The Value Proposition for Hardware Security Appliances

Microsoft Forefront Enterprise Edge Security Best Practices - Hardened Security Appliances by nAppliance Networks

Background

General purpose business applications such as Financials, Document Management, Email systems, Manufacturing and inventory, and thousands of others exist to provide a flexible and customized business environment. These applications run on servers which also provide a flexible infrastructure to support any business environment.

This flexibility injects security and reliability vulnerabilities. Each of these systems require extensive configuration and ongoing management. Systems must be managed, tuned, backed up and meet corporate compliance guidelines. Disaster Recovery and change management practices must be put in place, all of which increases the support and maintenance costs.

Configuration changes and maintenance injects new security risks. Business systems must be shielded from security risks and threats from intrusions. This security is provided by security technologies which surround and integrated with the business systems.

Security from remote intrusion is provided by edge security devices. These systems include routers, packet-filtering firewalls, application-filtering multi-purpose firewalls, VPN appliances, and other special purpose hardware devices. The best case deployment scenerios for these technologies involve hardened hardware systems which are hardened special purposed appliance systems. These systems are manufactured by Cisco, Juniper and many others network hardware companies.

Network and Security devices have the following characteristics:

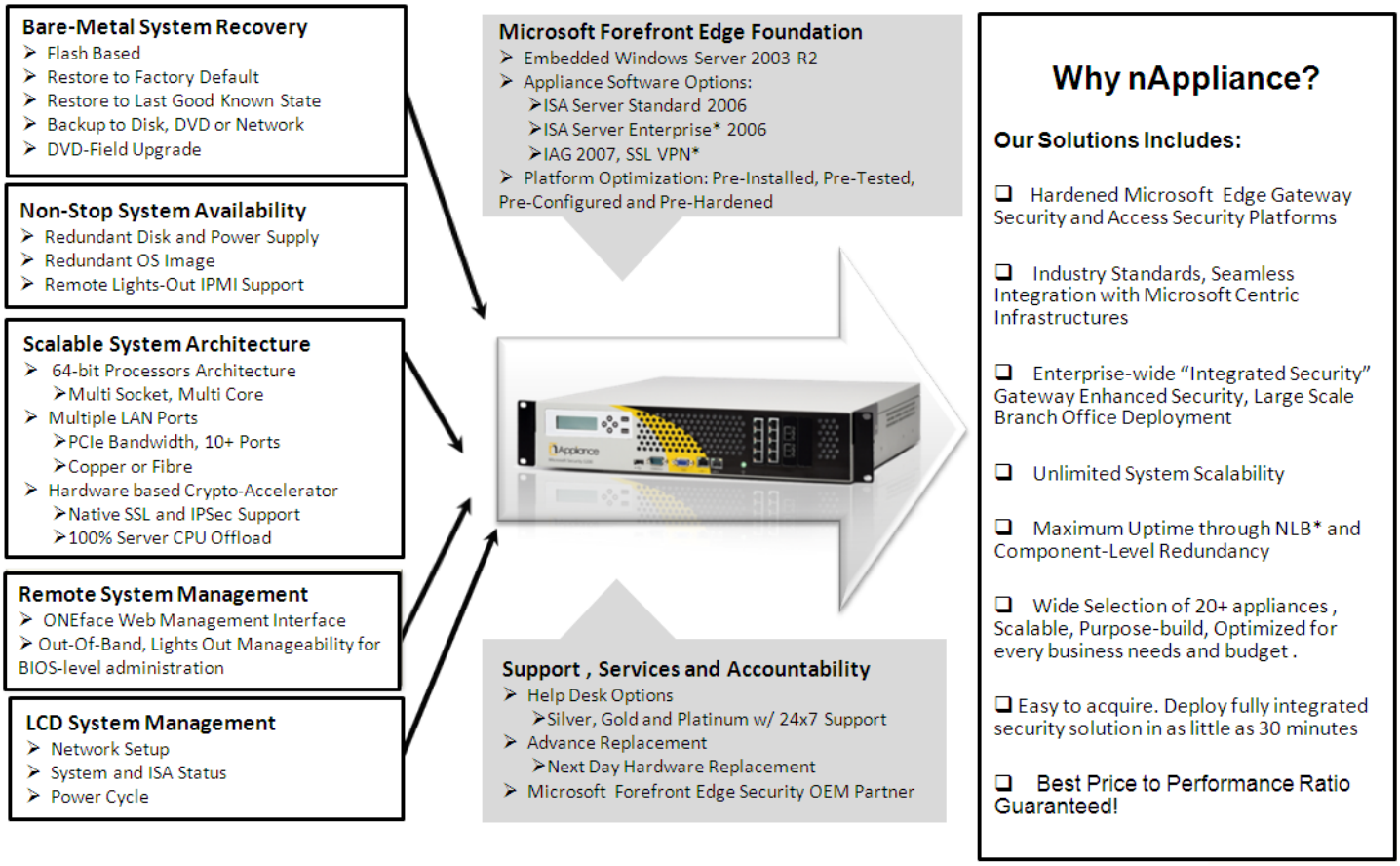
- Special Purpose configuration – highly reduced flexible configuration options than a general purpose operating systems
- Requires no backup or routine maintenance
- Configurations exported and imported as simple text/XML file, providing simple migration and management

Microsoft Edge Security technologies can be purchased both as software products installed and managed similar to other IT applications, and on hardened special purpose appliances. These security appliances running Microsoft Forefront Edge Security systems provide the security and management benefits of special purpose hardware products, and provide the familiar management interfaces of other Microsoft technologies.

Appliance products running Microsoft Embedded Edge Security technologies have the following advantages:

Security Hardened Configuration for "Out-Of-the-Box" Experience

Each security appliance has various software and hardware components installed and integrated. This configuration is then carefully tuned and hardened to maximize the security posture of each system. This hardening is exhaustive, costly and difficult to provide in general IT hardware and software implementations, but imperitive on edge security devices.



Special Purpose Hardware Configuratin Options

Security appliances often have special purpose hardware specific to security.

- Multi-Core 64-bit Arthitecture: Highly efficient processor architecture, lower power consumption, increased memory bandwidth for deep packet inspection and system scalability.
- *SSL acceleration and TCP/IP Offload* – SSL encryption is CPU intensive. SSL acceleration hardware provides all encryption operations on special hardware greatly enhancing performance.
- *HSM certificate management* – HSM hardware provides a certificate repository and generation facility. Certificates can be compromized if a system is compromized, unless the certificates are generated and stored in these special hardware components.

Advance System Recovery, FFRS

Flash based "Field Recovery and Restore System" combined with advanced LCD functionality offers appliance recovery to factory defaults and enables multiple system image copies backup to local disk or network, and instant restore to last good known state.

Simplified licensing
Microsoft embedded licensing can greatly simplify purchases. Often, CAL licenses are not requried with some of the appliance systems.

Third-party add-on applications
Appliance systems have numerous add-on software components, either pre-integrated or available for automated integrations. These add-on components include:

- ***High availability*** – High availability thru components level redundancy of disks, power supply and system images as well as load balancing and fail-over systems.
- ***Content Mangement*** – Content management systems from third party vendors including Websense and GFI provide web content management and filtering.
- ***Traffic Shaping*** – Integrated traffic shaping and QOS technologies allow administrators to manage traffic priorities and guarantee bandwidth availability for critical applications.
- ***Virus Management*** – Built-in virus scanning technologies are commonly integrated with the appliance systems.

Built-in Integrated Sytem Management
- ***Headless deployment*** – Appliance systems include LCD hardware and software which allows simple installations without connecting keyboard, mouse and video monitors. This greatly simplifies installs, including remote installs without local IT support.
- ***Remote access and mangement*** – Appliance systems include a web console, which allows simplified management from a web browser.
- ***Lights-out Management*** – Remote access to the hardware console is available via special purpose hardware, which allows adminsitrators to access the video monitor, keyboard and mouse, and power cycle systems from remote locations via an IP connection and web browser.

SNMP Operations Management
SNMP management of systems must include monitoring and management of the network components, power sensors, fan sensors, heat sensors, RAID controller components, operating system components, firewall logs and access logs and monitors. The appliance products will include both hardware and software SNMP management as a complete product.

Software and Hardware Update Services
Systems include numerous software and hardware components provided by multiple vendors. The appliance provides an Update Service which provides software and firmware updates for hardware systems, drivers, third-party software products and major operating system components.

Integrated security audits
Once an appliance system is built and packaged, it must go through complete security audits as a complete system. Various software add-ons, hardware components and system configurations will

change a system security profile. Each variation of configuration can be tested and audited on an appliance system for security and reliability.

Integrated Worldwide Support Plan

Security systems are constructed of a number of hardware and software components. Appliance vendors will provide a single point of contact and take responsibilities for the support and reliability for the appliance system as a whole. Flaws in a single component or vendors technology is managed by the appliance vendor.

Microsoft Technology Foundation for Easy Integration

Securing enterprise wide applications such as SharePoint, Exchange, CRM any almost all of the industry standard applicatino environments require intricate knowledge of underlying technologies utilized by each application. Microsoft Forefront Edge Security systems tightly integrate with applications based on the Microsoft platform since each is based on the same infrasturcture and underpinning technologies.

nAppliance appliance systems with embedded Microsoft systems provides state of the art enterprise wide systems and applicatino integration, best price-to-performance-ratios in the industry, deployment assitance for Microsoft's ISA and IAG technologies, global technical support, efficient appliance life cycle management and upgrades, and above all future proofing with Microsoft Forefront "Stirling" security architecture.

Summary

Best Practices in Forefront Edge Security based on Microsoft Security Technologies is achieved via nAppliance's Net-Gateway appliance products which provides the advantages of both high security and reliability of special purpose hardware systems and the high functionality and ease of use of the Microsoft Forefront Edge Security suites of software.