REPORT REPRINT

Cato Networks targets wide area disruption with secure networking as a service

DAN CUMMINS, JIM DUFFY

13 JAN 2017

The company aims to unify and secure wide area network, cloud resources and remote locations under one set of policies and managed performance specifications.

 |

Cato Networks' vision for secure cloud-based enterprise network services targets a list of pain points felt by the medium-sized distributed enterprises, from appliance and policy proliferation to remote enforcement to expensive backhaul. If successful, the Cato Cloud and Network abstraction, for a unified and secure network governed by one set of policies, may come to represent one of the significant conceptual takedowns of security-as-overlay.

The company's value proposition is stark and provocative, and prices global, encrypted and optimized WAN connectivity for a small fraction of the costs incurred by many companies today for a combination of managed MPLS and unmanaged internet connectivity, as well as the burden of distributed security appliances.

THE 451 TAKE

Cato CEO Shlomo Kramer brings impressive product development and competitive experience to his latest venture, offering a new breed of network as a service. Cato's SDN abstraction unifies and secures the wide area network, cloud resources and remote locations under one set of policies and managed performance specifications. Customers are not tied to POPs or static limitations of underlying security features or infrastructure – potentially delivering important SDN freedoms downmarket and to MSSPs. The company's vision is disruptive, and its opportunity significant. In the not-too-distant future, Cato could attract a long list of satisfied customers and appear on more than a few competitive enemy lists.

CONTEXT

Cato's concept of 'software-defined secure networking as a service' (sorry, acronym fans) takes the shape of a cloud-based secure WAN backbone, targeting the mobility and flexibility requirements of distributed organizations. Distributed companies spend tens of billions of dollars globally on MPLS bandwidth and connectivity, backed by service-level agreements for varying levels of high availability and low latency.

MPLS use cases vary, but typically include VoIP and enterprise applications directly benefiting from performance management or encryption, or both. SD-WAN's intelligent linkage and co-management with MPLS for internet-based services has supported some of the early adoption of cloud-based production environments.

The arrival of workable network overlay technologies such as Cato's approach obscures complexity and integrates security. Software-defined overlays are well-timed for and in response to maturing public cloud application networking and endpoint diversity (e.g., users, devices), and of course, all but dissolved perimeter boundaries. Pressured challenges regarding WAN costs, complexity, service levels, visibility and conformance to controls and policies, including those for security, are what Cato targets.

The Cato opportunity is not greenfield, but consolidated replacement. Incumbents threatened by Cato are likely to respond aggressively, with a mix of price concessions and all kinds of FUD messaging, including pointing to switching costs. In practical terms, companies using SD-WAN services could potentially save big dollars with Cato's simplified cloud WAN architecture; companies with a big investment in securing remote offices with networked UTM (unified threat management) can potentially simplify and improve their security architecture and policies, thereby also saving money.

Cato was founded in 2015 by Kramer and CTO Gur Shatz. Kramer is a security practitioner, former Israeli intelligence analyst, cofounder of Check Point and Imperva, and a notable early stage investor in companies such as Palo Alto Networks and Trusteer (a financial fraud and anti-malware firm, acquired by IBM in 2013). The CEO's operating roles at Imperva were primarily as CEO and president until 2014.

Shatz is the former cofounder and CEO of Incapsula, a provider of cloud security services spun in by Imperva. Shatz's roles at Imperva prior to founding Incapsula were as director of product development, VP of engineering and VP of products. Cato's sales VPs are Glenn Esposito, former Americas SVP of sales for Barracuda Networks, and Stree Naidu, previously VP of Asia-Pacific at Imperva. Cato's VP of operations (including IT and DevOps) is Aviram Katzenstein, a former senior director of R&D at Imperva. VP of marketing is Yishay Yovel, who formerly held the same role at Trusteer.

Disclosed funding totals $50m, including a $30m series B in September 2016 led by Greylock Partners. B round participants included SingTel Innov8 Ventures, US Venture Partners, Aspect Ventures, and founders Kramer and Shatz.

PRODUCTS

The Cato Cloud Network for all WAN, cloud and internet traffic represents a new breed of secure networking as a service, offered on the basis of last-mile bandwidth capacity. Geo-regional pricing varies, but end-to-end in the US is currently comparable to that of SD-WAN services, at roughly $4 per Mbps per month.

Base pricing includes the foundational security stack with NG firewall, application controls and URL filtering; additional security features such as malware detection are charged separately. We believe Cato's approach and its multi-tenant architecture will resonate with managed network security service providers, which have long sought the means to provision once, and easily change a unified security policy, covering internal and external (cloud) based applications, across users and locations.

Cato's software-defined security stack also features discovery and controls that are cloud access security broker (CASB)-like, as well as network forensics. Over time, Cato expects to add additional functionality to its security stack and the software-defined extensibility of its cloud-based network. As of November 2016, Cato had attracted 40 partners and activated 25 customers.

The company's largest deployment at that time covered 36 sites. We estimate Cato can exceed $2m in sales bookings in 2017, based on an average customer count of roughly 65 and an annual cost of $35,000. We believe customer count and customer satisfaction will be the most notable measures of success early on, given Cato's disruptive pricing.

TECHNOLOGY

In addition to Kramer's work and identification with Check Point and Imperva, Cato's was foreshadowed by the emergence of Incapsula, and that company's focus on website protection through the expansion of the security posture of the CDN. Cato offers service-level guarantees, low latency, failover protection, load balancing and route optimization, similar to those of a CDN provider, but in the context of enterprise application networking.

The Cato Cloud Network is a set of global distributed points of presence (PoPs) hosted on a mesh of Tier 1 backbones. Cato's multi-tenant PoP (physical and virtual) servers are composed of Cato's converged network and security stack. Design configuration supports uniform and seamless vertical and horizontal scaling, according to the company.

As noted, Cato's single virtual firewall and security protections address critical functionalities currently appropriate for midsized enterprise-grade adaptive protection and visibility. The product development roadmap could address requirements for other market strata and functionalities over time, however.

The company's logical architecture is composed of the Cato Cloud Network, Cato Security Services and Security Policy. Underlying the Cato Cloud Network are 22 physical and AWS PoPs. The company plans to add two to three PoPs per quarter. Customers are not tied to PoPs. Breaking the link between users and location from a static, assigned security checkpoint (i.e., physical appliance or virtual instance) is one of the company's essential breakthroughs in SDN terms.

Cato contends that dynamic access and portability is achieved by a few types of secure tunneling, including through Cato Socket, a physical black box, at remote branches, a Cato vSocket for cloud-based resources (e.g., datacenter) and a Cato Client for mobile VPN.

Management believes its architecture can appeal to companies taking a gradual approach to reducing managed WAN costs, using Cato as intelligent SLA-backed internet augmentation to MPLS links. In the short run, however, the company seems well-positioned to compete with a variety of proxy and cloud access broker offerings that attempt to solve (or just uncover) the problem of remote workers that access the internet directly and are beyond the reach of security policies.

COMPETITION

As noted, Cato is distinguished by its ambitious vision for secure networking as a service. If successful, the company and its competitors could potentially induce a steepening of SDN services adoption, and migration away from a slew of security vendors already facing intensified buyer scrutiny.

Cato is investing aggressively in lead-generation and marketing content targeted at SD-WAN shoppers, which dovetails with our expectations of continued migration to SD-WAN, and in particular, cloud-based security offerings of SD-WAN incumbents and startups, such as Cisco, Versa Networks, Viptela, CloudGenix, VeloCloud, Citrix, Silver Peak, Cradlepoint, Aryaka and Riverbed.

Versa, for example, highlights software-defined security with virtual firewalling in marketing for its FlexVNF SD-WAN product. Cisco's cloud-based IWAN-as-a-Service emphasizes security as well, through IPSec tunneling and VPNs. We believe MPLS investments will be largely capped with SD-WAN, as such embedded infrastructures and services are augmented with broadband internet and LTE, provided these services can offer the same SLA assurances, security and reliability as legacy MPLS. On the SD-WAN/CDN side, we think expectations that Aryaka will potentially add easy security options could be hastened by Cato's traction.

On the security side, Cato looks to replace zScaler as a top go-to option for moving proxy-based screening and filtering to the cloud. ZScaler recently added internally sourced and partner-provided options for its customers seeking intelligent WAN connectivity. Cato's unified approach to security policy management and aggressive pricing could trigger notable competitive responses, if not direct M&A in response, by a range of point product vendors.

In the UTM competitive landscape, innovation has been incremental, at best, for many years. A number of vendors, including iboss, zScaler, Bat Blue Networks, Sophos and Barracuda Networks are addressing demand for the substitution and replacement of remote UTM appliances with unified, cloud-based software instances. However, most of the security and UTM incumbents that have or are trying to add network connectivity to their cloud offerings lack deep integration with an SD-network overlay.

We view Cato as differentiated by its purpose-built, converged secure cloud-networking stack and multi-tenant architecture, which does not tie customers to PoPs, is not composed of custom appliances for customers (other than access sockets) and is unlikely to incur traditional scaling and activity costs attributable to customer expansion. In general, we believe a substantial portion of the multibillion-dollar UTM market targeted at distributed deployments will be at risk, over time, as managed network security takes hold in the mainstream.

SWOT ANALYSIS

STRENGTHS

Cato offers potentially compelling savings, as well as a greatly simplified approach for secured, cloud-based networking services for the mid-tier distributed enterprise market. Companies with significant dollar and resource investments in networked UTM appliances for remote offices can potentially simplify their security architecture and manage their organizations under a single cloud-enforced policy.

WEAKNESSES

Cato is small and modestly funded relative to its large market opportunities, and competitors potentially threatened by its innovation and success. Traction for Cato may develop gradually on the basis of discrete service replacements in series, customer by customer, and perhaps after lengthy, detailed trials.

OPPORTUNITIES

Managed network security service providers should welcome Cato's approach for managing a single unified security policy for an entire distributed organization, covering all applications across users and locations.

THREATS

Cato is not targeting a greenfield opportunity. The company's offering addresses a variety of enterprise networking, security and operational pain points, and thus may face tough sales and evaluation cycles. Threatened incumbents are likely to respond aggressively.