Virtualization and cloud security

This is an emerging category. For some time – if we can look relativistically – there was a notion that we could secure the cloud with the traditional protections we have used for years in the hardware-defined data center. That turned out to be only half correct. We still need the functionality of traditional protections – at least in part – but the manner of deployment is quite different.

This category looks at both virtualization and cloud security. At first blush these seem like the same thing. But it's a bit more complicated than that. First, the cloud is not a technology. Rather, it is a business construct. That means that all of the deployed technology is at the mercy of contracts, not products. These contracts determine what you can and can't do.

DETAILS

Vendor Catbird Networks
catbird.com

Flagship product Catbird Insight and Catbird Secure
Price Annual recurring fee based on number of physical hosts. Catbird Insight starts at $3,200; Catbird Secure starts at $8,000.
Innovation Approach to security visualization and security automation.
Greatest strength Ability to address very large virtual environments efficiently.

Catbird Security

This is another company that we have been watching carefully. They have an interesting heritage that gave them the foresight to envision a day when there would be a virtual infrastructure. They saw this back when the company was founded in 2000.

Their offering is split into two products: Insight, which allows grouping of assets and gives access to assets and flows; and Secure, which allows automated security policy, procurements, auditing and enforcement. This provides consistency across policies across platforms. The CatBird system does not require agents because it sits on the hypervisor. It deploys very lightweight security wrappers around assets to be protected.

Catbird is extremely customer-oriented. Much of the functionality of its suite came from customer input. For example, the company was challenged by customers to provide actionable intelligence based on changes from baseline, a technique CatBird calls baseline vs drift.

Then customers challenged the company to ingest third-party netflows allowing them to dial back the clock to see when a data breach occurred and to see impacts more completely.

The challenges continued and continue to shape CatBird's offerings. So far, among other requests, customers have asked for an executive dashboard, creation of a "bad IP" zone for more actionable intelligence, extending the model
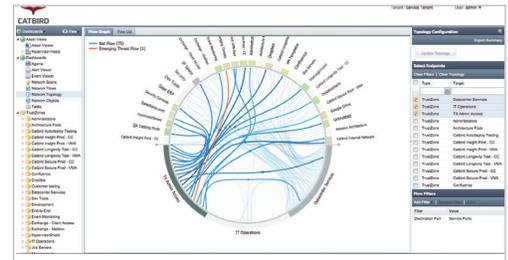
(the wrappers are seen as secure containers) to include physical and public cloud workload, and providing a single dashboard for an enterprise view of actionable intelligence. Customers usually start with Insight and then move on to Secure.

Although the suite currently uses an agentless model for in-fabric visibility, the future will likely be a hybrid of both agent and agentless.

Another innovation is CatBird's approach to visualization. This is the way it shows network data and is able to show and visualize massive volume in an application context. Also unique is the company's approach to security automation. In the virtual world an organization might have thousands of virtual machines. These machines come and go rapidly making the virtual landscape an ever-changing one. The organization cannot manage them manually. That's where the CatBird tools come to the rescue. Applying security policy uniformly and automatically in this environment is the challenge the company was formed to meet.

CATBIRD®

1800 Green Hills Road, Suite 113 Scotts Valley, Ca 95066
Phone: 866.682.0080
http://www.catbird.com/
Twitter: @CatbirdSecurity