

Catbird protects hypervisor as malware fears set the cat among the pigeons

Analyst: Rachel Chalmers

Sector: Enterprise Software

As virtualization sweeps into datacenters, the small and shrinking cadre of holdouts cling to one last shred of justification: It's not yet clear whether the hypervisor is secure. If it's not, adding an extra layer of vulnerability under datacenter Windows servers looks less like shrewd business practice and more like madness. Thus a cottage industry around securing the hypervisor has been born.

Catbird Networks is one of three companies The 451 Group is tracking in this sector. The company built its business around physical-world Web security and network access control. In June 2007 it introduced Catbird V-Agent to do the same for virtual networks running inside a single physical server.

IMPACT ASSESSMENT

The message

The company's V-Agent software runs as a guest system within a virtualized network, reporting on network services and vulnerabilities to a collector hosted on premises, with a managed service provider or inside Catbird's own NOC.

Competitive landscape

The other companies working on virtual security are Blue Lane Technologies and Reflex Security.

The 451 Assessment

The most obvious peril hypervisors pose to virtualized network security is simply that they take that network traffic out of the range of conventional security devices. A packet sniffing appliance can't see packets that never leave a given physical server. V-Agent solves that problem by residing within the virtualized network. It's a logical approach to the problem.

Context

Catbird Networks was founded in 2000 by **CenterGate Research Group**, a sort of incubator founded by programmers and infrastructure and network engineers. One of these, Ron Lachman, is also Catbird's CEO. A **Sun Microsystems** veteran, Lachman helped develop NFS and a streams-based TCP that was bundled with Unix System V. In 1989 he sold **Lachman Associates** to **Eastman Kodak's** Interactive Systems subsidiary for \$20m. In the 1990s, as a founder of **Sandpiper Networks**, Lachman helped pioneer Internet caching.

He's not the only experienced member of the management team. VP of sales Edmundo Costa and VP of marketing Tamar Newberger both joined Catbird from **Tarantella** and **Santa Cruz Operation**. During his stint at **Array Networks**, VP of development Samuel King helped build an SSL VPN. But Lachman's role is key, if only because the major investor in the company is **Lachman Goldman Ventures**.

Catbird describes its business as security software-as-a-service. Early products included the Catbird Shield, sold to partners as a way to provide their end users with branded Web security and network access control. Customers include the **Stanford Federal Credit Union** and **The Ohio State Bank**.

Strategy

With cost considerations, server consolidation and disaster recovery pushing server virtualization into mainstream datacenter operations, people are beginning to worry about security. Projects like Blue Pill and SubVirt have demonstrated the possibility of creating undetectable malware that runs inside the hypervisor. Traditional security approaches don't always work, because they can't necessarily see the traffic between a hypervisor and its guest OS. That's a big problem, because the hypervisor has unrestricted access to guest systems.

Technology

Catbird's V-Agent is a virtual security appliance that runs as a guest system. It's a hardened and stateless machine with no human interface. It doesn't store any configuration or sensor data. All task execution, updating and data extraction is performed by a collector using encrypted transport over existing IP infrastructure. The collector can reside in Catbird's own NOC, with one of Catbird's managed service providers or in the customer's datacenter. IT operators use a Web portal with role-based access control to talk to the collector.

The combination of V-Agent as a guest system and the external collector lets Catbird monitor network service and vulnerabilities from within the virtualized network. Compliance and configuration management can be handled centrally. Non-compliant guest systems can be quarantined, and the performance and security of the hypervisor itself can be monitored.

Competition

With its low-key acquisition of **Determina**, **VMware** picked up a well-qualified team of reverse engineers. But the idea is not to put its security partners out of business. Rather, Determina is slated to become a platform on which those partners can add value around securing ESX, or so VMware claims.

That's good news for Catbird and for the two other companies working toward hypervisor security: **Blue Lane Technologies**, whose VirtualShield software sits above the hypervisor and below the virtual servers, applying patches in real time as needed; and **Reflex Security**, with a virtual security appliance that looks even more like V-Agent.

SWOT ANALYSIS	
Strengths	Weaknesses
Catbird V-Agent should give datacenter operators and security staff much-needed insight into network traffic within a given physical server.	Let's hope the V-Agent itself can't be subverted. A few more reference customers would help Catbird's case.
Opportunities	Threats
As more and more servers are virtualized, more and more people are worried about how to secure them.	VMware promises it won't tread on its security partners' toes; but its continued growth is now mandated by the public markets. It may not have much choice.

About The 451 Group

The 451 Group is a technology industry analyst company focused on the business of enterprise IT innovation. The company's analysts provide critical and timely emerging-technology insight to clients at vendor, investor, services and end-user organizations – insight that aids both strategic and tactical decision making for competitive advantage.

The company's services include the 451 Market Insight Service, which delivers daily insight into emerging enterprise IT markets; 451 TechDealmaker, a weekly analysis service focused on forward-looking M&A within the enterprise IT business; 451 Special Reports, which are produced on a periodic basis to analyze key emerging enterprise IT markets in greater depth; and 451 Strategic Counsel, the company's analyst-inquiry program, which provides clients with direct access to 451 analysts. The company also produces via 451 Events periodic industry summits and investor conferences that address opportunities and obstacles facing emerging enterprise IT markets.

The 451 Group is headquartered in New York, with offices in key locations, including San Francisco, London and Boston. The company also operates Tier 1 Research – an independent division of The 451 Group, headquartered in Minneapolis – which analyzes the financial and industry implications of developments impacting public and private companies within the IT, communications and Internet sectors.

For additional information on the company or to apply for trial access to its services, go to: www.the451group.com