

### Key Benefits

- **Visibility:** full view to all applications flowing between VMs and how they are used. Complete VM and VM group inventory, including virtual network settings. Deep knowledge of VM state, including installed applications and services through VM Introspection.
- **Compliance:** enforcement of corporate and regulatory policies for must-have installed applications and services. Assurance of segregation of duties by use of VM Introspection to limit VMs to desired groups and VLAN assignments.
- **Control:** access control over all traffic via policies that define which ports, protocols, destination VMs, etc., should be blocked. Deep inspection of allowed traffic for malware suppression and intrusion detection.



Visibility & Compliance Dashboards

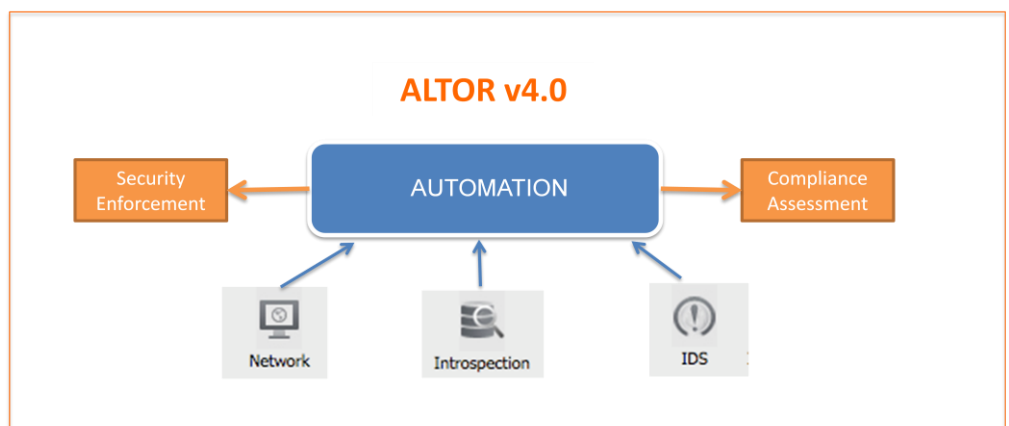
### Visibility, Compliance, Control

#### The Challenge

Server consolidation and the need for efficient data center infrastructure management have compelled 90 percent of the world’s organizations to virtualize at least some portion of their servers. Astoundingly though, virtualized workloads are still only a small fraction of the overall data center. This is largely due to concerns about security and compliance within the virtualized environment. CIOs, CISOs, and directors of security as well as IT operations want to be certain that the measures for auditing and protecting virtualized servers are equivalent to what is in place for the physical network.

#### The Solution

Altor is a leading innovator and provider of security for virtual data centers and clouds. With version 4.0 of its system, Altor rounds out a virtualization security package that includes a high-performance hypervisor-based stateful firewall, on-board intrusion detection, complete virtual network visibility and monitoring, as well as reporting. Altor v4.0 brings forward powerful new features that automate security and compliance enforcement within virtual networks and clouds. By leveraging Virtual Machine Introspection (VMI) data and intelligence, and coupling it with Altor system knowledge of the security and virtual network environment, Altor v4.0 creates an extensive database of control points by which security policies and compliance rules can be defined. Altor makes this rich data available in intuitive UIs that let administrators build the entire range of policies from corporate rules on global protocol handling (e.g., block Kazaa) to discrete regulatory compliance policies for how virtual machines (VMs) should be configured (e.g., must-have antivirus installed). Compliance assessment and security enforcement happen automatically and in lockstep with changes in the virtual environment. New VMs, for instance, will be scanned and quarantined if out of compliance with policies. The same applies to VMs whose “state” changes so that the security posture is weakened. Altor’s VMware VMsafe-certified security operates from deep within the virtualization fabric as part of the hypervisor. Consequently, the software delivers unprecedented levels of security, far beyond what is possible with traditional physical network security products.



“Altor lets us build a bubble around the VMs of each one of the units or colleges. This is a whole new and more efficient way of securing our virtualized environment. We don’t have to design around the limitations of our physical firewalls.”

—Joshua B. Slade, Information Technology Analyst, Syracuse University, Core Infrastructure Services

## Product Details

### VM Introspection

Virtual Machine Introspection (VMI) is a groundbreaking approach, analogous to an “X-ray” of VMs and the virtual environment from the hypervisor. VMI enables information gathering about VMs, the security of the virtual network, and virtual environment settings without the use of agents. The ability of malware to disable or hide from security agents is a classic unresolved security problem that has plagued the security industry for decades. VMI offers an innovative new approach to leverage the hypervisor for an uncompromised “X-ray” inspection of VMs, where malware has nowhere to hide! Altor incorporates VMI as part of its security policy definition and enforcement mechanism. By amassing information about the kinds of applications and services running on VMs, Altor sustains deep knowledge about the internal security state of each VM. This information is then made available through Altor’s point-and-click dynamic policy editor so that rules can be easily built to enforce a desired VM security posture. For example, a security rule could require the presence of anti-virus software to be present inside a VM or alternatively discover unapproved applications, forcing automated quarantine and alerts for non-compliant VMs. Altor’s unique vantage point in the hypervisor delivers unprecedented visibility and control over the virtual environment to achieve compliance with corporate standards.

### Compliance assessment

Altor lets VM administrators, security managers and compliance auditors define and report on the specific conditions (corporate and regulatory) that constitute compliant operation in their environment. Altor’s user interface allows for the building of custom “whitelists” (desired configurations) and “blacklists” (unwanted conditions). Altor continuously monitors all VMs, including newly created ones, to report on the overall compliance posture of the virtual environment. Virtual data center and cloud administrators can see their aggregate compliance posture at a glance and drill down on each VM to identify the exact condition that has triggered an alert of non-compliance (e.g., VM in wrong VLAN, or trust-zone, has been quarantined).

### Secure VMotion and live migration

Firewall protection is continuous as VMs move from host to host using VMotion. Unlike traditional firewalls, Altor keeps the “live” in live migration by maintaining open connections and security throughout the event.

### Smart policy for new VMs

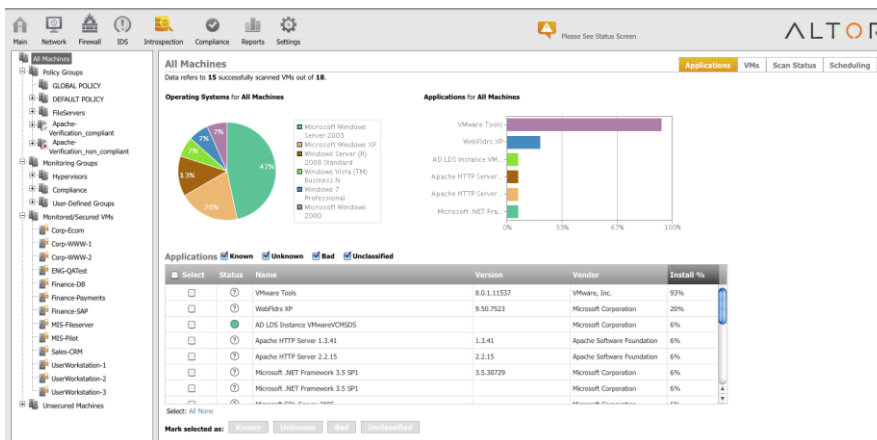
When a new VM is created, Altor assigns it an administrator-defined security policy. Allowing only admin and DNS protocols, for example, mitigates the risks of misconfigured or “rogue” VMs with vulnerable or infected workloads.

### Logging, reporting, and alerts

Syslog output gives security-event management systems insight into virtual network activity. Administrators can print reports of historical VM traffic data and configure SNMP traps to alert them to selected events.

### VMware hypervisor protection

Altor provides a hypervisor-based stateful firewall that inspects all packets to and from VMs, blocking all unapproved connections and subjecting allowed packets to deeper inspection (e.g., port-80 for Web applications). Administrators can enforce stateful firewall policies for individual VMs, logical groups of VMs, or all VMs.



### Automated VM security

Altor automates the application and enforcement of security rules. This is accomplished in two ways. First, Altor allows for the creation of highly detailed security policies that “dynamically” combine desired conditions from Altor’s own rich database of virtual infrastructure (VI) and VM information. The dynamic policy groups can then be associated with a single VM or a group of VMs. When additional VMs are created, they can be automatically associated with known VM groups and policies by matching pre-defined criteria. Administration overhead is reduced by allowing a “build-once” “apply continuously” model to security policy definition and enforcement. For example, a new VM with the name “Finance Server-New York,” running IIS Web Server and McAfee A/V, and connected to virtual-switch port-group 22, will automatically receive the “Finance Web-Servers” security policy, eliminating costly human configuration errors common to the dynamic virtual environment.

### System Requirements

#### Altor Firewall (VMSafe Mode)

Operating System Virtual Appliance  
Memory 512MB  
Disk Space 1GB  
Virtual Infrastructure VMware vSphere 4  
VMware ESX or ESXi 4.0, with vCenter 4

#### Altor Firewall (Bridge Mode)

Operating System Virtual Appliance  
Memory 512MB  
Disk Space 1GB  
Virtual Infrastructure VMware vSphere 4  
VMware ESX 3.0+ or ESXi 3.5+, with VirtualCenter 2.0+

#### Altor Center

Operating System Virtual Appliance  
Memory 1GB  
Disk Space 10GB  
Virtual Infrastructure Infrastructure 3  
VMware ESX Server 3.x.x  
VirtualCenter 2.x.x

For more information  
Call 1-888-734-6555  
Visit [www.althornetworks.com](http://www.althornetworks.com)  
Email [info@althornetworks.com](mailto:info@althornetworks.com)

Corporate Headquarters  
900 Island Drive, Suite 204  
Redwood Shores, CA 94065

**ALTOR**  
Virtualize Securely™