CORE
MANAGED IT | SECURITY | AUDIT
A HENAGON COMPANY

www.coreitx.com

Sensible Security WhitePaper

Did you know -?

In 2015, there was a total of 780 data security breach in U.S. alone – resulting in 177,866,236 personal records being exposed. 40% of these breaches were targeted towards businesses. (Source)

We have already seen some of the most high-profile data security breaches in 2017 - potentially affecting millions of individuals' payment cards' (e.g., credit cards and debit card) information, personal identifying information (e.g., first and last name, Social Security numbers, address, birthday, etc.), and medical records. Some of these were the Chipotle Payment System Hack, Hackers setting off Emergency Weather Sirens in Dallas, Gmail Phishing Scheme and the IRS Under Assault.

And as far as small companies are concerned, 60% of small companies that suffer a cyber-attack are out of business within six months.

What is managed infra services?

After setting up a business, security is a major concern for all organizations. Managing security issues can be difficult, if the root causes for such threats cannot be identified before laying the foundation of IT infrastructure. Managed Infrastructure Services is considered a crucial driver for growth and innovation. A smart and well-managed infrastructure services empowers businesses with agility, flexibility, enhanced efficiency and a comprehensive security. Though the market is seeing a vast transition from traditional security to Cloud solutions due to low CAPEX, many providers offer Cloud services just to stay in the current 'trend' and see this change as an alternative revenue stream for now. Many SMBs, if they are lucky, manage to get complete security options from Cloud while others find it difficult to run with Cloud after migration. So, new SMBs become prone to threats like information thefts, viruses, worms, a loophole in security legislation and many other unknown factors till the market learns the ways of the Cloud.

A solution to this managed unified threat management system is through the implementation of Cloud computing, storage, security and allied infrastructure. With this in place, IT operations gain service quality with secure operational facets that propel SMBs to the market in a cost effective and efficient manner by focusing on technological innovation.

Managed infrastructure for SMBs

For a business to survive in the volatile market conditions, the basic requirement is to keep capital handy as well as opting for a comprehensive management policy that is flexible to accommodate the changes without incurring huge costs. Such a strategy makes sense and gives an enterprise enough opportunities to grow.

SMBs looking for a complete threat management system look at several solution packages as a way to implement security into their business – sensibly, and without incurring high costs. Simplifying risk management, information access management, data encryption, isolating business functions from auxiliary activities, protection from malicious software, etc. are a part of this package, ensuring that your business stays protected from security concerns. With a UTM, a service provider intends to provide a practical protection service that ensures peace of mind to enterprise owners.

A complete UTM solution

Owing to the need to integrate several additional components in order to address an ever-growing list of security issues, IT administrators find it challenging to secure networks against all kinds of threats. Apart from this, SMBs often are not able to manage an elite threat management system due to the obvious reason of high cost.

This is where the Unified Threat Management (UTM) solution steps in. UTM products are now being used by a large number of Small & Medium businesses, because of their wide-ranging network protection capabilities from blended threats – both internal and external. Moreover, UTM solutions are flexible, can be deployed in different scenarios and configurations. Its compact nature takes up less space in the data center rack.

UTM benefits to small & medium businesses

Small organizations were the very first users of UTM solutions – because of its cost-effectiveness, ease of configuration and optimum protection. Even today, UTM offers a range of benefits to small and medium businesses, because of – Reduced complexity: They have a single, simplified management console. Ease of deployment: UTM appliances can be easily deployed and configured by nontechnical staff.

Integration capabilities: UTM solutions have the capability to integrate with standard network configuration methodologies and technology standards.

Troubleshooting ease: A simplified management console enables reporting data and events and hence, may guide administrators in troubleshooting.

Easier management: The unified management console allows administrators to manage their security environment remotely.

Added simplicity: Multiple device management from a single provider simplify troubleshooting, licensing and technical support situations.

Better performance: The use of latest appliances ensures and enhance higher performance.

Reduced training requirements: A single security solution on a single platform minimizes the learning curve for IT personnel.

Regulatory compliance: The console gives administrators more granular and more individualized (and group) policy management controls.

Comprehensive Security: UTM offers a comprehensive security against malware, worms, Trojans, phishing attacks, intrusions, denial-of-service (DoS) attacks, key loggers, spam, and other threats.

Regulatory compliances covered through UTM

CoreIT UTM provides security to SMBs that are compliant with global regulations. Regulatory compliances like HIPAA, GLBA, PCI-DSS, FISMA, CIPA, SOX, NERC, FFIEC, etc. are covered through our UTM. This gives visibility through identity-based security and meets the requirements of regulatory bodies for secure and ethical work management in enterprises.

How CoreIT provides managed security services to SMBs

CoreIT's Cloud management services are versatile enough to provide a good security measure without creating a need for high investment, and now it brings to you a 'Sensible' way to protect your enterprise from threats with its Unified Threat Management (UTM) especially geared to the needs of small and medium businesses - known as Sensible Security

Let's look at the aspects covered under SENSIBLE SECURITY and address each area of significance in a detail below:

Risk Management

With Sensible Security, protection of data from every stream such as the internet, network devices, internal work flow, etc. can be ensured to reduce risks and vulnerabilities. The unique single-click port forwarding and outbound traffic filtering service control the inflow and outflow of data and traffic throughout the system to keep away spam and malicious programs from gaining an entry into the system by blocking them. Management of employee access with web surfing access policies can be established to ensure a complete monitoring over internet viewing. Additionally, employee remote machine access with certificate-based authentication via the SSL VPN can make communication between field-personnel and enterprise a controlled and monitored process.

Information Access Management

Protection of personal information of important personnel within an enterprise from unauthorized access can be ensured with CoreIT's Sensible Security. Secure network zones for critical data and systems with restricted access to the enterprise can be achieved with our UTM – thereby, simplifying data security. Apart from this, the physical segregation of network interface cards (NICs) for each LAN can be provided with the UTM firewall architecture. Such a measure would reduce improper configurations of the system architecture and allows management to follow a streamlined path.

Access Authorization

With Sensible Security UTM, sensitive enterprise and employee information can be protected from illegal access. Complete end-to-end control on access authority can be implemented to safeguard employee information, entry, and exit of data, monitoring of traffic and its controlled viewing, etc. and protect the enterprise from external threats.

Protection from Malicious Software

One of the best parts of CoreIT's Sensible Security is the cost saving on antivirus programs that are used by traditional on-premise IT companies. Sensible Security has an all-round in-built antivirus system for detecting, safeguarding and reporting intrusions from malicious software. Every fragment of data undergoes scans and the monitoring tool can be configured to enterprise requirements. Emails and other forms of communications are scanned to ensure a complete protection from malicious software by blocking them with reporting capabilities.

Password Management

Our UTM firewall can generate unique, changeable and randomly generated passwords for each administration operator. The system can be configured to incorporate policies and procedures for creation, safeguarding and change of passwords as per needs. Additionally, enabling and disabling of remote access management to specific/limited IPs can be ensured with CoreIT Sensible Security options.

Automatic Logoff

CoreIT Sensible Security can be configured to manage every security concern to minute details. Configuring the firewall for automatic log off after an electronic session or predetermined time of inactivity, etc. can be implemented. Such measures would prompt a sensible and controlled way of system use and also ensure proper authentication each time for system access.

Encryption and Decryption

Sensitive enterprise information can be encrypted and decrypted with Sensible Security UTM’s industry-leading cryptographic algorithms. This helps to keep the data protected during transit between multiple systems and can safeguard communication of valuable information.

CoreIT UTM as the Comprehensive Protection for SMBs

CoreIT Sensible Security and UTM gives an all-round protection with an advanced firewall, an intrusion detection and prevention system, full VPN support for remote working, managed antivirus for maximum 5 users and a 24x7 unified management of threat from our support team. This premium service comes at a very cost-effective price and helps your enterprise stay protected from all possible threats.

To conclude, UTM is the best way to stay protected without making a large investment. Speed and accuracy with controlled and identity-based access make it a secure method to handle enterprise operations. Moreover, work flow gets regulated and a transparency is achieved with managed infrastructure services. CoreIT looks into the future where UTM would be a fundamental part of small businesses to stay protected and enjoy a premium standard of security for all its commercial operations in a sensible way.

CORE
MANAGED IT | SECURITY | AUDIT
A HENAGON COMPANY

☎ 1.212.271.8732
✉ info@coreitx.com
🌐 www.coreitx.com