NAC Attack: Today's Products Will Fail, Report Says

April 7 2007

Vendors say modern NAC products will fall by the wayside in favor of software-based technologies that manage risk by integrating endpoint security, access control, identity and risk management.

Forrester Research analysts are urging corporations to prepare for a shift in the Network Access Control market in the years to come, as NAC vendors move toward new software-based tools that leverage endpoint technology to proactively manage risk.

In a report titled "Client Management 2.0," Forrester analysts Natalie Lambert and Robert Whiteley forecast the death of modern NAC products, which they say feature too much complexity and not enough interoperability. Operations management teams want a unified solution, Lambert said in an interview with eWEEK.

"They feel they deploy tools to solve business problems but then find themselves with more solutions than they can handle," she said. "They want to consolidate, but they aren't seeing any compelling solutions that bring together the functionality they need."

The report also contends that many NAC products focus solely on compliance with security policies instead of the remediation problematic machines, and are not able to defend against newly emerging threats.

In addition, the researchers stated that existing NAC systems often result in multiple policies being established to control the same processes.

Lambert and Whiteley's answer to the situation is policy-based software technologies that manage risk by integrating endpoint security, access control, identity and risk management.

They dub this new generation of client and network security products "proactive endpoint risk management," or PERM.

Proactive endpoint risk management benefits enterprises from both an operational and technical standpoint, Lambert said.

Most firms, she said, are evolving their security teams to focus on risk and higher-level regulatory compliance issues, she said.

As threat protection and systems compliance mature, they will get thrown over the fence to IT operations functions. She called it a mistake for NAC solutions to focus on the network operations team.

"Network ops staffers typically don't focus on dynamic, policy-intensive tasks that require the management of tens of thousands of devices," Lambert said. "We think that desktop operations - which has been working with policy-intensive security and management tools for years - is a much more suitable home for defining NAC policies."

From a technical perspective, it's a more complete management solution, she added.

"Securing an endpoint means managing its entire life cycle," Lambert said. "But today's current NAC solutions don't focus on a complete life cycle. Instead, they specialize in either pre-admission scans or post-admission monitoring - some solutions - do - both - but don't focus on remediation."

Before PERM becomes a reality in the marketplace, however, Lambert

foresees widespread product and vendor consolidation - a process she said has already begun, with vendors such as McAfee integrating traditional client security with information leak prevention and vulnerability management.

For their part, several vendors said NAC products will change. However, not all said they would change in the way Forrester predicts.

At Cisco, company officials said Forrester used too narrow a definition of a NAC product because it only includes a health check of an endpoint.

Brendan O'Connell, product marketing manager within Cisco's NAC unit, said many NAC providers focus solely on whether or not a computer has the latest anti-virus software, and he called that a "mental blind spot."

NAC, he continued, should be composed of four things: authentication, quarantine, posture assessment and remediation.

"There are a lot of other NAC products out there that may have only a subset of those components," O'Connell said.

Contrary to the report's conclusion that the network needs to be de-emphasized, Cisco NAC Marketing Manager Irene Sandler said NAC has to be a network enforcement product - and that the network is where the bulk of the decision-making must lie.

Microsoft executive Mike Schutz said policy has a home in the network, though he said NAC products will evolve beyond the network device-centric approach commonplace today.

"Customers today deploy multiple point security products such as AV

and patch management, but these products rely on the end user to keep these solutions running and up-to-date," said Mike Schutz, director of security and access product management at Microsoft.

"It's easy for users to fall out of compliance, and NAP - Network Access Protection - addresses this problem by pushing IT policy into the network."

Lambert, however, said firms should de-couple their network access policy from their network hardware.

"This policy should then be mapped to the current security and management technologies that can do the heavy lifting and leave the enforcement to the network," she said.

In addition, she advocated realigning IT organizations so that those responsible for endpoint operations are security and IT ops professionals who know how best to create policy to secure and manage the environment.