CASE STUDY

Protecting Virtual Networks

A Telecom Case Study

CUSTOMER

Fortune 500, US Based, Multi-national Telecommunications Company

BUSINESS OBJECTIVE

Deploy a new software-based architecture with open standards designed for scalability, efficiency, and open architecture

CHALLENGE

Maintain consistent security through the deployment of run-time security for dynamic workloads

SOLUTION

Tunable policy with run-time security controls, simplifying deployment and management while integrating into existing security and operations platform investments

INTRODUCTION

Today's telecommunications companies are faced with many challenges in their data centers. The explosion of bandwidth requirements, ongoing competitive threats, and increasingly complex customer requirements are forcing carriers to find efficiency and differentiation through their infrastructure designs. These new designs take advantage of Software Defined Networking (SDN) and Network Function Virtualization (NFV) to avoid the high TCO of static architectures while improving their agility. Carriers continue to be a significant target of breach attempts so these new architectures need to include a security approach that are equally agile and address the gaps created by NFV and SDN which the legacy perimeter security model fail to address.

CUSTOMER SPOTLIGHT

One of North America's largest telecommunications companies embarked on a project to simplify, scale, and secure their network services for both internal and external consumption based around the concepts of NFV. It quickly became apparent that their best security solution would be one that supported a cloud-based software security platform, allowing them to de-couple security from hardware.

The physical network security solution they had previously, relied on perimeter-based protection at strategic choke points on the network. By moving to a cloud-based software solution operating within the virtual network fabric, they were able to assign protection at run time based upon user need, access method or application, which made it easier and faster to provide services. Run-time security virtualization delivered the additional benefit of improved overall security, as protection was now based on tunable policies.

THE CLEAR CHOICE

After surveying the market for a strategic vendor relationship to help meet these aggressive goals, Catbird® became the clear choice. Catbird worked with the company's internal teams to successfully deploy cloud-based security in multiple production environments on VMware and OpenStack platforms. The Catbird solution provided policy-based security controls applied at run time based on the application and business requirements. Catbird's solution easily integrated with the existing network security as well as delivering additional correlated intelligence for threat management, network management, compliance, and other stakeholders.

CATBIRD®

THE CHALLENGE OF "CONSISTENCY"

Telecommunications carriers, arguably, have the most complicated infrastructure in the world. This customer has over three thousand internal applications that will run in various configurations on the virtual network. Catbird provided a single piece of software to them that harmonizes physical and virtual controls as well as physical and virtual networks.

By choosing Catbird, this customer was able to solve their key challenges of maintaining consistency across their security controls, enabling rapid deployment of secured services with tunable policies, and ultimately reducing TCO with a solution that integrates with existing investments. Driving improvements in agility, situational awareness, and operational savings through security automation, Catbird enables protection at run-time, based on business requirements, and validated through the life of the assets. Additionally, Catbird supports future growth and technologies, such as SDN and NFV.

CATBIRD PROTECTION

Catbird delivers security policy for virtual and cloud infrastructure, verified and enforced to leading standards. Catbird secures the cloud by applying elastic policy protection across the network, making the cloud compliance-aware and enabling simplified scope management and cost reduction.

Visit www.catbird.com to learn more about how you can secure your private or hybrid cloud with Catbird.

vmware READY

VBLOCK READY

HOW IT WORKS

Catbird delivers security at run-time based on tunable policies.

FEATURES

Technical security controls include:

- Firewall Orchestration
- Network Access Control (NAC)
- Intrusion Detection and Protection (IDS/IPS)
- Netflow
- Vulnerability Monitoring and SCAP Configuration Checks
- Virtual Infrastructure Monitoring integrated with hypervisor APIs for network configuration, access control, auditing, monitoring, and policy enforcement

BENEFITS

- Logical segmentation via Catbird TrustZones®
- Perfect inventory of virtual assets
- Dynamic firewall control updates
- Enforcement of security policies with continuous monitoring, alerts, mitigation, and quarantine
- Security controls mapped to compliance frameworks (PCI, HIPAA, FISMA, SOX and more)
- Proof of compliance with audit capabilities, real-time data flow, compliance graphics and audit ready reports

CATBIRD®

www.catbird.com

Catbird 1800 Green Hills Road Suite 113
Scotts Valley CA 95066 USA
Tel 866.682.0080