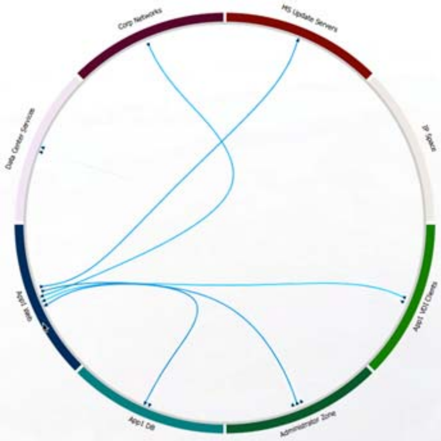
Catbird Insight

See Your Virtual Infrastructure in a Way Never Before Possible



- Virtual Asset Discovery
- Logical Asset Grouping (Micro-Segmentation)
- Visualize & Analyze
- Traffic Flows

> " *Thanks in part to emerging analytics and automation technology, network segmentation at a granular level – micro-segmentation – is now possible. This a significant security advantage of virtualization, and is a prime example of how software-defined innovations present an opportunity to reinvent defenses.*"
>
> Adrian Sanabria
> Senior Security Analyst at
> 451 Research

You Can't Secure What You Can't See

Security begins with knowing what's running in your data center or cloud. In a virtualized environment, Virtual Machines are being added and removed all the time. Having an exact inventory of all virtual assets at all times is a pre-requisite to secure your virtual infrastructure.

Beyond knowing the assets, you need to understand how virtual assets interact with each other. Observing traffic patterns between every individual Virtual Machine and all other assets in your virtual fabric would be cumbersome and probably not that meaningful. But what if you could group virtual assets into logical zones – based on applications or users, for example – and be able to monitor all of the network traffic going to and from each zone in real-time?

The Nirvana of Micro-Segmentation

Grouping virtual assets is a first step toward micro-segmentation – a concept at the heart of Software Defined Networks (SDN) and software-defined data centers. Micro-segmentation provides an opportunity to complement the traditional perimeter security model with workload-centric security.

Even if you are not yet at the stage of implementing SDN, or still have to choose a particular SDN technology, you could already reap some of the benefits of micro-segmentation today by monitoring and analyzing interactions between logical zones. You can start with this non-intrusive first-step that prepares you for future automated enforcement of fine-grained security policies for each micro-segment.

Catbird Insight

Catbird Insight gives you unparalleled visibility into your virtual infrastructure and prepares you for micro-segmentation and SDN. It is a non-intrusive solution that automatically and continuously discovers all assets in your virtual fabric, allows the grouping of these assets into logical Catbird TrustZones®, and visualizes asset relationships and the east-west traffic flows between them for improved analytics. Deploying Catbird Insight provides you with the following instant benefits:

- Real Time Inventory: You know exactly – in real time – all the assets that exist within your virtual fabric. A business unit within your organization just deployed a new VM? You'll know about it instantly.
- Logical Grouping: You can group assets into logical segments – which we call Catbird TrustZones (micro-segments) – allowing you to structure your virtual fabric to support the needs of the business. In fact, you can group assets any way you want – by application, by application tier, by business unit, by compliance framework, etc.
- Contextual Visualization: You can visualize the traffic flows between Catbird TrustZones. This detailed, real-time view of how traffic is flowing in and out of your logical groups is generated based on NetFlow traffic.
- Analytics: You can slice and dice all information gathered by Catbird Insight. A powerful analytics capability allows you to look for misconfigurations, anomalies, and opportunities to tighten security policies.

CATBIRD®

Challenges Addressed by Catbird Insight

- Lack of visibility into what is happening within the virtual infrastructure
  - No accurate real-time inventory of all virtual assets
  - No visibility into east-west traffic
  - No flexible way to group workloads around policies
  - No visual representation of the virtual infrastructure in a way that's understandable to the business
- Lack of security validation within the virtual infrastructure
  - Inability to alert on anomalies versus security baseline
  - No contextual information based on merging virtualization and security information
  - No analytics capability to assess effectiveness of security controls
- Seeking guidance on migrating apps from legacy security/networking to micro-segmentation
  - Struggle to understand existing application connectivity
  - Challenge to model ACLs for security groups / micro-segments
  - Application owners need visual reassurance that application connectivity requirements will be modeled correctly in micro-segmented infrastructure

How Catbird Insight Works

- Asset Discovery: By continuously monitoring both the hypervisor inventory and L2-L4 network events on your logical switches, Catbird gives you a real-time lens into your virtual environment. Our position on the hypervisor provides two correlated observation points so you'll know with confidence what's on your network.
- Zoning: Catbird provides the ability to group your assets into logical containers called Catbird TrustZones (micro-segments). Catbird TrustZones allow for a flexible method to arrange and view your applications, regardless of how your network is configured.
- Flow Visualization: You get a detailed, real-time view of how traffic is flowing in and out of your Catbird TrustZones. This gives you a deep understanding of how your applications and users are connected, and allows you to confirm that your firewall controls are properly in place.

Catbird

Catbird is a pioneer and leader in software-defined security for virtual infrastructure. Catbird's software suite of products was designed from the ground up to provide visibility into and protection of private clouds and virtual Data Centers, and is available for both VMware and OpenStack.

Catbird Insight Provides:

- DC/Cloud team:
  - Get exact and instant inventory of all virtual assets
  - Understand how virtual assets - organized into logical zones - interact with each other
  - Immediately know when new assets are deployed
- Network team:
  - Understand traffic flows within the virtual fabric at the vSwitch level
  - Prepare for micro-segmentation based on baselining
- Application owner:
  - Get real-time view into how your application interacts with other virtual assets and users
  - Validate application behavior
  - Understand application connectivity and firewall requirements
- Security and compliance team:
  - Validate whether security policies work effectively based on visualizing actual traffic flows
  - Determine baseline policies in view of micro-segmentation implementation
  - Baseline assessment, then continuous monitoring and alert on drift

www.catbird.com

1800 Green Hills Road Suite 113 Scotts Valley CA 95066 USA Tel 866 682 0080

CATBIRD