



---

**WhatWorks in  
Blocking Network-based Attacks  
with ForeScout's CounterACT**

**Automating Network Access, Endpoint Compliance and Threat Management Controls**

**WhatWorks is a user-to-user program in which security managers who have implemented effective internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know more about? Let us know. [www.sans.org/whatworks](http://www.sans.org/whatworks)**

## **About SIRVA, Inc.**

SIRVA, Inc is a leading worldwide provider of relocation and moving solutions, providing more than 230,000 relocations per year to corporations, government employees, and individual consumers. SIRVA delivers the best mobility experience at the lowest total cost to relocate. Brands include Allied, Allied International, Allied Pickfords, Allied Special Products, DJK Residential, Global, northAmerican, northAmerican International, SIRVA Mortgage, SIRVA Relocation, SIRVA Move Management, SIRVA Global Relocation, Inc. and SIRVA Settlement.

## **About Waqas Akkawi**

Waqas Akkawi is director of information security at SIRVA Inc. He is responsible for SIRVA's global information security program and operations across US, Canada, Europe, Asia and Australia. His is ISACA CISM and ITIL certified.

## **SANS Summary**

SIRVA's director of information security needed a tool that would profile and monitor regular and guest users' behavior and, if necessary, block access to his network. They also wanted to advance their intrusion prevent capabilities to reduce zero-day and targeted attacks. The Network Access Control (NAC) and intrusion prevention systems he found to protect the company's network and sensitive data is easily monitored, implements policies effectively and made his security operations even more efficient.

~~~~~

## **Interview**

### **Q. Tell us a bit about the role you play at SIRVA.**

**A.** I am the director of information security for SIRVA and have expanded responsibilities at headquarters based in Illinois as well as a global reach across sites in the USA, Europe, Canada, Asia and Australia. My team supports our security programs and operations. We have a major datacenter and test environment.

I've been here for five years. When I first came in, the organization was growing which lead to the need for change in our IT governance. We had an outsource initiative back then, which is not the case today. With the nature of our business, we are collecting sensitive information so the highest level of information security is critical and has always been first priority.

### **Q. Why did NAC and IPS problems come to the top of your list of priorities? You've got a lot of things you can do.**

**A.** Our security priority is to ensure the utmost data security for our employees and customers. Therefore we are constantly working to enhance our intrusion protection systems, access controls and endpoint compliance to ensure we maintain industry-leading systems.

We were looking for a system that enabled detection and prevention of global intrusion and one that would do so successfully with modest on-going administration/tuning. Secondly, we wanted to enhance our support of federal and state information and privacy security compliance laws such as Massachusetts CMR 201 (Standards for the Protection of Personal Information). And since SIRVA's security requirements are based on protecting the personal identifiable information of our clients, ensuring we continue to maintain industry-leading network defense is always a goal.

*\*To hear this user expand on his answers, view his presentation slides, and listen to his answers to many more detailed questions asked by other users from around the world, go to <http://www.sans.org/webcasts/archive.php>*

Lastly, we needed to continue to ensure that our computing environment was aligned and successfully secured with our configuration policies; thereby reducing malicious malware. We have consultants, guests, and trusted computers who access and navigate through our network every day, each with the potential to introduce worms and viruses. In order to monitor and respond to all the various types of users, devices and security settings, we needed to explore applying more automated defenses.

The ForeScout CounterAct system enabled us to do all of this, and provided us with a best-in-class mode of information security which involved minimal human overhead. With CounterAct, we can proactively investigate suspicious items and can ensure that the right people and systems are configured properly and have access to the right information.

**“ForeScout has a solid product that was effective as a standalone IPS and even incorporates IPS capabilities into a complete NAC solution.”**

**Q. What was the process you undertook to find a satisfactory solution? What executive members and teams were involved?**

**A.** First, we needed management buy-in. Once we had that, we conducted a technical and business assessment, involving key members of IT. From the CIO down to the network engineering analysts--we put together a small team that was to evaluate the effectiveness of the intrusion prevention system options and make the decision. We went online to examine products in both network intrusion detection and subsequently network access control. We narrowed down a short list, did a preliminary comparison, and invited vendors in to conduct a deeper technical assessment.

**Q. What criteria, both technical and operational considerations, did you use to evaluate the candidates? How did you evaluate them?**

**A.** We first looked to advance intrusion detection capabilities. The top technical criteria was that we needed IPS not IDS. Many IPS vendors have similar features since the products are mature. So we looked at new approaches and also considered the operational impact on our organization. IPS solutions are known to have false positives and require tuning. We honed in on those products that seemed to have a more definitive approach in order to stop intrusions and worms--and those that required less administrative effort to maintain without a sacrifice in quality. We also prefer appliances, as they are more turnkey in terms of deployment. These criteria helped in determining the candidates and picking the most effective solution.

Subsequently, we compiled requirements for network access control. In conjunction with our operational users, we defined a list of policies concerning network access based on types of users, the devices utilized and how these devices should be configured with security settings (such as different anti-virus, firewall and VPN client security applications). Based on that effort, we could assess the different NAC products' level of ability in various areas, such as: identifying devices and users, authenticating access and responding to policy violations.

Unlike IPS, we did see a variety of capabilities and differences with how NAC functionality is delivered. Some required a variety of components and network infrastructure changes, which we felt would add costs to deploy and maintain. A few focused on 802.1x for authenticated network access. We felt that solely relying on 802.1x could present agent management issues and potential issues with non-managed devices from guests and contractors. This could also

present potential disruptions for those network and endpoint devices that do not support 802.1x, which would require considerable exception management--impacting operations.

Three other key areas were ease of use, how the product can scale and price. Next was deployment and interoperability--support for our current infrastructure and how it can support future changes and broader deployment. Price is negotiated once the other criteria have been proved.

For evaluation, we opted for a proof-of-concept to assess the architecture as well as a lab environment to review the processes for set up, configuration, basic functions and administration.

**Q. I didn't understand the connection with the network access control issue, particularly when it doesn't have an agent associated with it. Can you kind of help me with that one?**

**A.** Definitely. We wanted to advance our network access control and continue to defend against network attacks with the goal of furthering the level of our security. ForeScout's CounterAct product offers both a NAC Network Access Control solution and they have an IPS solution.

Other vendors back then either had an IPS or NAC--few had both and usually the NAC does not work with the IPS--they are separate. For NAC, many required agents for each device in order to assess if the device and user can connect to the network. This would be required if we went only with the 802.1x NAC way. ForeScout did not require an agent or use of 802.1x.

**“The biggest payoff is our ability to give customers enhanced assurance that their data will remain secure.”**

With ForeScout, we could manage devices that do not support 802.1x and we could do NAC without an agent. What that means is that we will assess any device that comes into the environment and will look at who the user is or how the device is configured and whether it matches any of the

security policies we have. We're going to assess it to find out if it has up to date antivirus, an active firewall, up to date Windows patches, etc. If it is an unknown user or device, or one that is not on our guest list, or if they are not compliant with our requirements--we can restrict access and investigate. Some of the intrusion monitoring mechanisms are also built into their NAC to monitor devices once they are already on the network. So once they are on the network, the device is automatically monitored for malicious behavior.

Our goal was to further scale and grow our policies and defenses for superior data protection.

**Q. What tests led you to decide some of the candidates were not going to be acceptable?**

**A.** On the IPS side, we looked at how they responded to certain types of attacks and security threats such as worms. And also how much configuration and fine-tuning would be necessary. Of the vendors we tested, a few relied heavily on threat signatures and we experienced false positives. When this occurred, we were required to review the IPS/IDS logs manually and conduct further research in order to verify valid intrusion, which was very time consuming. And we would need to rely on new signatures to keep up with threats. We felt a behavior-based approach, like ForeScout's, would satisfy our requirements.

NAC product selection was more involved since it adds another layer of security to all devices and users accessing network resources. To apply policy and respond to issues, vendors would need to show how well they integrated into our existing environment. And the vendor had to

demonstrate how flexible the products were in supporting different policies and processes, such as guest management. For example, we wanted to see how the products addressed guest networking--and users who have devices that we don't manage such as the iPad and other smartphones. We needed to understand how well the products supported different devices and our network infrastructure and how easily policies could be built and enforced.

In terms of implementation, we preferred to limit the use of agents--which can be troublesome to manage. To receive all the NAC functionality, many required separate components for authentication, pre-admission security checking and remediation. This would add costs and be cumbersome to maintain. We felt that pure 802.1x authentication products would be too onerous and take too much time and effort to implement.

As we went through some of the candidates feature-set, we began to see the value in a more integrated product, which provides greater operational visibility and comprehensive results proving access control.

**Q. Which one did you pick and why? Which of the various criteria did the product you selected excel at? (what advantages did it have over alternatives)**

**A.** We selected ForeScout's CounterACT system. The product well satisfied the advance intrusion detection capabilities we required and addressed our network access control criteria and requirements. It also met our key criteria--ease of use, integrated features, interoperability and an appliance architecture that scales.

ForeScout has a solid product that was effective as a standalone IPS and even incorporates IPS capabilities into a complete NAC solution. ForeScout has an intrusion detection method to identify advanced persistent threats including worms and "low and slow" attacks based on a behavior model. Once a device performs certain unusual activity, such as scanning or using a port in an atypical way, the system sends fake results called markers that are maintained by CounterACT. So if the marker or set of markers is used again, we know the attack is valid, enabling us to isolate the attacker or attacked device.

Not only that but the solution is easy to deploy and manage. The NAC product does not require agents. The interface appears to be well thought out. And, it has a broad feature-set which would support different policies and uses. Once you set up the policies, the solution blocks attacks, enforces access policy and remediates systems--summarizing all activity into an alert or in a report for analysis.

**Q. How long did it take to initially deploy and what was involved? How many endpoint/devices are being monitoring and how is the product being used?**

**A.** We have over 6,500 endpoints being monitored by CounterAct--and that number is expected to grow. The initial deployment went through the design and architecture phase. We tested deployment, configuration, network infrastructure and directory service integration, plug-ins, policy settings, upgrades and managing multiple appliances in a reasonable test environment. We did this to ensure that the solution implementation phase would be successful. We currently have our headquarters online and plan to extend to 5 sites within the next few months. It took about 8 weeks to complete the first phase (integration, policies, exceptions), but now we expect

**“CounterACT blocks attacks, enforces access policy and remediates systems--summarizing all activity into an alert or in a report for analysis.”**

only a day or two for each additional location. The next NAC project is to start applying policy to VPN users.

The key is visibility first, then control. Since ForeScout CounterACT does not initially block unknown or unmanaged devices or guests, we have an understanding of our environment before applying or enforcing different policies--and know the impact of those policies ahead of time.

The CounterACT product enables a high level of device intelligence as we can view all the devices connected to a given network--this is based on built-in device classifications. This covers a variety of network endpoints and their configurations including MAC, IP, OSs such as Windows, Linux and Mac, ports and applications, and even VMs and mobile devices. They use a network-based approach that does not utilize agents. Once the device is discovered, it is automatically placed into the appropriate device category.

For unknown devices, we can use any of the discovered attributes, such as ports, MAC, registry settings, to create a new device type--from VOIP phones to badge readers. This gives us tremendous real-time visibility. At any point in time we know where a device is on the network, and who is associated with it. Based on this, we know which devices are not managed by corporate or are outside of required security settings.

The CounterACT Edge product is not an inline appliance and the IPS deployment is similar to the former IPS product we used. However, since it is behavior based, we have fewer exceptions to manage and no signatures to update.

**Q. How do you know its working?**

**A.** What's great about these products, both NAC and IPS, is that they have a very easy dashboard and interface, as well as centralized management. With NAC, we see everything on our network, and so we know that all devices are being monitored for potential threats before and after network access. Not only do we get notification of access violations and suspicious activity, but also a visual of what's being monitored, device configuration or security issues and what's being fixed or blocked in real-time. We have caught machines that have infection and low and slow attacks, so we know it works.

**Q. What NAC policies are being applied and enforced?**

**A.** The policies we have implemented concern guest management, which enforces security controls for guest and contractors before they can access our network. A few of the protections we currently have in place are: the ability to identify and block rogue IPs. Assuring specific endpoint compliance such as security settings for anti-virus, firewall and windows updates. With CounterACT we are able to cover our endpoint control scenarios; specifying device, IP, MAC address, user, time, registry settings and any other combination of discovered attributes as a basis to create a rule. The rule sets the condition logic and the response can vary from reporting and notification, notifying the end user or help desk, hijacking HTTP sessions to enable registration, segregating access via VLANS, to remediating a variety of security application issues.

**“CounterACT is easy to deploy and manage.”**

**Q. What type of rollout was involved? Were there any additional implementation considerations?**

**A.** We are conducting a site-by-site rollout. Since the product works within our current environment, after the initial design and architecture phase, it has been a straightforward implementation. We have implemented the IPS at various network ingress points.

For NAC, we needed to determine where it made sense to deploy architecturally in terms of access, distribution or core network layers depending on the discovery and response functionality that we needed. Since CounterACT does discovery before enforcement, it does not impact operations. The users don't know it's present and we can rollout out policies with different enforcement strength as needed. This results in easier exception management.

**Q. What more advanced features have you implemented?**

**A.** We started with the standalone IPS product called CounterACT Edge. For NAC, we have implemented a lot of the core functionality from CounterACT such as guest management, endpoint compliance for anti-virus, firewall and other basic security settings. And we will eventually use NAC policies for our VPN users.

One built-in feature that we utilize heavily is the device monitoring which begins once a system is allowed onto network. This is identifying and stopping devices that perform unusual activity. For example, one well-known security risk occurs when an attacker spoofs a printer connected to the network. CounterACT can pick up this change and block the threat.

**“We have become more proactive, with a complete situational awareness.”**

Implementing the built-in mobile security capability is next on our list. We are continuously working to ensure our data security process remains world class.

**Q. What changes to processes, the organization or infrastructure were necessary to achieve results?**

**A.** Changes to the infrastructure were very modest and consisted of minor configuration or access credential changes. As far as processes, the NOC needed to learn how to monitor and respond as level one support. The Network Engineering, Security, and desktop teams serve as the second and third level of support. It was essential that we informed the support group about policy changes in advance, so end user calls and issues were not a surprise. With enforcement, the notification and reports are sent to the appropriate departments and helpdesk so details are in hand and exceptions can be easily accommodated for.

One of the advantages of the NAC implementation was having the perfect opportunity to revisit and refine network access control and endpoint compliance policies. In addition, the tool provides us with a more uniform method of enforcing our security policies.

**Q. How has the product supported your programs/controls/ policies with regards to: network access, guest access, endpoint compliance or mobile security requirement?**

**A.** We now have an even more comprehensive understanding of each host attached to our network and a real-time view of our environment. This provides us with a complete view into the standardization of hosts, potential vulnerabilities, and compliance issues. It also gives use the means to push out policies proactively to protect our environment.

**Q. After its use, how have any policies or procedures changed? How have your automated security processes and controls evolved?**

**A.** We have become more proactive, with a complete situational awareness. We can receive alerts, reports, threat levels or policy violations within the environment immediately. Furthermore, the automation of policies for guest access, security settings and mobile security means that we can better fortify our defenses and security compliance requirements; resulting in a higher level of productivity for my team and most important--data security for our valued customers.

**Q. What do you believe is the best approach to deploy, maintain and maximize your investment in the product?**

**A.** Plan ahead. Know the policies and risks that you need to address. Look at your operating environment and architecture to understand what is required in order for the product to meet your requirements. Centralized management is a must. Design and architecture according to specific environments is critical too. You need to consider where to place the appliances depending on the level of visibility and control desired. Do a proof-of-concept if possible. Deploy and enforce in phases. Test policy before enforcing policy. That way you need few resources to manage/support the product without sacrificing quality.

**“The CounterACT tool provides us with a more uniform method of enforcing our security policies.”**

**Q. How do you know your use of the NAC solution leads to better security or risk management? How do you / did you measure success with regards to the results achieved by the use of this product? Have you realized any savings in time, costs or resources?**

**A.** Since we control which users and hosts can join our network, the enforced conditions for access network resources and sensitive data, and the compliance information we get--the results we receive are very positive--and we are able to maintain the superior quality of our system with fewer resources and decreased spend.

**Q. Where does this product fit as part of your security program and in relationship to other security product investments?**

**A.** Both NAC and IPS are at the core of our security program, and ForeScout serves as a significant product for us.

**Q. How would you characterize the product support and respective professional services?**

**A.** The product is straightforward to install and operate once you invest reasonable time and effort. We have received continued support from the vendor as well.

**Q. What perceptions did you have going into the project that were incorrect or correct as you now look back with your results? Is there other functionality that you would like to see in this product?**

**A.** Because we were prepared, 90% of our perceptions were correct. In terms of other functionality, ForeScout is very receptive to our suggestions. Currently, we have the necessary functionality--however our needs continue to evolve.

**Q. What lessons did you learn that you think might be helpful to others?**

**A.** Planning. Having a design and architecture phase. Evaluating policies. Centralized monitoring. Involving operations and the help desk is a must. Take the time to do due diligence during the design and architecture phase...the result is a more seamless implementation.

**Q. How do you feel about the product overall, pros and cons?**

**A.** We have been very satisfied with the outcome thus far. It's uncomplicated to configure out of the box. And it takes approximately one hour per device to put it online, and once it's working, it's efficient to manage. The end results are very satisfying--when we put a policy in place, we are confident that it's implemented.

Ultimately, the biggest payoff is our ability to give customers enhanced assurance that their data will remain secure. At SIRVA, we believe it is our responsibility to ensure customer data is protected at all times--and we have made this possible.

**SANS Bottom Line on ForeScout CounterACT and CounterACT Edge at SIRVA:**

1. Helps ensure customers' data is secure at all times and contributes to industry-leading network defense;
2. NAC provides end to end visibility and flexible policy enforcement;
3. Integrates well in diverse networks – very easy to install, use and maintain;
4. Manages guest access and defends the networks from external attack and threats; and
5. Assures that anything and anyone connecting to the network meets security policies.

**“We have been very satisfied with the outcome. The results we receive are very positive and we are able to maintain the superior quality of our system with fewer resources and decreased spend.”**



**For more information on ForeScout CounterACT and CounterACT Edge:**

**Visit: <http://www.forescout.com>**

**E-mail: [info@forescout.com](mailto:info@forescout.com)**

**Phone Toll Free: 866-377-8771**