intelligence on threats and vulnerabilities
- The ability to work with existing infrastructure and security technologies
- An understanding of how risk management affects business processes like application deployments, compliance management, supply chain and more
- A strong audit and compliance posture that ensures alignment with your organization's needs
- A global delivery footprint that provides global geographic coverage and continuous service availability

Industry Leading MSS Solutions:

- Managed Network & Server Protection
- Managed Application Protection
- Managed & Monitored Firewall Protection
- Managed IPS & IDS
- Managed Unified Threat Security
- Vulnerability Assessment & Penetration testing
- Incident Monitoring & Alerting

Components of the Managed Security Services suite from Netmagic Solutions:

The MSS suite comprises:

- Vulnerability Assessment and Penetration Testing (VAPT)
- Comprehensive Network Attack Monitoring (CNAM)
- Webcontrol
- Appsecure Web Application Firewall
- Email Security

Vulnerability Assessment and Penetration Testing

Guarantee uninterrupted access to your online presence & data. Comply with stringent regulatory requirements. The on-demand automated VAPT solution lets you run tests over the Internet anywhere, anytime. VAPT blends automated testing with security expert analysis to provide high-quality test coverage, and faster. The unique technology identifies all possible attack vectors.

Appsecure

Appsecure, a web application firewall (WAF) service from Netmagic, delivers optimal protection against SQL injection, cross-site scripting, website defacement and many other types of attack. Appsecure is powered by an award winning application firewall, dotDefender, from Applicure Technoglogies (www.applicure.com). Netmagic provides the complete management of this firewall on your web server and delivers it in a SaaS model.

Webcontrol

Webcontrol from Netmagic Solutions is a web security service that provides policy-based secure internet access for any employee, on any device, anywhere. WebControl reduces your total cost of ownership and streamlines your IT security management through a cloud based model that delivers an ultra-low latency solution. Netmagic offers three subscription packages along with add-on modules that will help you secure and manage every aspect of your employees' internet usage.

CNAM

Comprehensive Network Attack Monitoring (CNAM) is a 24X7 real-time threat monitoring and detection solution that protects your IT infrastructure from cyber-threats. It correlates information from multiple devices and applies intelligence to determine if any activity is suspicious. Available on a Software as a Service model from Netmagic Solutions, CNAM ensures that you pay a predictable monthly charge while applying global security intelligence for to your business.

Managed Security Services delivered via the cloud by Netmagic Solutions

Netmagic Solutions is India's leading provider of managed IT services including Managed Security Services. Netmagic offers its customers end-to-end solutions for their IT security needs, covering risks across data centers and corporate usage. With a market repute of reliability and experience to match, Netmagic Solutions has state of the art infrastructure, best of breed technology and industry best practices and processes, giving its clients a unique and complete blend of reliability, security, efficiency and affordability.

Netmagic Solutions gives its customers the option to choose from a unique framework that ensures market leading performance. Its three stage security framework includes:

Monitoring: 24/7/365 real time monitoring that enables detection of threats well ahead of time, facilitating timely precautionary measures.

Manage / Control: We understand that our clients have their unique individual IT security needs and take great care to provide them with an MSS solution customized for them, which makes better control of malicious entities and threat, increasing security levels.

Validate: Although our constant monitoring and controlling of our clients IT perimeters ensures safety, we also regularly analyze and validate their security framework to prevent breaches before the threat even arises.

MSS Offerings from Netmagic Solutions

With Netmagic Solutions' robust Managed Security Services, organizations can transfer all their IT security needs and requirements and relax in the knowledge that the safety of their IT is in the best hands in the industry. Netmagic offers the following solutions as a part of its Managed Security Services Portfolio:

InfraSecure: Comprehensive network attack management, vulnerability analysis and automated penetration testing, web security and web application firewall

InfraManage: Delivers 24x7 operations support and coverage for mission-critical IT infrastructure with end-to-end management of incidents, faults, configuration, change, availability, performance and security.

Managed Hosting: Managed Firewall, IDS/IPS and Data Backup & Restoration

Email Security: Anti-virus, Anti-malware, anti-spam and phishing filter

Disaster Recovery and Business Continuity Plan Consulting

Conclusion

As managed security services market is gradually picking up, similarly the demand of trusted MSSPs are also on rise. Issues like tight budget, lack of adequate skilled staff, lack of proper infrastructure etc. are obviously accelerating the growth of this industry. Partnering with a cloud based Managed Security Services Provider like Netmagic Solutions provides the much needed support in the form of state of the art infrastructure, staff that is experienced and experts in the field and high levels of scalability and performance. For organizations that have not evaluated cloud-based security options, now may be a good time to revisit these solutions. As cloud-based security solutions grow and mature, more creative options will be developed and prices will decrease as more security vendors develop comparable solutions.

For more information visit www.netmagicsolutions.com

1800 103 3130

marketing@netmagicsolutions.com

Follow Us: http://blog.netmagicsolutions.com http://twitter.com/netmagic http://linkedin.com/company/netmagic