Integra Networks Leads Virtualization Initiatives for its Customers with Trend Micro

**Overview**

For 30 years, Integra Networks has designed, built, and supported enterprise-level technology solutions in Ottawa, Ontario. The company began focusing on data center virtualization in 2002 when virtualization was still in its infancy. During this time, Integra Networks introduced many Canadian federal and local government agencies to virtualization. They have been named a top Canadian Federal Government Partner, and recognized as the VMware vendor of record for the municipal government of Ottawa. Today, individual federal government departments and agencies account for a large part of the company’s business. Integra Networks also supports virtualization efforts for commercial enterprises, higher education, and healthcare.

Over the years, Integra Networks has received numerous awards from VMware, including VMware's Top Partner in North America for Thought Leadership. Its business and technical executives belong to VMware’s North America Partner Advisory Council and Partner Technical Advisory Board. The company employs 25 full-time employees and brings in additional expertise for large virtualization implementations. While the company has a much smaller IT environment than its enterprise customers, its infrastructure is more complex than that of most organizations its size. Its IT environment includes over 70 servers and has been fully virtualized for five years. Integra recommends Trend Micro Deep Security for virtualized environments and protects their own data center with the solution.

**Challenges**

Data center virtualization has given Canadian government agencies and other Ottawa enterprises a way to control costs through server consolidation as well as creating more flexible data centers. “As government agencies implement more private cloud technologies based on VMware, developers and test labs spin up virtual machines constantly and commission and decommission them at will. An agentless approach allows security service provisioning to keep pace with server provisioning,” said Nagwa Koressa, founder, president, and CEO of Integra Networks.

Similar to trends with the United States government, security is a top priority for the Canadian government as it revamps systems in an effort to better protect Canada’s intellectual property and the programs it runs to safeguard citizens. Traditional agent-based security can negatively impact performance and resources in virtual environments, but these pitfalls have not always been widely understood by clients. As a front-runner in virtualization technology, Integra Networks needed to help clients get the most out of their investments in virtualization. This required education on the problems associated with using traditionally architected security in a virtualized data center.

The first issue Integra needed to overcome was instant-on gaps. The activation and deactivation of virtual machines in rapid cycles requires consistent and immediate provisioning of security and consistent application of security updates. This is because a virtual machine can be activated much faster than traditional security can configure an agent and conduct security updates. In fact, it’s possible to introduce massive security vulnerabilities simply by powering on a dormant virtual machine.

Another issue was resource contention. When traditional antivirus solutions simultaneously initiate scans or scheduled security updates on all virtual machines on a single physical host, it creates an extreme load that greatly reduces performance. Applying traditional security architecture to virtual systems also requires a significant footprint that can detract from server consolidation efforts.

Finally, IT compliance presents its own set of issues. For example, the dynamic nature of virtual machines can jeopardize compliance by making it difficult to maintain an auditable record of the security state of a virtual machine at any given point in time.

“Because of the creative nature of today’s cyber attacks, we need to look at new and different ways to protect our customers’ data,” said Rami Courtemanche, director of operations for Integra Networks. “As attackers find new ways to penetrate the perimeter, it becomes vital to minimize how far an attack can spread following perimeter penetration.”
Virtualization solutions like VMware NSX enable dynamic data centers. Agentless security with Deep Security enables security to keep pace with virtualization, enabling more agile data center operations and faster application deployment.

Rami Courtemanche, Director of Operations, Integra Networks

“By developing Deep Security in the early stages of virtualization, Trend Micro allowed us to provide more mature solutions, offer security expertise to our clients, and position ourselves as the leading provider of virtualization solutions in Ottawa.”

Nagwa Koressa, Founder, President and CEO, Integra Networks

Why Trend Micro

To improve security in virtualized environments, Integra Networks began working with VMware partner Trend Micro 10 years ago. If their clients were going to keep up with the pace of virtualization, they would need a faster, agentless method of updating security on virtual machines. “Trend Micro is a leader in agentless security solutions that integrate tightly with VMware technology,” said Courtemanche.

An analysis of other security solutions in the evolving marketplace convinced Integra Networks that Trend Micro Deep Security continues to be the right choice for their customers. “Competing products have a bigger footprint in the IT environment and are not as easy to deploy,” said Courtemanche. “You often have agents to install, which drives up operational costs. Trend Micro offers more efficient VMware integration than the competition.”

Trend Micro has helped Integra Networks in its efforts to expand client services and educate clients on virtualization security. Together, the partners developed their Security Assessment for Virtualized Infrastructure. They have also jointly delivered many courses on virtualization security.

Solution

Deep Security provides comprehensive server security for Integra Networks’ customers. Its tightly integrated modules can easily expand to ensure server, application, and data security across physical, virtual, and cloud servers as well as virtual desktops. “Our clients like Deep Security’s agentless anti-malware modules because they provide a secondary non-network path for virtual machines that simplifies deployment, maintenance, and extensibility of the security platform in all Windows environments,” said Courtemanche.

Integra Networks uses Deep Security to improve performance and increase server consolidation ratios for clients. Rather than deploying hundreds of megabytes of security software to every guest virtual machine or physical host, organizations can deploy a security virtual appliance and leverage a VMware driver with a small footprint in each virtual machine to perform the necessary offload. Deep Security also prevents bottlenecks associated with simultaneous scans by serializing operations across virtual machines.

Deep Security offers the visibility and control needed to comply with industry regulations and internal data protection policies. And it provides active monitoring of file system activity and detailed logging of relevant security events.

“Because attackers are able to penetrate perimeters in new ways, we’ve had to find new ways to segment the environment and minimize how far an attack can go once the perimeter is breached,” said Courtemanche, who sees value in VMware NSX for addressing this vulnerability. VMware NSX, the new network virtualization platform, works with Deep Security to prevent lateral movement of data center attacks, further simplify security deployment and provisioning, automate workflow across protection layers, and solve the most critical challenges of perimeter security with micro-segmentation.

Benefits

The integration of agentless security and central management provided by Deep Security with NSX have allowed Integra Networks’ clients to realize the promise of virtualization and increase server density in their environments while reducing the attack surface in the data center. “The agentless capability of Deep Security makes it easier to automate the deployment of virtual machines and ensure they are automatically protected through policy from Day 1,” said Courtemanche.

“We find that Deep Security helps us secure virtual desktops centrally the same way that we secure virtual machines. Whenever we spin up a virtual desktop, it is protected right away and centrally managed,” said Courtemanche.

Support from Trend Micro has been exemplary. “Every time we pick up the phone to call Trend Micro, we have a very knowledgeable engineer on the other end of the line to help us with our problem,” said Courtemanche. Integra Networks can also resolve urgent problems with help from the Deep Security development team in Ottawa. “Even the presales engineer has been known to jump in and give us a hand,” Courtemanche added.

As a Trend Micro Partner, Integra Networks remains in a position to confidently adopt security technology as it emerges. “By developing Deep Security in the early stages of virtualization, Trend Micro allowed us to provide more mature solutions, offer security expertise to our clients, and position ourselves as the leading provider of virtualization solutions in Ottawa,” said Koressa.
What’s Next?

Integra Networks is well known as the company that educates clients on new technology. They see VMware NSX and micro-segmentation being deployed by some of the industry’s most dynamic data centers and have begun holding sessions with VMware and Trend Micro to help clients understand the technology.

While Deep Security is the solution sought by the majority of Integra Networks customers, the company sees opportunities in the marketplace for Trend Micro™ Deep Discovery to prove its value in countering targeted attacks. They believe Deep Discovery could potentially mitigate some of the threats that have recently plagued government agencies in Canada. “Deep Discovery could help the government detect breaches sooner and discover their origin,” said Courtemanche.

For More Information

For more information, please visit www.trendmicro.com/virtualization