REPORT REPRINT

Portnox connects enterprise reality to its risk-based perimeter

DAN CUMMINS, PATRICK DALY

23 MAY 2017

The company is bringing automated, adaptive controls to network access with a lightweight architecture that enhances customer visibility into network activity.

portnox™

As the foundations of enterprise network perimeters continue to erode under the pressure of IoT use-case and BYOD adoption trends, a wave of demand for lightweight, automated, and robust network discovery, policy and enforcement controls is surging. At 10 years of age, Portnox is a relatively young vendor in the mature network access control (NAC) product segment, with a focus on agentless risk-based controls combined with automated policy enforcement for on-premises or cloud deployment and protection.

THE 451 TAKE

Portnox is helping to redefine the value proposition of NAC, tilting toward visibility and flexibility. The company's sensible risk orientation and the lightweight architecture of its CORE on-prem and CLEAR cloud services appear well aligned to help meet enterprise demand for a better NAC experience. The new value proposition in NAC is about leveraging valuable data hiding in plain sight across diverse environments, increasing visibility and defending a business-driven virtual perimeter. Portnox's deep focus on risk-based assessment and its agentless approach target nearly all vertical markets, addressing IoT device visibility and monitoring challenges, where a light touch is the only way. NAC is a crowded field, and adjacent market competitors are encroaching to address network visibility challenges, as well as the numerous risks associated with unmanaged device proliferation. The potential upside for winning innovations is substantial, and we would not be surprised to see nimble and focused competitors come out ahead in a few years.

CONTEXT

Network access control continues its long journey around the IT galaxy. Upon return from marginalization due to feature bloat and awkward complexity, demand for trimmed and focused NAC is steady and more than respectable, with a number of vendors finding sustainable niche customer strata and focused capabilities. Device and environmental visibility derived from lightweight technologies are among the most valuable product attributes in IT currently. Visibility combined with continuous monitoring, including of user and device behavior, is among the necessary defenses for IoT challenges.

Portnox was founded in 2007 by CEO Ofer Amitai, COO Idan Kuperman and chairman Nir Aran. Amitai has served as CEO since 2015, and previously established the first IT security team in the Israeli Air Force, managed the security division for professional services firm Xpert Technologies and was a regional director of security at Microsoft. Kuperman was previously COO of IAM vendor Datanin and managed the security team of the Israeli Air Force. Aran served as Portnox CEO from 2008-2015, and was previously a managing partner at Datanin and CIO at Laureate Online Education. A fourth cofounder, Ben Kapuler, also worked with the Portnox team at Datanin. Portnox is headquartered in Herzlia, Israel, and has offices in California, Maryland and London. Portnox's headcount today is close to 50 employees, and the company currently indicates a customer count of approximately 500, primarily in North America.

PRODUCTS

Portnox CORE and CLEAR are similar in that they both provide customers with visibility into managed, BYOD, or IoT devices with a vendor-agnostic and agentless implementation. The company also offers a hybrid of the two. CORE and CLEAR each allow customers to see what devices are connected to the corporate network in real time and centrally control network access based on an individual device's risk level. Portnox's implementations are agentless, which is increasingly common and especially important for IoT, given that many of the network-connected devices likely to be found in an enterprise are unable to support an agent-based security product. Both of Portnox's offerings support 802.1x, as well as native protocols, allowing them to profile and understand the risk posture of a wide variety of devices. While CORE and CLEAR are similar in many ways, they have some key differences in terms of how they create value for customers.

Portnox CLEAR is a security-as-a-service offering that works across multiple access layers, including wired, wireless and VPN access points. The company says that it is currently focusing the majority of its development efforts on CLEAR.

CLEAR employs machine-learning algorithms to continuously analyze hundreds of different endpoint parameters, including the state of security applications, known vulnerabilities, insecure system configurations and missing patches. In the case of detecting vulnerable or compromised devices, CLEAR will automatically notify the security officer or IT manager about the high level of risk and remove such a device from the network.

CLEAR is designed to provide rapid, detailed visibility and discovery of endpoints and their configurations. Through the CLEAR web portal, administrators can query connected devices with respect to OS, patch levels, installed applications, running services, other connected peripheral devices and other states. CLEAR enables virtual perimeters defined by business constructs, including remote access VPN integrated with Active Directory and PKI.

In addition to agentless implementation, organizations that prefer or require a managed device framework can opt for AgentP, a lightweight device agent designed for continuous monitoring that supports Windows, Mac, iOS and Android. Portnox recommends AgentP for advanced automation and enforcement use cases on the endpoint, including for vulnerability assessment, provisioning and configuration, and policy-based hardening. Device onboarding with AgentP is also very simple for the customer, and only involves logging into the Portnox cloud portal with email credentials, downloading the software and registering the device. This approach can enable monitoring and control beyond the reach of corporate networks.

On-premises and agentless CORE delivers IoT device identification and profiling, segments devices according to their unique characteristics, and automatically blocks suspicious devices from accessing the network. Portnox also recently released new behavioral analytics capabilities that let customers monitor devices for suspicious configuration changes and automatically react to these changes, quickly identifying and blocking compromised devices. CORE's new dashboard also provides enhanced visibility, with the ability to drill down into the data collected and see all of the activity on the network on a device-by-device inventory basis or via a NAS view. While the device view allows customers to see what is happening with each individual device, the NAS view offers visibility into the network equipment information.

COMPETITION

Network access control is a mature market composed of large, established infrastructure vendors and focused specialists. Portnox's primary competitors are ForeScout, Cisco, HPE Aruba, Juniper Networks and Bradford Networks. Of these, Portnox's offering most closely mirrors ForeScout's in that both emphasize easy implementation and device onboarding, without agents. In the industrial sector, Portnox may run into Sensify, a blockchain-based NAC vendor specifically focused on securing SCADA field devices with intermittent network connections.

We expect the NAC products as a whole will increasingly compete against a slew of emerging visibility, enforcement and automation technologies with the potential to cannibalize some enterprise NAC investment. Primarily, software-defined perimeter (SDP), policy provisioning and enforcement vendors like Vidder, Soha Systems, FortyCloud, Illumio, Verasynth and Cryptzone may come to represent appealing alternative approaches to securing network access, as compared with more traditional NAC technologies. Some view SDP as a potential answer to the deteriorating network perimeter caused by forces such as BYOD and IoT. While NAC typically involves determining access after an initial connection has been made, SDP technology inverts this approach by trusting nothing and denying everything until specific permissions are granted. We note that Portnox and other NAC vendors have incorporated SDP-like principals and functionalities into their products. For example, Portnox is capable of establishing trust before access to the network is granted, and then the device is continuously monitored from then on.

SWOT ANALYSIS

STRENGTHS

Portnox's focus on cloud-advantaged visibility, along with its lightweight architecture, is ahead of the curve in terms of bringing a strengthened value proposition to a mature NAC market.

WEAKNESSES

Portnox is subscale with a mild competitive profile, in relative terms, when compared with NAC segment leaders Cisco, HPE and ForeScout. The company, however, is a nimble, focused and well-regarded vendor in a product segment where value is being redefined.

OPPORTUNITIES

Portnox can continue to primarily focus on selling to the North American market while increasing growth by expanding into other geographical regions.

THREATS

The dissolving network perimeter presents all kinds of competitive and existential threats to all kinds of vendors. Portnox appears well ahead of the general threat to NAC, helping organizations cope with heterogeneity and shifting contours of on-prem and cloud IT environments.