NAC Battle Card

HIGHLIGHTS

- Headquartered in Campbell, CA (Silicon Valley).
- Product: PrecisionAccess™
- PA protects some of the world's most sensitive applications.
- Exec team includes co-authors of Software Defined Perimeter specification.
- No product breaches, including three hackathons (2 RSA; IAPP-CSA Congress)

USE CASES

- Network Access Control
- Data Center Segmentation
- Cloud Migration
- Field Worker Remote Access

PROTECTION AGAINST

- Server exploitation
- Credential theft
- Connection hijacking
- Compromised devices

VALUE PROPOSITION

PA's single layer of enforcement across the most complex, demanding networks, including cloud, delivers unprecedented scale, security, control and economy.

INNOVATION ADVANTAGE

Software Defined Perimeter technology combined with Vidder's Trust Assessor™ gives PrecisionAccess a superior architecture for protecting large, complex networks from advanced threats.

CATEGORY OVERVIEW

NAC solutions emerged in 2006 as a viable way to protect networks from internet worms as WLAN adoption went mainstream. Most rely upon primitive posture check parameters for enforcement, essentially allowing devices to connect to a network and access all internal servers. There are two basic types: 1) traditional using 802.1x and 2) based on dynamic switch or firewall controls. Sometimes they integrate with remote access. Basic policies: ON, Guest, Remediate, None. Vidder delivers on the promise NAC struggles to deliver, namely application specific segmentation and authorization.

PAIN POINTS WE ADDRESS

1. **Cost:** Protecting a large, complex network with NAC can cost millions upfront and require very high ongoing OPEX support. Hardware purchase required, also not futureproof for cloud or hybrid cloud use case. Every connection point device requires support for NAC (switches, routers, wireless access points).
2. **Management Issues:** Enforcing granular access for many enterprise networks can require millions of ACLs. Very difficult to segment resources via access control list rules.
3. **Limited protection:** Ten years ago it was enough to simply posture check a device before granting access to a network. Today, with advanced threats and malware, connected (and posture checked) devices are one of the most common routes of network compromise.

WHY VIDDER IS BETTER THAN NAC

1. **Unprecedented scale and control:** PA offers a single point of enforcement (internal, external and cloud) with complete control of data exchange and no dependence upon switch or firewall interoperability. Actionable with manual, semi-automated and automated options.
2. **Enhanced security:** Open networks can be easily segmented into "zones of trust" based on easily enforced, trustful, context-aware access decisions based on tMFA and granular access policies based on user and application. Encryption from user to server, even on the LAN.
3. **Superior visibility:** Deep trust and risk assessment based on: machine learning, multi-feed, dynamic trust assessment; immediate recognition of known malware; zero-day detection with low false positive rates.
4. **Superior economy:** Much more cost effective than traditional NACs, especially in large networks. PA can handle 100,000s of users and 1000's of apps (no ACLs, VLANs, FW rules). Yet initial deployments can start with critical apps with small subsets of users.

NAC Battle Card

PROOF POINTS

- Gartner 2016 Cool Vendor in Security
- SGN Case Study
- No customer or hackathon breaches, including three high profile hackathons
- PA protects some of the world's most sensitive, business critical applications.

COMPETITION

Cisco ISE: Cisco has a very complex licensing model for ISE requiring significant investment, including typical upgrade cycle to every switch and router (any port supporting NAC) See Licensing Notes: https://supportforums.cisco.com/discussion/11898171/understand-ise-licensing. No multi-factor authentication.

ForeScout: Requires 802.1x or agent to dynamically provision routers to support real time ACL functionality. Hardware dependencies, expensive, plays havoc on network as firewall rules and routing tables are dynamically updated via SNMP. Not a network friendly approach. No multi-factor authentication.

FUD

"Vidder requires an agent?"
Yes, but as do most NAC to take advantage of advanced features. Also supports tMFA out of the box at no additional cost. Also replaces most remote worker VPN requirement.

"Vidder does not give visibility to non-authorized device attempt."
True, we are developing visibility, but non-authorized devices can never access Vidder protected resources.

"I already have a NAC solution."
Great! Then you address what can get on the network, and Vidder provides the critical last mile protection without the need to build the ACL's that make NAC so difficult to deploy on a per application use case.

PROOF POINTS

1. Gartner 2016 Cool Vendor in Security
2. SGN Case Study
3. No customer or hackathon breaches, including three high profile hackathons
4. PA protects some of the world's most sensitive, business critical applications

910 E. Hamilton Avenue Ste 410
Campbell, CA 95008
408.418.0440
precisionaccess@vidder.com | www.vidder.com

VIDDER