

## Leveraging STRM Investment to Manage Virtualized Assets

Rapidly growing “virtual networks” of server and desktop virtual machines (VMs), connected to each other through virtual switches, are fundamentally changing data centers and enterprise networks. Yet despite virtualization’s increasing positive impact on business results and continuity, the lack of controls and visibility could deter from the customers’ anticipated benefits. Inter-VM traffic is typically not monitored, inspected, filtered, or strictly segregated into higher and lower trust security domains. Communication between VMs is a dangerous blind spot. Inter-VM traffic doesn’t touch the physical network, so it is not protected by the physical network security infrastructure. In particular, VM traffic is not incorporated into physical network event correlation or threat response systems.

### Challenge

“Virtual Networks” inside virtualized servers can hide unmitigated risks because inter-VM traffic is invisible to network monitoring and event management systems. Until now, enterprises haven’t had the integrated network security and threat response solution needed to remediate their virtual network exposure cost-effectively.

### Solution

The integration of Juniper Networks’ STRM—Security Threat Response Managers with the purpose-built Altor Networks VF™ virtual firewall overcomes the unique security challenge of visibility gaps in the virtual environment by extending best-in-class physical network security.

### Benefits

- Extends physical network threat management to virtualized environment
- Increases event analysis and incident response value of STRM
- Fast and simple configuration of the integrated solution
- Easy for administrators to learn and use

### The Challenge

An unmonitored and uncontrolled virtual network inside a virtualized server with no enforceable security policies presents daunting challenges for network security managers. Unbridled and possibly undetected malware outbreaks can compromise all VMs on a host. Conficker is one recent example. Attacks that span physical and virtual networks can take longer to identify and shut down. Privilege escalation can occur when virtualized workloads with different trust levels, such as production and QA VMs, reside on the same physical server. When VMs move from host to host via live migration technologies like VMware VMotion and DRS, the potential for malware infections and trust level breaches is amplified.

Management of logs, threats, and compliance shouldn’t stop at the boundary between the physical network and the virtualized environment. Without data about VM traffic, effective event correlation and response will be increasingly hard to achieve. As more and more production systems move from the physical to the virtual world, traditional security information management systems are losing granular visibility into the network activity the newly virtualized workloads generate. Redirecting all inter-VM traffic out to physical network security devices in many cases can be an inefficient “solution” that reduces the performance and optimization gains of virtualization. Enterprises need a cost-effective solution that extends best-in-class threat response management and high-performance, proven security to the virtualized layer.

### The Juniper Networks and Altor Networks Solution—STRM for Virtualized Data Centers

Juniper Networks and Altor Networks have partnered to create a solution that leverages physical network security to monitor and protect the virtual server environment. The solution integrates Juniper Networks’ STRM Series Security Threat Response Managers

with the pioneering Altor Networks VF™ virtual firewall. By extending STRM data collection and analysis capabilities into virtual servers, the joint solution increases the return on investment for our joint customers.

The Altor firewall uses patent-pending technology that was designed specifically to meet the unique security challenges of virtualized data centers. It gives administrators fine grained visibility into virtual network activity, eliminating a dangerous “blind spot”. It also lets administrators control virtual network traffic by enforcing a rule-based firewall policy for each VM, even during vMotion events. And because its architecture can support the primary virtualization platforms (including VMware and Hyper-V), Altor VF ensures that enterprises retain the ability to choose the virtualization technology that best fits their needs, now and in the future.

*continued...*

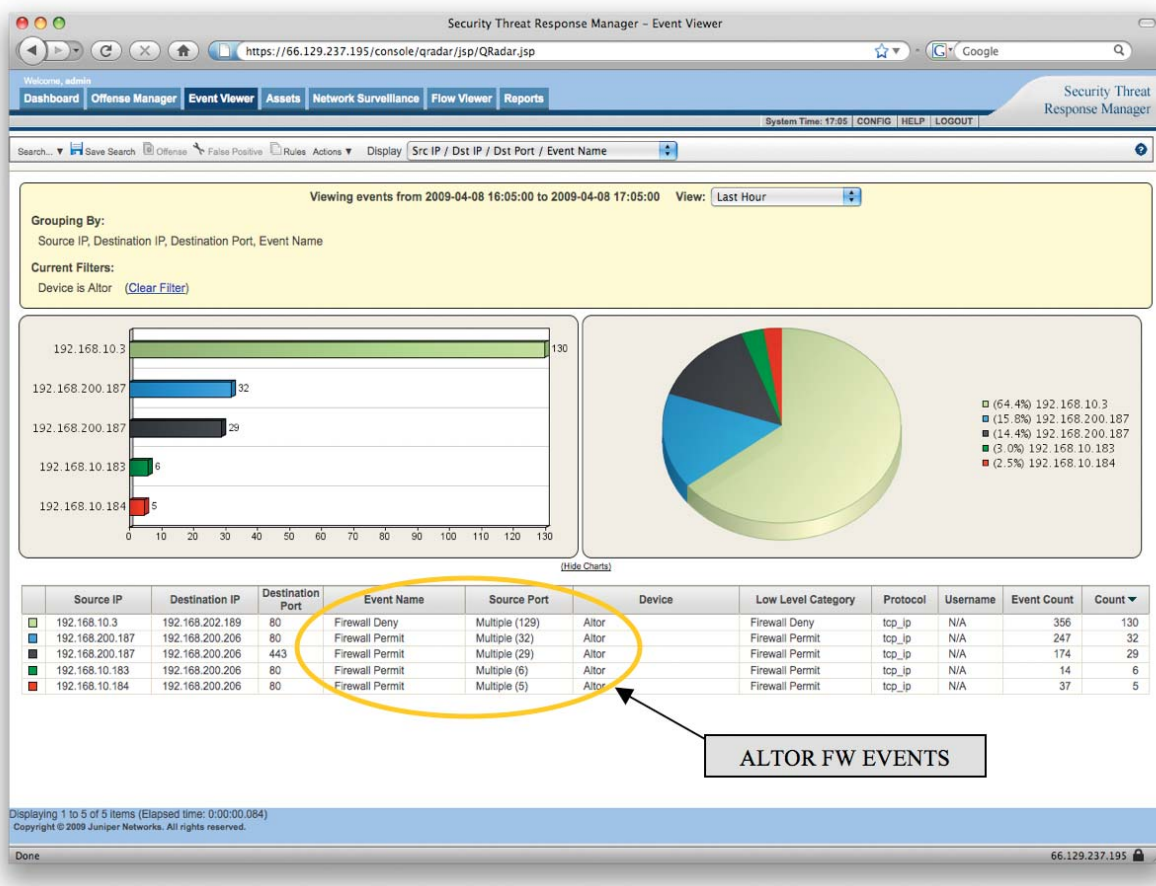


STRM combines, analyzes, and manages an unparalleled range of surveillance data—network behavior, security events, vulnerability profiles, and threat information. The Altor virtual appliance increases the scope of STRM event collection by sending syslog-formatted virtual firewall logs to STRM in real time. Altor also supplies STRM with continuous VM network flow data – even during VM live migrations around the data center. Configuring the Juniper and Altor components to interoperate is literally accomplished with a few keystrokes and mouse clicks.

The STRM management UI blends virtual and physical network events and traffic records, using Altor VF simply as a critical sensor device. STRM administrators therefore need little or no training to use the joint solution effectively. It gives them a more complete view of the enterprise network, with new visibility into anomalous behavior inside the virtual server environment and attacks targeted at VMs. By deploying this unique solution, enterprises gain the ability to quickly identify and stop threats, uncover compliance violations, and expose potential privilege escalation across the combined virtual and physical networks, with minimal performance overhead.

Features and Benefits

- Combining logs and flow data from physical networks and virtualized environment mitigates hidden risks
- Leveraging physical network security to protect VMs increases the ROI of STRM
- Certified STRM/Altor VF integration makes configuring the solution quick and easy
- Displaying virtual and physical network data in a common UI makes the solution easy to learn and use



Firewall events sent by Altor VF from the virtualized environment are fully integrated into the STRM

Solution Components

- Juniper Networks STRM Series Security Threat Response Managers
- Altor VF virtual network firewall for VMware ESX



## Summary—An Innovative Approach to Threat Management for Virtual Networks

Rapidly growing networks of VMs lack safeguards considered critical for physical network security. Virtualized assets need the protection provided by traffic monitoring and filtering, event consolidation and analysis, and enterprise-wide threat management. Only a solution that uses purpose-built virtual network technology to leverage best-in-class physical network defenses can deliver this protection cost effectively.

By extending physical network threat management to virtual environments, the Juniper Networks and Altor Networks solution detects and contains malware outbreaks, mitigates VM privilege escalation risk, and supports regulatory compliance in virtual networks. Tight integration of STRM and Altor VF makes the solution easy to deploy, learn, and administer. Together, Juniper and Altor are delivering unmatched protection for virtualized resources and the key business functions they support.

### Next Steps

To learn more about how the STRM for virtual networks solution can provide cost-effective, market-leading security for your virtualized data center, contact your Juniper Networks or Altor Networks representative.

---

## 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 firewall and security analysis system. 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 security and networking experts from Check Point Software, Cisco, NetApp and Oracle, Altor Networks is funded by Accel Partners and Foundation Capital and is headquartered in Redwood City, California. For more information, visit [www.altornetworks.com](http://www.altornetworks.com)

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net)