All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

How secure is your data center and how can you tell?

Data centers are a prime target for compromise because (to misquote Willie Horton) “that's where the data is”. The people running data centers know this, and when you hear terms like “advanced persistent threat”, the data centers are in most cases the ultimate target.

But the data centers have to execute too!

They understand that they need to secure their data centers, but they need to do so without compromising the critical business function and performance that their data centers are designed to enable. The challenge for many lies in trying to secure the data center using solutions designed for the Internet edge. But data centers have unique requirements around provisioning, performance, virtualization, applications, and traffic that Internet-edge security devices are simply not designed to address. Most implement the minimum security possible to limit the impact on the business critical services the data center provides.

Securing data centers require solutions that:

- Provide visibility and control over custom data center applications.
- Handle asymmetric traffic and transactions between devices and data centers.
- Adapt as data centers evolve to accommodate
  - Virtualization
  - Software-defined networking (SDN)
  - Network function virtualization (NFV)
  - Application-Centric Infrastructures (ACIs)
  - Cloud services like burst traffic and usage
  - Whatever shows up tomorrow as a critical business need
- Address the entire life cycle of an attack:
  - Blocking as much malicious traffic as possible
  - Monitoring for threats that bypass gateway security
  - Preventing the spread of an attack through intelligent segmentation
  - Identifying and rooting out embedded or dormant threats
  - Detailed forensic analysis
  - Effective removal and future prevention of malware
  - And more
- Integrate and collaborate with security and networking solutions across the enterprise
- Support geographically dispersed inter-DC traffic and deployments.

Defending a moving target

Data centers are also moving targets. They are always in the throes of a major evolution, migrating from physical to virtual to next-generation environments, such as SDN, ACI, and private and public cloud, growing at an accelerating pace while maintaining high efficiency, dealing with increasing cloud utilization and the emerging Internet of Things (IoT), providing for “Big Data”, supporting the expansion into manufacturing floors, energy delivery, healthcare facilities, and transportation, and increasing use for real-time decision making. And these are just some of the changes in the last few years.

Modern data centers provide a host of applications, services, and solutions to businesses. And many organizations rely on services that have been deployed across geographically dispersed data centers and multiple entities and enterprises to support their growing cloud computing, traffic, and highly mobile work force needs. They also need to support strategic initiatives like big data analytics using completely different architectures and business continuity management, that make redundant data centers an even more critical part of the enterprise backbone.

Provisioning and performance requirements significantly impact how and where security solutions, like next-generation firewalls, are deployed, and the traffic they can inspect without impacting the business. Security cannot undermine data center performance, applications, or services, but must be provisioned dynamically in real time and scale to handle high-volume bursts of traffic.

Five things to consider

While a comprehensive review of data center protection requires a lot more than a short piece can include, here are five of the key things to look at:

Provide visibility and control over custom data center applications. Data center administrators need visibility and control over custom data center applications if they are going to take responsibility to protect them. If they don't have this ability, all they can really do to secure things is isolate applications and limit their usage. They cannot recognize, inspect, or secure custom data center applications without visibility into and control over them..

Manage asymmetric traffic flows and application transactions between physical and virtual devices or data centers. Security must be integrated into the data center fabric, not simply sit at the edge. Solutions on the edge cannot inspect both inbound-outbound and inter-server traffic flows without severely impacting performance and functionality. Inter-server transactions represents the bulk of today’s data center traffic, and in many organizations it is lightly inspected, if at all. If application traffic must be sent to the perimeter for inspection, dynamic traffic flow and application performance required by modern data centers cannot be facilitated. In order to make good decisions about protection, traffic and content of application flows must be understood and addressed. In dynamic situations, component parts and communications change in real time, so efficient provisioning of protection requires integration at the same level of the provisioning takes place.

Adapt as data centers evolve. As data center environments migrate over time, protection must also migrate, scale dynamically, integrate across generations and

versions, and support reversion and hybrid data center environments. Automatic policy creation and enforcement is required as new devices are provisioned and identity management integration becomes critical to reducing deployment times to hours or minutes. While a single solution would be great, the reality today is that there are many moving parts that must be integrated, and architectural understanding that has to be codified in order to automate deployment and provisioning of relevant components and configurations.

Address the entire attack spectrum: Intelligence, entry, expansion, persistence, and exploitation. Traditional network security approaches offer limited threat awareness and visibility in a data center environment, and focus primarily on blocking at the perimeter. Addressing the entire attack spectrum requires protective mechanisms at multiple locations and levels. A holistic approach to securing the data center the full spectrum architecturally is a fundamental requirement for success.

Protect the entire network. Any data center security solution must acknowledge the remote user's need to connect to critical data center resources. It needs to provide transparency between the remote user and data center resource, and be an integral part of a complex network environment extending through branch offices, across the core, into the data center, and out to the cloud. The security solution must be part of the data center architecture and a broader solution that can seamlessly address the full spectrum of integrated components required for overall protection of the enterprise.

How to get from here to there?

Lots of companies are in the space of implementing whatever you decide you need, and systems integrators are available across the space. But the real costs and consequences of success and failure stem from the core decisions you make early in the process. Good decision-making about protective architecture leads to reduced costs and consequences and bad decisions end up propagating to all aspects of implementation, provisioning, and most importantly change management. A well devised architecture starts with the understanding for the need to evolve this critical business infrastructure over time and addresses the protective needs without unduly constraining the implementation. Integrated architecture with a sole source supplier can produce very high quality integrated solutions, but the best of breed approach, if integrated using standards, allows for adaptation over time and point solutions that may be far higher quality. Finally, great care should be taken in deciding whether and how much to evolve versus redo. In many cases, it's better to start anew than to carry the baggage of prior decisions with you, and it's often feasible to transition smoothly if the process is well thought out.

Summary:

Data center security has changed. To truly protect the modern data center, comprehensive architecture supported by strong and automated provisioning is a core requirement. They need a comprehensive collaborative and integrated security strategy and architecture that provides consistent and intelligent protection across the entire distributed network, from the Internet edge through to the data center and out to the cloud, without undermining performance, provisioning, or business objectives. Starting with the protective architecture for the enterprise, data center protective architectures should be well thought out in advance taking these critical issues into consideration.

