



Altarum Institute Improves Network Health with ForeScout's NAC

“ After we evaluated CounterACT, the search for a NAC solution pretty much ended since it had literally everything we wanted and so much more than we even realized we wanted or needed. With it, you get three mature products in one—NAC, malicious traffic detection, and vulnerability assessment. ”

AI Wendt
Network Manager
Altarum Institutend user

Altarum Institute, like many organizations, faced the issue of consultants and contractors coming into its buildings and logging onto the network with laptops infected with worms. The most troublesome worm the organization had to fight recently was the Code Red worm, which actually shut down one office for almost two days as the network team tried to contain it. From a business standpoint, deploying a proactive solution became a critical need. Altarum also wanted a solution that would allow it to control who was able to get onto the network and what they would be allowed to do once they had access to the network and its resources.

AI Wendt, Network Manager with Altarum Institute, and his colleagues considered network access control (NAC) solutions from several vendors, including Cisco, ForeScout Technologies, Lockdown Networks, and Mirage Networks, after doing extensive research in trade publications and analyst reports. “After we pared down the list, we asked each to present a webinar so we could learn more about each product, how it operated and how to manage it,” said Wendt. “And finally, we asked vendors for an onsite evaluation to see how it would function in our environment.”

Why ForeScout?

The organization's first priority was that the solution had to be clientless. In addition, management simplicity was important since there would be a small staff responsible for administering the solution. Finally, a solution with low false positives for pre- and post-connect threat detection would be looked at most favorably.

“After we evaluated CounterACT, the search pretty much ended since this product had literally everything we wanted and so much more than we even realized we wanted or needed,” said Wendt. “With it, you get three mature products in one—NAC, malicious traffic detection, and vulnerability assessment.”

How ForeScout Helped

Malware is contained immediately. For example, an employee opened an infected attachment that started sending out spam. CounterACT caught this immediately and blocked the user from sending any more messages. The employee actually had an updated virus protection program yet it failed to catch the malware — but CounterACT did not miss it.

Infected mobile devices cannot infect the network. A guest to Altarum brought in an infected laptop, but once it was connected to the network, CounterACT recognized the malicious activity and immediately blocked it from the network.

An Altarum employee was using various Peer-to-Peer (P2P) applications, which are against the organization's technology policy. CounterACT recognized the applications, alerted Wendt and his team, and the programs were removed.

The ForeScout Difference

Wendt sums up the protection Altarum gets with ForeScout by noting that CounterACT provides not only network access control, which is what the organization began looking for in the first place, but also protection against zero-day viruses and worms.

“While it's not against policy for employees to bring in personal laptops, it does pose a threat, and the same goes for contractors,” said Wendt. “CounterACT eliminates those threats. Even more serious are threats posed by zero-day viruses and worms. With CounterACT's behavioral detection method, our risk is pretty much removed. And in the future, we'll have every user authenticate against Windows Active Directory for more control over who's allowed on the network. So, for consultants coming onsite, we will supply a time-limited username and password which will allow them access only to certain areas of the network for a certain amount of time. CounterACT makes this extremely simple to implement and gives us great flexibility.”

Wendt concludes, “We won't have any more two-day shutdowns because of a worm outbreak with CounterACT protecting us, so the product is pretty much paying for itself. And aside from the many business benefits, a huge benefit for me is that I sleep better at night knowing my network is well protected by CounterACT.”