

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

SQL INJECTION

http://www

CYBERWAR: DEFENDING A COUNTRY
PRACTICAL CLIENT SIDE ATTACKS
INTERVIEW WITH GORD BOYCE



Vol.7 No.01
Issue 01/2012(49) ISSN: 1733-7186

PLUS

TOOL TIME: SECURE YOUR DNS
(IL)LEGAL: WHY CAN'T ONLINE BANKING
BE LIKE FACEBOOK?

Interview With

Gord Boyce

CEO at ForeScout Technologies

by Aby Rao



Gord, your company survived the early NAC vendor shakeup and NAC is more mainstream with demand in the last couple of years accelerating. To what do you attribute the increased market demand?

The early *Network Access Control* (NAC) market did see a lot of consolidation and failures. Early vendors promised more than they delivered in terms of functionality and deployment ease. Many of those products required managing different components and replacing infrastructure, with results sometimes disrupting users from doing work. So the cost and impact was greater than the expected benefits. Network Access Control has definitely matured since then, but so have the reasons for why organizations are buying.

Enforcing authenticated access and facilitating guest networking are still common NAC drivers. But companies are now looking at ways to manage the risks of personal and mobile devices on their network – the IT consumerization issue is a challenge that is finding most customers playing catch up. Given increased network dynamics and connectivity, and the velocity of new attacks, companies are also seeking ways to converge endpoint, network and identity intelligence so that they can improve how quickly and efficiently teams can respond to security issues, if not prevent threats in the first place. NAC can support these initiatives.

What do you attribute your company's ability to take advantage of these NAC trends?

Early on, ForeScout was an *Intrusion Prevention Systems* (IPS) company who had developed some very innovative technologies that identified malicious network and application behavior to stop threats without relying on signatures. This product, CounterACT Edge, still prevents a good majority of today's zero day attacks and targeted threats – the product has a great following. But soon after, we entered the NAC market with our IPS heritage and evolved our CounterACT platform to meet various NAC customer requirements and environments, leveraging our IPS technology and networking expertise.

We incorporate network-based infrastructure discovery, traffic monitoring and endpoint fingerprinting teamed with a strong policy engine and flexible means to take actions. As a result, we have an agentless, non-disruptive and highly interoperable approach that really gives us a competitive advantage in our space. More importantly, CounterACT solves a variety of security problems and enables real business benefits for our customers. That said, I feel our biggest asset is the zeal at which our developers and employees work with customers to get things right and meet requirements.

What is CounterACT and what can organizations benefit from that platform?

CounterACT is our flagship product that, as an automated security control platform, serves four major security categories. Obviously, we are a leader in Network Access Control, but we also provide mobile security, endpoint compliance and threat prevention. When our appliance is placed in a corporate network, CounterACT enables real-time visibility and control capabilities for medium and large organizations.

Our customers are using CounterACT to apply uniform rules across their enterprise to limit or block access to network resources based on user, device, time and location attributes; to enable guest networking; to identify and classify known and unknown devices; to find and even fix endpoint security violations; and to stop malicious actions and attacks. And it does so working with our customers' existing infrastructure.

The value of automating these controls is bottom line cost savings and operational efficiency. For example, many of our customers start off with processes around access, endpoint compliance and guest networking. They can use 802.1x, non-802.1x or both as methods for controlling network access. They often first build out policies around required endpoint configuration and security client software. Policies can start in monitoring mode and then move to stronger enforcement – this way a set of policies can be phased in and exceptions can be managed proactively. The same is true for guest networking where our system provides the mechanisms to register and limit guest access.

Often we are brought in to address one or two critical problems or initiatives. Soon after, organizations see broader application and value. Many of our more progressive customers take advantage of our real-time monitoring, enforcement and remediation capabilities – essentially lowering helpdesk calls and more manual security incident response.

What are some of the advantages and disadvantages of automating solutions over an experienced security team supervising the function?

That's a great question, as companies aren't searching on Google for an automated security control platform – though they would find us. From a tactical viewpoint, they want to solve a security issue or meet compliance requisites. But our platform's capabilities does lend itself to allow network and security operations to do more. It's a powerful platform. There are some that shudder when they hear the words *security automation*. But organizations are already doing this – when they apply firewall rules, activate anti-virus, invoke encryption gateways or set VM zoning, for example.

It's not about putting a tool ahead of experienced security teams, but it is about how to optimize security

operations, which is a valued and expensive resource. It is also about coping with the sheer number and volume of threats that exceed human processing capacity. There are certain security scenarios that are black and white – you don't want the attack or violation to occur. So you are relying on your security team's experience to define policies in order to enable defenses to react faster and fix problems with little helpdesk and IT intervention where possible.

The disadvantages of automation could be working through policy exceptions, interfacing with different operations, tracking activity, and potential business disruption – but these are manageable. It is a matter of building out the controls and responses. What is not simple is being able to actually extend more dynamic and granular controls across the entire enterprise. For what we provide, our platform approach is proven and I believe there is more that ForeScout can offer.

The advantage, by operationalizing security, is risk reduction and increased savings. In some respects, CounterACT offers job enrichment because we free up the experienced security team to focus on more interesting initiatives, processes and issues.

With Bring Your Own Device (BYOD) commonplace in various organizations, what are some of the major security threats that are introduced to the work culture and how can organizations respond?

BYOD and mobile security are two huge issues that our clients and prospects are working on. Organizations need to embrace the fact that their employees are using personal mobile devices at work – these devices are already on the corporate network, possibly taking advantage of existing credentials. Companies want to realize productivity and connectivity gains of such devices but not at the expense of security. The threats right now are less about mobile malware (although there is certainly potential), but more about data leakage, phishing and privacy.

Organizations need to assess technologies that will allow them to segregate personal from corporate information and network access – but that's more likely for corporate-managed devices. On unmanaged devices, companies need to be able to identify these smartphones, netbooks and tablets, and have a roles-based, non-intrusive way to enable appropriate access to either the Internet or specific network resources. ForeScout offers many of these capabilities today where we can enforce policy for managed and unmanaged, wired and wireless devices, as well as monitoring for post connect threats. With regards to BYOD and securing personal devices, this has to be handled in a manner that is legal and acceptable to end users.

Since ForeScout is a global company, what are some of the regulatory and compliance laws that you have to deal with outside USA?

Our customers know that any product by itself does not let an organization be compliant, but, instead, it is the combination of policies, processes and technologies which help support meeting privacy and other compliance mandates. For example, one of our customers was looking at how to assure wireless network scanning and elimination of rogue wireless access points across multiple sites to support PCI. Another customer wanted to add a layer of protection to segregate and monitor user access to cardholder data. We were able to quickly support these requirements with controls and reports. These customers were able to use our built-in policies and implement enforcement with no change to their environment; even if the network between multiple sites is different.

Other regulatory requirements can involve how ForeScout complies to security standards. For example, our appliance needed to be FIPS certified to support many financial institutions. On the government side, CounterACT recently achieved Common Criteria EAL 4+ status, the highest level for a NAC solution, which was required by ForeScout to support government and military installations seeking to satisfy a variety of endpoint and access control mandates.

As a CEO, what kind of questions do you face when you interact with new clients? What are some of the top areas they need help with?

When I meet customers, it is often with more senior IT and security executives, and not always the staff actually operating our product. Senior IT members are more involved with establishing a more strategic dialogue beyond what might be the specific project. They inquire about our support, corporate stability, futures and how to design policies to enable proactive defenses. Discussions seem to be more about operations rather than just compliance. The majority of clients are extremely focused on lowering costs and managing risk so they ask about product usability and how well you will be able to support new devices, or ways to manage new types of threats. We have gained a great deal of product insight by listening to our customers.

So as a pure-play NAC vendor, how do you contend with larger vendors that offer broader suites of product?

NAC products must be usable out of the box, easily managed, flexible to meet different security scenarios, and scalable – not all are. To be competitive, our products must be highly extensible, have a lower overall cost of ownership, and offer more assured

implementation versus that of larger incumbents. As a pure-play vendor, you are also forced to support a broader range of infrastructure products and to be vendor agnostic.

We have to fully leverage our customer's existing network, security and process investments. Every customer has at least something with a vendor that we compete with. As you can imagine, while we compete with Cisco and Juniper for NAC, we need to support their network and security devices so our deployment is seamless.

When you're a broad-based vendor, you typically focus on roadmaps that support selling more product and assume a more homogenous customer environment. You also have significant legacy product support that can affect the speed at which you can deliver new and customer-requested features. We've gained decent industry visibility, but we are not yet a household name in the data center. However, when prospects compare us to the larger vendors in terms of architecture, technical merit and our means to be responsive, and to support a customer's evolving requirements – we compete quite effectively.

You mention infrastructure interoperability. In terms of the security eco-system, what are the more interesting industry partnerships that provide customer's more value than either product alone?

I have two answers. First, is how we can protect a customer's security investments. CounterACT identifies and assesses devices in real-time and we support the majority of popular endpoint protection products such as anti-virus. We have found that as much as 30% of client security tools have conflicts, are out-of-date, removed or deactivated – and incorrectly reported. We have the means to fix many of these issues as background processes.

More recently, we have been extending the value of CounterACT by integrating with other vendors' offerings, such as helpdesk, systems management and security management. Our product supports the SIEM (*Security Information Event Management*) and *Common Event Format* (CEF), for example. We can send our security event data to products such as HP ArcSight and Nitro Security (now McAfee). With ArcSight, we offer added capabilities where we can send real-time endpoint configuration details to ArcSight. ArcSight can also use their correlation engine to send commands to ForeScout CounterACT to take action such as to block an attacker, quarantine malicious systems or re-activate a security agent. We anticipate opening up our platform to enable other products to obtain CounterACT's real-time visibility and control functions.

Does ForeScout offer any solutions in the virtualization and Cloud computing space?

Our family of appliances is also available as virtual appliances. You might think that as soon as we announced the availability of a virtual appliance that it would immediately outsell physical appliances. There certainly are datacenter consolidation advantages, but at the same time, many IT organizations remain more comfortable with the plug-and-play physical appliance.

Both our physical and virtual models are identical and even our management appliance can support a mixed physical and virtual environment. Our virtual appliance models offer more deployment flexibility since customers can more readily obtain and provision VM images and licenses using their own hardware. And we offer the means for virtual appliance licenses to be upgraded, which you can't do with a fixed physical model.

More recently, we announced packaging of our virtual appliances to support cloud computing in terms of a NAC as a Service platform. We needed to satisfy customers seeking to offset capital expenditures and outsource security expertise. If you take a look at our platform being integrated, interoperable, vendor agnostic, non-disruptive, scalable – and virtual – that really offers a service provider a solid means to deliver NAC as a hosted or managed service. We had received quite a few inquiries to support managed service providers and actually had a few large accounts in North America already using CounterACT through a managed service delivered by a few partners.

We had a proven implementation, but we really didn't fully package NAC for the services market. We now offer our authorized service provider partners a subscription license and the means to quickly adjust licenses to better serve their clients. This provides for rapid deployment, monthly billing, on-demand scaling and marketing support for our partners to offer our solution as a hosted or managed service for customers that want a service option.

Having started in sales, then moving into a chief operating officer position – and ultimately a CEO position – for our entrepreneurial readers who want to take the helm of their own security business, what advice would you offer them in this economy?

Be sure you have a solution that provides demonstrable results in terms of not only risk reduction, but also operational savings. In a tough economy, people buy aspirin, and hold off on vitamins. As a start up, outstanding support is as equally important as outstanding product. Ultimately, you want to forge a relationship with every strategic customer and partner so you can learn how to improve your product or

service, understand where the market is heading, and gain referrals to grow your business in conjunction with conventional selling and marketing.

ForeScout has made visible strides in the Network Access Control space. Tell us a little about what the future holds for ForeScout?

It is exciting times for ForeScout and we are growing. We are very mindful to continue to invest in our platform to assure our customers, partners and prospects that they will continue to receive best-in-class functionality, support and services. Beyond NAC, which is core to our business, we also have identified ways to bring our value to mobile and cloud environments. Our platform closes operational gaps by bridging what are often blind or silo'd management areas that affect security. We see an opportunity to empower security operations to gain visibility and control over what is surely an extended, borderless network for both managed and unmanaged devices with greater user, network, security posture and application context.

About ForeScout Technologies, Inc.

ForeScout enables its customers to unleash the full power of their network through enterprise-class security and control. ForeScout's automated solutions for network access control, mobile security, threat prevention and endpoint compliance empower organizations to gain access agility while preempting risks and eliminating remediation costs. Because security solutions are easy to deploy, unobtrusive, intelligent and scalable, they have been chosen by more than 1,000 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. Headquartered in Cupertino, California, ForeScout delivers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com.

