



Tailored Enforcement that Minimizes Disruption

As Interviewed By John Siefert



T. Kent Elliott
Chief Executive Officer



Q How does ForeScout define Network Access Control/Endpoint security?

A A NAC product must:

- Be clientless so it can detect and interrogate every device connecting to the corporate network, no matter what type, without the need for prior knowledge of the device,
- Not require quarantine by default when immediately identifying company-owned devices and ensuring compliance with network security policies while simultaneously enforcing real-time protection from self-propagating threats,
- Customize the level of enforcement to directly match the level of policy violation, thus avoiding unnecessary loss of user productivity at both the point of connection and for the duration of connection,

- Provide the ability to deploy and enforce with minimal to no disruptions for the network, IT staff, and compliant users – while automatically guiding noncompliant users into compliance, speeding their ability to gain appropriate connection.

Q 40% of the 300 early adopters surveyed in our recent study said a key NAC feature is to “provide controlled access for unmanaged users.” How does ForeScout enable this?

A ForeScout’s CounterACT has the ability upon connection to differentiate between company-owned assets (domain-credentialed devices) and guest or contractor devices.

Logical and physical enforcement. For a contractor attempting to access with a non-managed device, CounterACT can grant access to either a specific range of IP addresses (logical enforcement) or to a specific network segment (physical enforcement) that would enable only allowable resources, thus ensuring the contractor’s productivity without compromising network security.

For a guest who passed through physical security, CounterACT will detect any network access attempt identifying the device as a guest and, based on network policy, either block access completely or automatically move the guest device into a pre-defined guest segment (virtual LAN, guest network, etc.) thereby narrowly restricting access privileges (i.e., Internet access only).

A virtual firewall. CounterACT uniquely features a virtual firewall option to limit access. All this is accomplished using the existing infrastructure and without the need to reconfigure the network.

Q Ongoing threat analysis and containment is considered another key factor in a NAC solution. How does ForeScout’s CounterACT Architecture ensure this?

A CounterACT delivers the ability to provide the same level of compliance assessment throughout the duration of device connection as it does at admission. This is accomplished by re-interrogating connected devices periodically throughout the entirety of their connection and

triggers enforcement if security posture has changed.

If a device falls out of compliance, the same broad spectrum of enforcement options that were available at the time of admission remain in force, ranging from email notification to a hijacked browser session, deploying a virtual firewall, or working with remediation systems (i.e., SMS), or completely blocking access.

Q In our research, 37% and 36% of respondents, respectively, cited HIPAA and SOX as drivers behind their NAC decision making. How is ForeScout taking federal compliance issues into consideration in product development?

A CounterACT leverages existing identity-based information, enabling role-based access enforcement that ensures only the right people are permitted to gain access to assigned resources. From the network level, this means ensuring that the appropriate devices are granted or denied access to the appropriate IP resources.

CounterACT captures all security event and access data, providing the ability to generate specific reports to show compliance trending, employee/security/access event correlation, and security access event resolution.

Q The CounterAct solution is at the core of ForeScout’s network access control play for the enterprise. What differentiates it from other approaches in the market?

A ForeScout’s CounterACT differs from other approaches in four fundamental ways:

1. CounterACT enables dynamic access control security to be extended to the existing switching infrastructure, extending the lifecycle of current infrastructure by leveraging and orchestrating existing networking investments to further automate IT security processes.
2. CounterACT enables unlimited, automated real-time movement between the network and QVLANS as devices fall out of compliance and return into compliance, maximizing both security and the employee’s productivity without disrupting IT personnel. Policy is enforced without having prior knowledge of the device or requiring any form of client to reside on the endpoint.
3. CounterACT incorporates a simultaneous intrusion prevention system, customer proven to stop zero-day self-propagating malware and other network attacks. Since this most critical threat is addressed in real time at the point of connection, managed users without infection gain immediate access to the network while the device is interrogated for network security policy compliance. Compliant users are not affected by the CounterACT interrogation, keeping the NAC process transparent to the end user.
4. CounterACT’s measured/tailored enforcement minimizes disruption of network operations or the diminishing of employee productivity. Rather than having only on/off enforcement and thereby inappropriately blocking devices or network traffic for minor policy violations, CounterACT’s full-spectrum enforcement mechanisms offers the alternative of automatically guiding the user back into compliance while simply raising an alert or restricting access – but not eliminating access – as determined by the security posture of the company.

Hot Online

ForeScout Customer Case Stories:

Omnicom Achieves Global NAC Deployment

Omnicom Media Group, a global leader in advertising and marketing communications, selected ForeScout’s CounterACT network access control solution for its worldwide offices to ensure that all connecting devices comply with corporate security policies.

A primary product selection criterion was the ability to provide full access control and endpoint policy enforcement without the use of an agent on each endpoint.

Clientless NAC was rapidly deployed, ensuring global adherence of corporate security policies. Kenneth Corriveau, CIO, Omnicom Media Group, appreciates the simplicity of the clientless solution and said, “CounterACT interrogates every device that touches the network without disrupting business.”

Department of Interior Uses NAC to Control Unmanaged Contractor Devices

The US Department of the Interior (DOI) selected ForeScout’s CounterACT to detect infected machines and disconnect them from the network without the requirement of quarantine by default or the use of approved device list.

Immediately upon installation, CounterACT identified a contractor connecting to the network with a zero-day threat and blocked the user from damaging the network. Stu Mitchell, Enterprise Services Network System Manager of DOI, stated, “CounterACT repeatedly helps ensure that our network remains safe from noncompliant devices. ForeScout has become a trusted partner and continues to deliver innovative access control technology.”