EXECUTIVE OVERVIEW

The CISO Series

Elastic Infrastructures Need Elastic Security

Organizations are adopting virtualization and cloud technologies as a foundation for their strategic business growth. Whether they deploy private cloud, public cloud or hybrid architectures, this is where IT investments are going today and in the years ahead. The bulk of new IT spending by 2016 will be for cloud computing platforms and applications, with nearly half of large enterprises having cloud deployments by the end of 2017, according to Gartner, Inc.

In particular, the Infrastructure-as-a-Service (IaaS) market is soaring. The general manager for Microsoft Azure says the service is adding a thousand new customers a day, and Amazon claims its Amazon Web Services (AWS) is expected to bring in up to $10 billion in revenue for the company in 2014.

While the hockey stick growth pattern indicates mass adoption, there are still opportunities for increased growth. Even with the secure infrastructures provided by leaders like AWS and Microsoft, security is often a big unknown, with organizations expressing that they do not have a thorough understanding of what is needed to securely deploy in the cloud. No longer can IT professionals walk into their own data center and this loss of control is an important detail in their overall security strategy.

Many organizations have attempted to use legacy security in their cloud infrastructures, which does not scale and is harder to manage. The challenges and costs they have faced with traditional approaches highlight the need for a different approach to security in the cloud.

Cloud computing has unique characteristics that don't exist in the legacy-style data center: rapid elasticity of resources, dynamic workload management, mixed OS environments, on demand self service, and even measured service with pay per use billing. The advancement of cloud offerings requires security to keep pace in this ever-changing environment, and continuing with legacy solutions is no longer a viable option.

The principles of security don't change just because the data center is no longer on-premise, but the approach security professionals take does need to change. Legacy data center security solutions are traditionally deployed as hardware appliances at the perimeter. Firewalls, IDS/IPS, web filters, network access, and encryption control are typically independent of each other but have started to converge as opposed to standalone deployments.

Standalone hardware-deployed security solutions deployed in a cloud environment where hundreds or thousands of virtual servers can be spun up or down in a matter of minutes is not scalable and compliance reporting visibility is lost.

A NEW PARADIGM FOR CLOUD SECURITY

Cloud computing requires a new approach to security:

- Deploy security as software rather than hardware so it can be deployed where it matters most: at the server or instance.
- Security must be adaptive in order to provide controls specific to an environment's needs at any given point.
- Controls must be context-based according to the workloads they are assigned to protect.
- A comprehensive platform is a more effective approach to security in the cloud, removing the challenges of managing independent silos like firewalls.

securitycurrent

There is opportunity to deploy security within the software instance, which is a different approach, but necessary to evolve. This allows the organization to take advantage of automation and to have security embedded in the workload, where it belongs.

On demand computing in the cloud is no longer one-size-fits-all and the rate of change requires that security be part of the computing benefits, not a byproduct. Cloud providers such as AWS, Microsoft Azure and VMWare vCloud offer a secure foundation and some security controls for organizations to manage, but according to recommendations from cloud service providers, this is not enough and the gap needs to be filled.

Trend Micro at a Glance

The Trend Micro Cloud and Data Center Security Solution brings necessary innovation to support modern data center and cloud security requirements. Trend Micro's advancement is a result of their experience from helping customers shift to virtualization, with additional specific enhancements that can now be applied to cloud computing.

Trend Micro has developed its Deep Security platform with advanced integrations with the leading cloud technology providers, including AWS, Microsoft and VMware, and with orchestration management tools like Puppet, Chef, OpsWorks, Salt and RightScale. This tight integration allows security to be automated as part of the cloud provisioning process, enabling customers to realize the efficiencies of the cloud.

When a server instance spins up, Trend Micro's solution detects this action and automatically applies security policies based on the server environment and attributes. Trend Micro quickly is able to apply security controls, such as firewalling, IDS/IPS, integrity monitoring, and encryption, across multiple operating systems.

Trend Micro's tight integration with leading cloud service providers allows organizations to apply what is needed automatically and dynamically, making the provisioning of security an integral part of the deployment process. When servers are decommissioned, they are removed from the central management interface to provide for a real-time view of the environment, while still capturing what security was in place while the instance was active.

The Trend Micro security solution provides defense-in-depth through numerous controls that are centrally managed through a single pane of glass. The controls include:

- Intrusion detection and prevention, shielding servers from vulnerabilities by virtually patching them until actual patches can be applied
- A host-based firewall that provides a customizable perimeter around each virtual server
- Anti-malware with real-time web reputation filtering
- File and system integrity monitoring to watch for changes to critical files
- Web application scanning to detect vulnerabilities (Trend Micro is one of only two vendors with pre-approved scanning on AWS)
- Log inspection and consolidation across multiple sources for critical security events
- Data encryption for data in motion and data at rest

A single dashboard facilitates continuous monitoring of multiple controls across physical, virtual and cloud environments. Security administrators can focus on what is important through Trend Micro's Deep Security reporting and alerting capabilities. The solution also addresses key compliance requirements for regulations like PCI DSS 3.0 by providing both comprehensive security controls as well as detailed, auditable reports that document prevented exploit attempts, detected attacks, and policy compliance status.

All of these capabilities are delivered with pricing that is similar to models offered by cloud providers, including the option to pay based on usage. Trend Micro's flexible pricing model allows organizations the opportunity to cost-effectively enter the cloud and grow with their deployments.

Trend Micro brings to market a single platform with a broad range of security capabilities that span physical, virtual and cloud environments. Organizations that are making that progression with their IT operations can use one platform to support the security needs all along the way, thus reducing the cost and complexity of securing critical assets.

Trend Micro's Differentiators

- A broad security platform that can support an organization through the range of physical, virtual and cloud environments
- Tight integration with the most popular IaaS providers and orchestration management tools
- Defense in depth with multiple security controls, all managed through a single dashboard
- One of the largest security companies in the world, with extensive experience and thousands of customers protecting millions of servers every day

This Executive Overview is sponsored by Trend Micro. For more information, visit www.trendmicro.com