REPORT REPRINT

Illumio aiming high at scalable security policy portability, all workloads

DAN CUMMINS, ADRIAN SANABRIA

2 MAY 2016

The company's mission is to protect distributed, dynamic and heterogeneous application workloads. Illumio's platform targets the role of authoritative and scalable datacenter policy management console, starting with control over host-based firewalls, and pointing toward broader orchestration use cases.

451 Research®

 |

Illumio's Adaptive Security Platform (ASP) is designed as a whitelist policy control layer for physical and virtual enterprise datacenters. The Illumio ASP layer leverages an understanding of business-driven application policies above, to secure virtual or physical infrastructure below. The company has, so far, articulated use cases ranging from automated segmentation at network and application layers to dynamic application migration. According to Illumio, users of its ASP are gaining experience with unified and flexible application-centric policy management in corporate datacenters, in multivendor virtual environments and with bare metal servers.

THE 451 TAKE

Illumio takes aim at hardening the datacenter's infamous 'chewy center,' leveraging automation, orchestration and intelligence of the business context of application data flows. Simply put, Illumio observes the resources necessary for an application to function. The inverse (what the application doesn't need) can then be leveraged to restrict access to application components through the platform's automation and orchestration. Illumio aims to accomplish this using products and components already running in the customer's environment, reducing the cost and complexity of this approach. The platform targets the role of authoritative and scalable policy management console, starting with control over host-based firewalls, and pointing toward broader orchestration use cases.

CONTEXT

Datacenter network virtualization continues to pave the way for security virtualization, the most notable networking construct of which is application-centric micro-segmentation. While virtual networks can track and serve connectivity requirements of distributed applications and workload components, micro-segmentation is necessary to isolate and protect distributed workloads from prohibited connectivity. Illumio contends that its approach to micro-segmentation is value-additive, using business-context policy whitelisting at sub-workload process levels, running on virtual hosts or bare metal servers. With respect to datacenter heterogeneity (i.e., physical, virtual, multivendor), Illumio is targeting an important role as a single, authoritative and scalable policy management platform, starting with a broad sense control span solution for distributed virtual firewalls, and pointing toward a broader orchestration use case.

Illumio is led by CEO and cofounder Andrew Rubin, CTO and cofounder PJ Kirner, and chief commercial officer Alan Cohen; the CEO and CTO were previously president and CTO, respectively, at Cymtec Systems, a cloud-based IDS and network-monitoring vendor that Rubin cofounded. Prior to Cymtec, Kirner was a senior distinguished engineer with Juniper Networks. Cohen was previously with Nicira and Airespace, acquired by VMware and Cisco, respectively; he previously led Cisco enterprise marketing. Recently the company added Nathaniel Gleicher, former director of cybersecurity policy for the National Security Council at the White House, as head of cybersecurity strategy. Illumio's VP of engineering, Ben Verghese, worked at VMware, where he was chief management architect.

Illumio's board of directors currently comprises Rubin and Cohen, Steve Herrod of General Catalyst Partners, John Jack of Andreessen Horowitz, Joe Lonsdale of Formation 8, and John Thompson, former CEO of Symantec. Total funding to date is $142.5m, including $8m series A led by Andreesen Horowitz, $34.5m series B led by General Catalyst and $100m series C co-led by Accel Partners, Formation 8 and Blackrock. Andreessen Horowitz participated in all funding rounds to date, while General Catalyst and Formation 8 were B and C round participants. Non-lead investors also include Juniper Networks (series A), InstantScale Ventures (series B), and Data Collective (series C); Private investors in series C, in addition to Thompson, included Marc Benioff, CEO of Salesforce. Jerry Yang, founder and former CEO of Yahoo, is also among the company's private investors.

As of early April, Illumio's customer roll had jumped to 45 from fewer than 10 a year ago, and includes companies such as Morgan Stanley, Plantronics, Salesforce, NetSuite, King Digital Entertainment and Creative Artists Agency. Management indicates that 90% of current deployments are within corporate datacenters, and can be characterized as early adopters. Such companies have immediate requirements to monitor and control connectivity within datacenters, scale security policies over growing numbers of virtual machines and containers, and prepare for longer-term plans to run and secure hybrid virtual datacenters.

Headcount is currently 152, with about 10-15% of staff garnering experience with virtualization adoption at companies such as Nicira and VMware. The annual subscription revenue model is priced per workloads managed. We estimate the current annual sales (run rate) at $16-24m, based on our annualized revenue per customer estimate of $400,000 to $800,000. The platform's selling points around scalability and automation in complex environments imply to us that Illumio is unlikely to seek market traction below large business tiers. Annual spending by large customers could approach or exceed $1m-plus per year, we believe. On the customer side, management indicates that sponsorship and funding is diverse, including infrastructure operations, security initiative funding and the business at large, given complementary capability with GRC, for example.

PRODUCTS

ASP's key characteristics are independence from infrastructure, distribution to application workload levels, and consistency across virtual and physical computing environments. ASP's core service capabilities are Illumination (inspection and visualization), Enforcement (workload policy provisioning and monitoring) and SecureConnect (encrypted connectivity between all workload elements). The user interface centers around an interactive communications map, with drill-down inspection and rule editing at host, flow and process levels. Use cases include establishing highly controllable and visible borders around high-value applications and data, migrating applications and consolidating datacenters, separating functional environments, managing hybrid infrastructure under consistent policy, and controlling identity-based domain access. The average firewall administrator would likely see the value here quickly – Illumio is automating the tedious task of doing the due diligence, rule-writing and testing necessary when making changes to a firewall. The fact that network segmentation is still largely a painful manual process today makes it clear why Illumio chose to tackle micro-segmentation as one of the first use cases for its platform.

Management believes that ASP's workload and process level automation focus can help build capability for continuous delivery of applications, which integrates compute capability and enables DevOps-friendly orchestration use cases. Illumio also indicates that some customers find particular value with abilities to quickly meet regulatory requirements, such as establishing PCI-compliant infrastructure, data isolation zones or continuous monitoring.

According to the company, ASP interoperates out of the box with existing security solutions, and does not require changes to networks. In terms of its potential to extend the capability of existing assets, the Illumio platform targets a 90% reduction in complex and highly manual work, smaller attack surfaces, higher visibility over traffic flows and wider spans of control. Management reports customers are also finding particular value informing configuration management systems with Illumio's application discovery data.

In mid-April, Illumio announced its Attack Surface Assessment Program (ASAP), a new consultative risk diagnostic. ASAP cleverly functions as a compelling sales tool, demonstrating the problem ASP is suited to address by using the customer's own environment as the demonstration, or proof of concept. ASAP highlights server and communications flows that represent high-value targets, logical attack paths and areas ripe for intensified policy focus and monitoring; the diagnostic can be run remotely over a few hours, and will be offered free for a limited time.

TECHNOLOGY

Illumio's ASP is comprised of a distributed system controller called the Policy Compute Engine (PCE) and a guest-OS/workload level agent called the Virtual Enforcement Node (VEN). Patented IP includes the PCE's capabilities to analyze context across distributed workloads and rapidly generate and adaptively iterate large-scale policy models. VEN agents profile workloads contextually and continuously, by system properties, connective relationships and dependencies, and environment. The PCE controller combines VEN workload discovery data, system-level telemetry and monitoring, with business rules to compute optimized workload policies. Policies are then communicated back to VEN agents for provisioning to the real enforcers – kernel-level filtering. The host firewalls built into Linux and Windows, iptables and the Windows Filtering Platform, respectively, provide granular policy enforcement. Illumio contends that the VEN, as a lightweight agent, does not impede performance; the VEN is not a packet processor or filter, but rather akin to an antenna to collect and transmit workload context to the PCE, receive policy from the PCE and provision policy to workloads' OS kernel. The company has formed technology alliances with Nutanix, Citrix, F5, Docker and Mesosphere. Illumio recently added capability to query user and group level entitlements in Windows Active Directory, in order to generate contextualized user-to-workload policies.

We expect Illumio to complete additional integrations with identity vendors, as the focus on east-west traffic visibility and control dovetails with the necessity to monitor and control credential escalation risks, such as those associated with virtual desktop infrastructure. Illumio also integrates with DevOps application lifecycle configuration and orchestration tools such as Chef, Puppet and Ansible (Red Hat).

COMPETITION

An important differentiator in this market revolves around the architectural approach to which vendors commit. Illumio, as an agent-based approach, is limited only by the operating system in use (Linux and Windows at the time of publishing). Vendors such as vArmour and Catbird leverage virtualized networking frameworks, and as such are limited to the borders of virtual platforms. For example, if Catbird is being used in vSphere or OpenStack environment, its capabilities are limited to the virtualized workloads running within each respective environment. Illumio can deploy to any environment (virtual, cloud, bare metal) as long as versions of Windows or Linux compatible with its agent are in use. While products from the cloud infrastructure security (CloudPassage, Dome9, ThreatStack, FortyCloud) and software-defined security (vArmour, Arkin, Catbird, VMware NSX, Cisco ACI) space have some overlapping features, we've not seen any that compete directly with Illumio's particular set of features and compatibility.

SWOT ANALYSIS

STRENGTHS
Illumio's whitelist policy control layer for physical and virtual enterprise datacenters focuses on much-needed visibility, scalability and business context controls for securing dynamic workloads.

WEAKNESSES
Illumio's platform is seen primarily in the context of advanced, dynamic policy management for public and hybrid cloud workload migration, despite valuable capability away from the leading edge and in traditional datacenters.

OPPORTUNITIES
The Illumio ASP platform targets the role of authoritative and scalable policy management console, starting with control over distributed virtual firewalls, but pointing toward broader IT orchestration and business use cases.

THREATS
Illumio is a small enterprise security vendor, vying for market attention against considerable go-to-market resources of VMware and Cisco and in-house offerings by public and private cloud service providers. With a value proposition challenging to explain to many buyers, Illumio runs the risk of losing to competitors it isn't actually competing with or losing sales due to a lack of comprehension. The challenge will be to convince prospects to try the product, because direct use or demonstrations are most likely to address this problem.