Reaping the Benefits of Continuous Monitoring and Mitigation at Pioneer Investments

with

ForeScout

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

About Pioneer Investments
Pioneer Investments is a global investment manager, founded in 1928, dedicated to growing and preserving client assets. We offer a diverse range of products across both traditional and non-traditional asset classes, managed by our global investment centers in Boston, Dublin, London and our local investments center across the regions. Today, Pioneer Investments has a presence in 27 countries worldwide and an experienced team of more than 2,060 employees globally, of which nearly 350 are investment professionals.

About the User
Ken Pfeil is the CISO at Pioneer Investments responsible for global security operations and compliance. He is a seasoned CSO and IT veteran with experience spanning over two decades with companies such as Microsoft, Dell, Avaya, Identix, and Merrill Lynch. In 1998, he founded "The NT Toolbox" and oversaw all operations until its acquisition by GFI Software in 2002. He served as a technical contributor and subject matter expert for CompTIA's Security+ certification, ISSA's International Privacy Advisory Board covering GLBA, and Microsoft's MCSE Exam and course curriculum "Designing Security for Windows 2000". He also contributed vulnerability analysis content at Windows and .Net Magazine's "Security Administrator" publication. He is the coauthor of the books "Hack Proofing Your Network - 2nd Edition", "Stealing the Network - How to Own the Box", and a contributing author of "Security Planning and Disaster Recovery" ,"Network Security - The Complete Reference" and "Network Security Assessment: From Vulnerability to Patch" and Microsoft's "Best Practices for Enterprise Security" whitepaper series.

SANS Summary
A forward thinking security team responsible for operations and compliance was searching for a network security solution that would provide intelligence across users, devices and applications, enforce granular policy control, and enable control interoperability. The network security solution they implemented from ForeScout allowed them to gain visibility and apply specific policies at both the client and network levels, enhance control integration among different tools, and reduce costs by saving man hours in terms of issue prevention, awareness and response. They were able to demonstrate an immediate return on investment. "Phenomenal" interoperability and technical support was an added bonus.

~~~~~~

Interview

Q: Tell us a little about you and the role you play at Pioneer Investments organization and within your parent company.
A: I'm Chief Information Security Officer at Pioneer Investments where I oversee global security operations, and respective technical architecture and technology, policies, compliance and staff . We have 31 offices operating in 27 countries with roughly 2,100 employees spread out geographically. We are a wholly owned subsidiary of the UniCredit Group and I've been with Pioneer for four years now.

Q: Do you report to the CIO?
A: I report to the CTO. It's a little bit different in finance. The title CIO is usually reserved for Chief Investment Officer. So my boss is the head of technology or Chief Technology Officer.
~~~~~~

Q: What was the problem? What started you looking for a solution and ending up with the ForeScout product?
A: Like other organizations, you can't manage what you are blind to – and that presents risk. I was considering solutions for network and host visibility and the means to extend policy and technical controls with regard to how to better manage users, devices and applications on our network – preadmission and post admission. Network Access Control (NAC) was a core technology to enable this visibility and control.

"Now we can better monitor and enforce policies before and after network admission, and we have the capability to instantly send warnings, isolate, limit or move systems to appropriate resources, or directly remediate the endpoint or trigger another system to take action."

Prior to Pioneer, I was vetting NAC vendors and looking at potential solutions in late 2008 – a lot really has changed in the space, but some things haven't. Our need for preadmission and post admission compliance (non-intrusiveness, agentless installs, etc.) still exists. At Pioneer, we started to look at next-generation NAC technology again a couple years ago. We were primarily interested in approaches that had more useful integration aspects and flexibility towards being able to apply specific policies, either at the client or at the network level based on certain conditions – interoperability and extensibility was paramount.

Q: What was your preconceived expectations/notions about next-gen NAC and how did that change?
A: The basic expectations of NAC technology is authentication and configuration compliance before admission – which can be operationally challenging and disruptive. Next-gen NAC offers more flexible implementation, offers greater visibility, and also control interoperability. It's matured to provide even more value. While some folks are just using NAC for basic access control, the "new" NAC serves to provide an approach for security intelligence and response.

Q: In 2008, you were mostly looking for a check for configuration and compliance upon connection and making some decisions on allowing connection or not. Now now you're looking for the ability to do some more granular policy control?
A: Exactly. NAC was a fairly immature technology in 2008. We wanted to simplify switch port management and we didn't want anyone walking into the office and having a hot connection to our network. In 2008, preadmission control was a fundamental aspect of NAC, but the value we were seeking for our organization had changed – we looked for broader application in 2012. ForeScout CounterACT, as a network security platform in particular, has excellent visibility, some pretty granular control and more flexible implementation capabilities for both wired and wireless network. I can't really call it a NAC anymore since it's so much more than just access and checking configurations. It is serving as a control integration and endpoint remediation solution.

Q: How did you convince management to fund this? Was this driven by compliance, threats, operational improvement… All the above?
A: It was pretty much all of the above. We need to be in compliance with certain things. For example, I can't solely rely on host-based security because endpoint and threats change. It is not a static world, so we need more oversight. Like others, I don't have unlimited resources. I put forth the solution and an architectural vision of how things could be improved and expressed the potential operational savings. I was able to show how this would support compliance, allow us to be ahead of the threat curve, and improve our operational bottom line. Management was very supportive of the investment.

Q: Was there any other triggering event?
A: There was no triggering event. It was about a better way to monitor things and use our resources more effectively. The integration aspects of ForeScout are definitely a timesaver because now I don't have to micromanage ten different security products to achieve the same effect. In some respects, the interoperability and rules engine allows us to use ForeScout's product across more applications. Saving time was absolutely paramount, but also supporting regulatory objectives helped, as well as being able to show some sort of a return on investment. In terms of the operational cost aspect versus the capital cost aspect, the ROI was pretty evident from the beginning.

"In terms of the operational cost aspect versus the capital cost aspect, the ROI was pretty evident from the beginning. "

Q: It sounds like you used operational and cost-reduction benefits to justify the purchase. Did I get that right?
A: Yes. In this space, we're always trying to be forward thinking rather than behind the curve; when you get behind the curve it costs ten times more then trying to stay on top of things. Whatever technology we use, we need to be able to get visible value out of it. When you can explain to management how a product can enhance the use of other products and our responsiveness, it becomes a much easier to justify - especially when you can knock out some initial initiatives and then show how a product can be repurposed for other applications.

Q: Can you walk us through the process? Did you take competitive bids or did you look at different solutions and compare them? How did you go about it?
A: In 2013, we not only looked at control objectives both from preadmission and post admission standpoints, but more so from an architectural impact. How could we apply this technology to different projects and policies, and what would be the impact of doing so. One of the things that definitely stood out from ForeScout was its ability to sit out of band and easily capture both managed and unknown devices. Every other product vendor needed an in-line tap, agent or something similar to work. They did not offer very extensive endpoint details – unless the device was pristinely managed. They did not offer same level of preadmission or post admission enforcement. Most required us to change our wired network configuration, and would force big upgrades… we believe they would be administratively heavy to roll out and maintain.

We evaluated three or four different vendors, ForeScout included. We approached this from the perspective of having examined this technology in the past and looking to see

what changed. Other vendors we looked at included Cisco, Bradford and someone else that didn't even make the first cut. Once the technology side was considered, we also looked at things from the perspective of “launchability” in the business, stability of the company, etc. Obviously, we looked at price as well as operating cost.

Q: Did you do any test bedding or prototyping of solutions or was it a feature and architecture kind of analysis?
A: It was more of a architecture kind of analysis and a reasonable amount of actual product analysis - and it really took way too long. When you find the right product, there's really not a whole lot of sense in beating around the bush and evaluating 20 other solutions. That being said, look hard at the functionality, how it works with what you have and implementation impact, as that’s where the rubber meets the road. As we know, many vendors claim similar features. Of course, reading up, asking questions and talking to references in part of the process.

Q: Walk us through getting the new ForeScout capability installed and what products you were using.
A: In the first couple of weeks we had it rolled out globally. With ForeScout, we did not have to take a piecemeal deployment because it was not inline, had agentless options, and worked with our wired and wireless implementation. At first, we set up standard policies in monitor-only mode and were doing logging and informational analysis. We weren't doing any blocking on policy at that point, but we were using it to inform us. Literally, we were up in a couple of weeks at our main site and got fantastic intelligence. That alone was worth the cost as our team was better informed to make decisions.

“One of the things that definitely stood out from ForeScout was its ability to sit out of band and easily capture both managed and unknown devices. Every other product vendor needed an in-line tap, agent or something similar to work...we believe they would be administratively heavy to roll out and maintain.”

The product allows our team to see an issue and take action on demand or within the policy. We then stepped up policy enforcement and endpoint remediation such as port blocking, updates and things of that nature. About 10 months ago we began working on broader integration with all of our security products and it's going very, very well. I'm quite happy with the policies and the compliance that we've been able to achieve and we've got an even better roadmap going forward with the integrations for other systems like Bromium.

Q: What did it take planning-wise to successfully get through the initial rollout?
A: First, we had to evaluate our architecture, and there were a few things that were in consideration, like potentially needing to upgrade much older switches at some of the smaller sites to make them more manageable. And we did a capacity planning check so we could purchase the right number of appliances to see everything on our network. ForeScout is centrally managed and deployment did not require an appliance at every switch. We assessed what capabilities we needed in terms of visibility and enforcement

and deployed accordingly. We have the CounterACT manager appliance to centralize administration and roll up visibility from all the appliances.

Q: Roughly how many appliances did it take to cover your network and what did it take to get those appliances installed – is that something the local IT people could install?
A: We've got five appliances right now of various sizes and one management appliance. Some are physical and some virtual as we sent a virtual appliance to our Asia facility. Once we did some initial legwork at the main site, that was pretty much it: We ship it to the location where local IT racks it, stacks it and gives it an IP address. Then we remotely configure it. You need to set the interface to things like a switch mirror or span port, Firewall, VPN and other systems… pretty basic networking stuff. To install, you are not changing settings on those devices, just enabling them to talk – since you are not stepping on another's turf, that is a political win. Once configured, ForeScout CounterACT can then be managed centrally with standard policies from our main site. The GUI is very well done and easy for folks to use. It also has a web portal so IT staff, like the help desk, can do queries on users, devices and security questions. All authorized staff can use it based on role restrictions. The appliances run with corporate policies, but more policies can be run by the regional admin at the regional level too.

Q: How long did it take to implement it? And how long did it take to realize value?
A: II took a couple of weeks to install at our main site and to expand the policy set. This was more about approvals and getting the connection details than actually configuring. At that point, we realized much value in just operational visibility. It took a couple months to fully rollout. We have spent the last few months expanding the implementation and initiating stronger controls. The ForeScout product has a lot of built-in templates and integrations. It is a simple matter of using and customizing the templates. For integration, we could download plug-ins from their website and install them on the system. This would be for things like anti-virus, Windows patching, etc. The same is true for more advanced integrations, like integrating with advanced threat detection. Again, it is very easy to get up and running as the plug-in adds template properties for rules and reports.

"Tech support has been absolutely phenomenal. Very responsive."

Q: What's the staffing load to run your deployment of ForeScout?
A: Once you get it set up and get the policies configured, it's just a matter of maintenance. The majority of the policies are already built as templates within CounterACT, which just needs to be applied and adjusted. Initial policies are to identify devices, systems and applications, and can be adjusted for less popular and custom ones. The other policies cover everything from guest management and rogue devices, to anti-virus, and so on. Once you set and test in monitor only mode, you can adjust and make exceptions before broader roll out. Once policies are set, it is more about responding to very critical alerts or dealing with exceptions. For our enterprise, based on the level of alerts that are generated, it doesn't even require one full-time staff member.

Q: One of the problems people used to run into with NAC-based technology were non-user, non-8021X type login devices. Have you found that to be a problem?
A: Not really. ForeScout operates in a way that supports managed and unmanaged devices without requiring 802.1X. We can handle non-802.1X devices, BYOD devices and rogue devices pretty easily. We found post-connect assessment to be way more flexible. Also, the rate of change isn't really that great in our production environment. The few instances that we have a blip are a learning experience. ForeScout provides us with all the characteristics of our environment so we can make the right exceptions. In some cases, you need to get the right folks involved for processing exceptions – this is a good thing. For example, building a new system requires going to XYZ server to download the build, but no one knew the specifics behind it. We were able to figure that out because the ForeScout console was telling us what resource that system was trying to access. We made the exception there and then kept at it until we got the build process to snap through with no issues.

Q: What are some of your most impactful policies and integrations and why?
A: Device authentication and endpoint protection such as anti-virus, encryption and threat protection. If we can remove unknown devices and ensure endpoint security, there is improved compliance and less susceptibility to "bad" things happening. Now we can better monitor and enforce policies before and after network admission, and we have the capability to instantly send warnings, isolate, limit or move systems to appropriate resources, or directly remediate the endpoint or trigger another system to take action.

"We were up and running in a couple of weeks at our main site and got fantastic intelligence. That alone was worth the cost as our team was better informed to make decisions."

Q: When you first turn it on in monitoring mode, what surprised you or prompted you to fix some things before you could move to quarantining?
A: You really don't know what you're missing or think you have under management until you bring in an external control. Just relying on host-based security agents to talk with management systems proved to be not enough. We had some non-standard builds that were built ad hoc, missing patch management agents, clients that weren't getting antivirus updates, or had unsanctioned applications, etc. ForeScout sheds light on all this and then allows you to rollout policy-based actions to fix those issues. Then there is the benefit of real-time hardware and software inventory that ForeScout gives. We can see failed patch rollouts and we can also predict the impact of a possible vulnerability or needed update.

It is not about quarantining, it is about policy and actions. We can chose to inform the end user or help desk on an issue. In many cases, just warning end users that they are possibly violating an acceptable use policy is enough to change behavior. We can take direct remediation actions on an endpoint or invoke actions from other integrations. We have and are starting to bring on integrations with firewall, endpoint protection, patch management, vulnerability assessment, web and email filtering, virtualization such as VMware, security information management and advanced threat detection such as Bromium.

Q: You mentioned integration of ForeScout with Bromium. So Bromium essentially identifies zero days and then ForeScout pushes infected systems into a quarantine zone or a limited access zone? What else?
A: Right – Bromium does 0day protection and we have set up policies in ForeScout to integrate with Bromium to alert immediately, restrict Internet access and then enable our IT to follow up. However, Bromium can only work on certain Windows systems and applications. We use ForeScout to identify those systems that should have Bromium installed but don't and we can initiate action. We have systems that have Bromium installed in the field that are logging potential threats, and that intelligence is being pulled out of the Bromium and captured by ForeScout so that we can make decisions for the older hardware based systems. For example, if we found a particular piece of “badware” at a URL, ForeScout policy can update the Proxy blacklist to add it. ForeScout can also look at the rest of the computers in the enterprise for the presence of threat properties identified by Bromium. ForeScout can find those infected systems and flip them over to a Quarantine VLAN and send us an alert so we can have someone go and look at it. So it's a real-time detection and remediation scenario. It saves us quite a bit of time and gives us the ability to sleep a little bit better at night knowing that we're not going to get popped by an 0day just because the antivirus didn't pick it up. ForeScout allows us maximize what Bromium offers.

Q: Are there any lessons learned you'd like to pass on or things that you would have done differently?
A: From a lessons-learned perspective, you've got to evaluate the technology, the use cases and its application across the entire enterprise. If you're going to have any type of visibility and enforcement, you have to assess how you can do that with your current network environment and security products - even verify the compatibility of the switches. A lot of the companies, smaller satellites or places that have been acquired have disparate architecture and you want to standardize as much as possible. Also, quantify things from the start before the purchase. Calculate the real cost, not just product purchase but total investment, against potential payoff, because saving operational costs motivates companies to spend money on security.

“The interoperability and rules engine allows us to use ForeScout’s product across more applications.”

Q: Are there any features or new things you've told ForeScout hey, I'd really like to see it do this or change this?
A: I've told them I'd really like to see them get away from their Windows console running in Java. Whenever I see Java I cringe, but I'm running Bromium so that helps with my confidence level. From the feature set standpoint, I think the integration set I've asked for as a customer was either already in place or they already had it tagged on their roadmap. I'm very happy with that and I'm very happy with the ease of use. Setting up policy was very complex with the other vendors we evaluated. Here it's a few clicks. If you understand Boolean logic and branching statements, then you're good to go. Since policy templates are open, you can customize and build new ones as you see fit.

Q: How have you found the support from ForeScout tech-support and any support you've needed over your deployment?
A: These guys have been absolutely phenomenal. Very responsive. Even their SE drops us an email every once a while to check in and ask if we need anything. I've been

really, really impressed with the dedication after the sale, not just when they were trying to get it on board.

“I'm very happy with the ease of use. ”

Q: Where do you expect to take the product next in terms of application?
A: We will expand infrastructure integration. That is where this is all heading as part of a more integrated intelligence and control architecture. We are currently expanding into vulnerability assessment and will also investigate capabilities in our web/email filtering solution.

SANS Bottom Line on ForeScout:

1. Adapt your team, processes and technical controls to a continuous monitoring and response model; NAC is among technologies to help get you there;
2. Modern NAC is beyond admission control – it now offers huge visibility, a way to share control intelligence, and a means to quickly contain and remediate issues;
3. Think ahead about use cases, your environment, and policy requirements before you jump in;
4. ForeScout is relatively easy to deploy and use. It it is very extensible and scalable;
5. Extensive interoperability, flexible policies and “phenomenal” technical support.

For more information:
Visit www.forescout.com;
Call 1.866.377.8771 or
Email sales@forescout.com