

Situation

LockNET, Inc., based in La Crosse, Wisconsin, is an MSSP (Managed Security Services Provider) specializing in the integration of network security for financial, healthcare, government, education and general business clients. LockNET began in 1980, initially under the name Computer Bay, and have shown extensive growth while evolving to meet the changing needs of its customers. Its mission is to provide small and medium sized businesses (SMBs) a secure and stable managed information network and offer a variety of products and services.

Most SMBs don't have the manpower or the financial capital to maintain an enterprise level network and therefore enterprise network security. LockNET has solved this problem with its nfire™ network security management product offering. Providing network security assessment, regulatory compliance consulting and network security management services for secure client networks, including remote monitoring and maintenance for its SMB customer is the core of LockNET's nfire business.



By providing comprehensive network security reporting and full Internet content management, nfire goes a step further in protecting its customers' network. nfire provides a Unified Threat Management (UTM) solution that evolves with the constant barrage of external attacks. Comprehensive threat reporting also helps its customers align with current compliance regulations, such as those in place for financial institutions.

After deploying a SonicWall firewall and Symantec desktop product as part of the nfire solution offering, LockNET quickly realized that the solution didn't have the robust capabilities that its customers were asking for – integrated firewall, VPN, intrusion prevention and comprehensive reporting, to name a few.

"After discussions with our customers, we quickly realized that we needed integrated security functions," said Steve Lubahn, vice president of sales and marketing at LockNET. "Based on customer needs, it was imperative for us to find a unified threat management solution that would easily scale to the growing needs of our extensive and expanding customer base."

Solution

After meeting with Fortinet and a thorough evaluation of the company's unified threat management product functions and management capabilities, LockNET recognized the opportunity to realize their goal of streamlining the deployment and central management of security services through the use of Fortinet unified security platforms. The Fortinet platforms integrate firewall, antivirus, Web filtering, anti-spam, VPN and intrusion prevention. One of the critical requirements for LockNET was to have an integrated solution rather than an offering composed of multiple vendors, such as SonicWall and Symantec. The integrated approach allowed LockNET to realize operational efficiency as well as keep deployment as simple as possible. LockNET also concluded that the management and reporting of security services would become much easier due to the common graphical user interface across all Fortinet platforms, protection and management platforms alike.

Because of Fortinet's unified threat management solution, LockNET has been able to replace its SonicWall firewalls and have standardized on Fortinet's FortiGate™ multi-threat security systems to provision its nfire network security management solution. LockNET's nfire network security offering provides firewall, antivirus, Web content filtering, anti-spam, VPN and intrusion prevention functionality to its small and medium business customers.

LockNET has installed many different models of FortiGate appliances ranging from the FortiGate-60 family of multi-threat security appliances through the FortiGate-400A multi-threat security system. In addition, they have also deployed FortiClient, FortiManager and FortiAnalyzer for

Deployment:
FortiGate-60 through the
FortiGate-3600
FortiClient

Industry:
MSSP

endpoint security and central management needs. Many of LockNET's end users are leveraging the FortiGate appliances to help create secure and encrypted VPN connections using the Internet between locations. This in turn helps to save customers significant dollars per month in connections between locations compared to traditional dedicated private circuits.

LockNET has also used multiple Fortinet installations at different locations to allow individual clients to establish disaster recovery and business continuity in the case of a failure at the main location. For endpoint security, LockNET uses Fortinet's FortiClient™ PC endpoint security on each customer machine, offering customers superior protection with a lower cost-per-device as compared to other competitive desktop antivirus software packages.

Deployed at LockNET headquarters is Fortinet's FortiAnalyzer centralized reporting system and FortiManager centralized management system. These devices allow LockNET administrators to easily manage and analyze traffic traversing the network for its customers. FortiAnalyzer systems are purpose-built appliances that provide valuable intelligence and simplify and centralize the collection and analysis of log and event data from Fortinet's FortiGate multi-threat security appliances. They deliver highly relevant network reports, valuable intelligence on network usage and assistance with demonstrating regulatory compliance. Since deploying the FortiAnalyzer and FortiManager, LockNET is now able to provide customers with detailed monthly reports on network usage and attempted attacks detected by Fortinet appliances located at each of the more than 200 customer premises.

Success

Since deploying the Fortinet solution, LockNET has been able to provide customers with effective managed security services, while also noting many operational advantages over their previous offerings. The FortiGate systems immediately met LockNET's needs for a more robust security solution but are also providing the MSSP with integrated network security services, better functionality, consistent GUI across product lines and increased reporting capabilities.

With Fortinet's integrated approach to network security, rather than having multiple vendors such as SonicWall and Symantec, for different security functionalities, LockNET is benefiting from having one vendor to partner with for success. This has proven to save time and money for the growing company while reducing the cost of services for LockNET's customers.

"Fortinet has allowed us to expand our offering from a basic firewall provided by multiple vendors to a single network security solution that includes firewall, VPN, intrusion protection, Web content filtering and much more," said Lubahn. "Fortinet's robust security solution along with its high-performance ASIC processing has allowed us to help our customers' businesses grow while ensuring their networks are secure."

With more than 200 Fortinet appliances deployed at customer sites, LockNET has benefited greatly from Fortinet's consistent GUI across product lines. Instead of having to figure out how to manage each individual appliance for different services, LockNET only has to know how to manage all services through one single interface and the knowledge transfers directly to all other Fortinet appliances.

Finally, unlike the previous rudimentary reporting capabilities from SonicWall, LockNET customers now receive detailed reports, including technical details for network security support staff and customized high-level summary reports for executives, giving everyone the right level of network security statistics and Internet usage they want. Not only is this added functionality beneficial to LockNET, but its customers are now able to receive detailed reporting on their network usage – something that wasn't previously available to them.

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection—including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: (Firewall, Antivirus, IPSec, SSL, Network IPS, and Anti-Spyware). Fortinet is privately held and based in Sunnyvale, California.

CAS163-1107