

LARGE FEDERAL CREDIT UNION

CLIENT

Federal Credit Union

LOCATION

Denver, Colorado

INDUSTRY

Financial Services

THE CHALLENGE

In virtualizing, maintain a three-pronged approach to defenses: secure the perimeter, each VM and each key application.

THE SOLUTION

For security per VM and monitoring of key applications:
ALTOR Virtual Firewall (VF) & IDS

BENEFITS

- Visibility to all traffic between VMs
- Access control by application, protocol, VM, VM Group
- Malware detection and alerting

"We considered VMware's vShield but Altor really stood out especially with security policy granularity to really lock down each VM. The rules were easy to implement so there wasn't much of a mind shift required to transition from physical to virtual network security."
— IT Infrastructure Manager

Customer Success Story

"We wanted a full fledged firewall between our VMs so that we could be as secure as we can. Altor's heritage in building leading security products gave us the confidence to try it; the product's security features compelled us to buy."

THE CUSTOMER

Credit unions are more than a financial services institution. Because they operate regionally and are member owned, they are truly part of the community they serve with programs that educate and reinvest toward the betterment of the local economy. And today's credit unions offer nearly the entire range of services that people often associate with larger financial institutions including lending for home and automobile purchases, retirement planning and money management. This is in addition to online banking facilities for bill paying and the management of checking, savings and investment accounts. So when it comes to IT infrastructure, a federally insured credit union like the one showcased here has the same responsibilities and challenges that larger banks do, to innovate and secure its digital assets.

THE CHALLENGE

For this particular credit union, innovation and collaboration are key operating tenets and the teams really demonstrated that philosophy when it came to adopting virtualization. They knew there were cost benefits to virtualizing but understood the risks of deploying without a well-laid plan for security. The infrastructure group, together with development networking and security drafted out those must haves that would ensure all Virtual Machines (VM) would have the best protection possible. Key to meeting their National Credit Union Administration (NCUA) security certification and their own rigorous auditing, was a virtualization security solution that delivered the following:

Evaluation Parameters

- Enterprise grade firewall
- Hypervisor-based implementation
- Granular security policy
- Support for vMotion and live migration
- Integration with vCenter
- Familiar management interface
- 10Gbps firewall throughput
- Integrated intrusion detection (IDS)

THE SOLUTION

After hands on evaluation, this federally insured credit union selected the Altor virtual firewall VF with integrated intrusion detection (IDS) for their virtual network security needs.

Security Per Virtual Machine

When securing people's money no amount of security is excessive. At least this is the operating philosophy of this organization. They drafted a requirement for controlling all access into and out of each virtual machine. This meant having the ability to enforce the policy as they had defined it – to allow or block access by application and protocol to every virtualized resource especially those hosting application critical to online banking. This strict requirement meant that approaches applying security by zones or groups of VMs were not granular enough or for that matter secure enough to meet the need.

Hypervisor-Based Solution

All network security practitioners know that the challenge of the work is in applying controls that are sufficient to protect but don't impede the flow of business. For credit unions, that business is conducted with many people who opt for them over large banks. Therefore resource accessibility and superior customer service are operational imperatives. For these reasons, the credit union's infrastructure team made high-performance a top -level requirement for any approach to secure the virtualized ecosystem. Their research led them to Altor and the company's hypervisor-based firewall. By operating within the virtual machine monitor or hypervisor, Altor's firewall is able to receive and process packets extremely efficiently achieving throughput of nearly 10Gbps. The end result is high security applied at high speeds with no discernible latency.

Layered Defense

Financial institutions understand all too well the importance of ensuring fault tolerance in their security practice. High availability and multiple layers of defense are thought of as absolute requirements so that there is no single point of failure in the protection fabric. The Altor solution delivers on both fronts with high availability for both the enforcement module that sits within the hypervisor and applies policy, as well as the management console that runs as a VM in the virtual network and from which all virtual network security is administered. Further, Altor layers on protections for that traffic which is allowed by inspecting it to ensure it does not match known attack patterns and signatures. The capability, known as intrusion detection (IDS) servers to alert administrators of potentially anomalous activity and enables rapid response to possible breaches.

Compliance

All credit unions must maintain network security to the requirements put forth by the NCUA. Certification is contingent on an annual audit, although this particular organization imposes on itself two supplemental audits to ensure year-round compliance. The credit union's infrastructure and security teams understood that virtualization adoption should not put their NCUA certification at risk of non-compliance, so they prepared with purpose-built protections for their virtualized workloads. The selection of virtual security software from Altor gave them the visibility and monitoring capabilities they have in their physical networks, but couldn't achieve in their virtualized one. And with the ability to report on both the traffic, access and enforcement events, the team can now furnish its auditors with proof that the virtualized network's access controls and segregation of duties are equivalent to those being enforced within the physical network.

WORLDWIDE HEADQUARTERS

350 Bridge Parkway Suite 6
Redwood Shores, CA 94065
Phone: 650-492-5419
sales@altornetworks.com