ALTOR NETWORKS SECURES VIRTUALIZED DATA CENTERS WITH INDUSTRY'S FIRST VIRTUAL NETWORK FIREWALL AND SECURITY ANALYZER

Breakthrough Security Solutions Making Virtual Networks More Secure Than Physical Network Infrastructures

Redwood City, Calif. – March 17, 2008 – Altor Networks, pioneering a new class of virtual network security solutions, today announced the launch of the industry's first virtual switch traffic analyzer and Virtual Network Firewall™. Each system supports multi-vendor virtual platforms and is purpose-built to make virtualized data centers more secure than their physical counterparts.

Altor's Virtual Network Security Analyzer™ (VNSA) and Virtual Network Firewall™ (VNF) provide unprecedented visibility into virtual switch traffic and control over virtual machines (VMs) being deployed by enterprises, government agencies and organizations in regulated industries. Altor's VNSA and VNF solutions enable network administrators and security professionals to apply security best practices for virtual networks and help companies meet increasingly stringent HIPAA, PCI and SOX regulatory compliance requirements—at a fraction of the cost of legacy security products.

"One of the key drivers for virtualizing our data center is operational agility," said Nicholas Portolese, senior manager, data center operations, with Nielsen-Mobile, the world's largest provider of syndicated consumer research to the telecom and mobile media markets. "Altor Networks' Virtual Network Security Analyzer provides us, for the first time, with crucial insight into our virtual switch traffic with real-time and historical monitoring and analysis capabilities. This enables us to weed out, analyze and report on network bottlenecks caused by a number of sources including unwanted protocols, multicast and broadcast service announcements."

"Most people don't realize security virtualization has lagged far behind virtualization of storage, networking, and servers," said Andreas M. Antonopoulos, senior vice president and founding partner at Nemertes Research. "The lack of suitable security is actually thwarting more widespread adoption of virtualization in some cases. Ironically, traditional static security solutions are subverting some of the operational return-on-investment offered by virtualization such as live migration."

This "security gap" can be traced to the shortcomings of traditional security solutions that include legacy firewalls, intrusion detection/prevention systems, operating system firewalls and VLANs. Aging firewalls and IDS/IPSs that were designed to defend static, perimeter-based physical networks have no visibility into VM traffic and control over virtual networks—nor do they integrate easily with virtual network management systems. VLANs lack virtual switch traffic inspection capabilities, are complex to manage, and restrict usage of VM migration tools like VMotion. And OS firewalls suffer from lack of central management, inconsistency across differing operating systems and poor support for legacy OSes.

"Virtualization, as with any emerging technology, will be the target of new security threats," according to Neil MacDonald, security & privacy vice president and Gartner Fellow, in a March 6, 2007, Gartner Research Note titled, "Security Considerations and Best Practices for Securing Virtual Machines." Added MacDonald: "Many organizations mistakenly assume that their approach for securing VMs will be the same as securing any operating system (OS) and thus plan to apply their existing configuration guidelines and standards. While this is a start, simply applying the technologies and best practices for securing physical servers won't provide sufficient protection for VMs. Several areas are often overlooked completely … Because of the rush to adopt virtualization for server consolidation efforts, many of the[se] issues are overlooked, [and] best practices aren't applied, or in some cases, the tools and technologies for addressing some of the security issues with virtualization are immature or nonexistent."

Altor's Virtual Network Security Analyzer

Given the increasing adoption rates of virtualization, data center administrators must be capable of discovering inter-VM traffic for auditing, security and regulatory compliance. Altor's VNSA delivers on these requirements by providing real-time visibility and historical views of virtual switch traffic though a centrally managed, comprehensive dashboard that integrates with existing virtualization management systems to import network, host and event information. The VNSA can also analyze virtual network traffic to track and organize VMs by network usage and create user-defined groups.

Unlike network security and monitoring solutions that are completely "blind" to inter-VM communications, Altor's VNSA can alert data center administrators to security vulnerabilities and operational problems through the discovery of:

- Port scans, tunneling, insecure and unwanted protocols
- Configuration anomalies due to external DNS and NTP access and DHCP auto-configuration errors
- Multicast and broadcast service announcements that can erode network performance
- Optimize VMotion/DRS by grouping VMs based on network usage
- User defined and automated groups to monitor access to business-critical resources
- Report generation for regulatory compliance

Altor's Virtual Network Firewall

Specifically built to secure inter-VM communications in highly dynamic virtual network environments, Altor's first-of-its-kind Virtual Network Firewall uniquely enforces granular security policies that remain "attached" to individual VMs, even as they move about the data center. Centrally managed, the VNF supports and enforces roles-based security policies per-VM.

Altor's VNF is built from the ground up for multi-vendor platform support which will include virtualization servers from VMware, Citrix, Microsoft, Oracle, Sun and others.

"As more servers are virtualized on multi-core systems capable of hosting dozens of VMs, CIOs and CSOs are beginning to recognize that securing the new access layer—the virtual switch— is a strategic imperative," said Amir Ben-Efraim, CEO and founder of Altor Networks. "In view of the soaring adoption rates of virtualization in production data centers, we have a unique and considerable market opportunity to cost-effectively improve the security posture of organizations across a broad spectrum of industries."

Pricing and Availability

Enterprise licenses for the Virtual Network Security Analyzer, (VNSA) start at $500 US per physical server, supporting an unlimited number of virtual machines. A single Altor Center management system supporting unlimited VNSA agents is available for $1,500 US. Annual maintenance and support licenses are also available. Release 1.0 of the Virtual Network Security Analyzer is generally available now. Free demo versions of the Altor agent and Altor Center can be downloaded at www.altornetworks.com.

About Altor Networks

Altor Networks is pioneering a new class of virtual network security solutions, purpose built to secure virtualized data centers. The company's initial product lines include the industry's first-ever virtual network firewall and security analysis system. Altor's Virtual Network Security Analyzer™ [VNSA] proactively monitors and analyzes the security readiness of virtualization deployments to help enterprises meet stringent regulatory compliance requirements. Data center administrators can now pinpoint a broad range of virtual network security compromises and easily create roles-based security policies. For the first time, security policies can be continuously enforced on individual virtual machines, even as they move throughout the virtualized data center. Founded by former Check Point Software security experts, Altor Networks is funded by Accel Partners and Foundation Capital and is headquartered in Redwood City, California. For more information, visit www.altornetworks.com.

# # #