SANS

WHAT WORKS™

A Credit Union Increased Network Security With Network Access Control Based on Great Bay Software Beacon

SPONSORED BY

GREATBAY SOFTWARE

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 about? Let us know.

www.sans.org/whatworks

ABOUT AIR ACADEMY FEDERAL CREDIT UNION (AAFCU)

Member-owned since 1955, AAFCU is committed to providing a full range of cost-effective products and services to their members (in all 50 states and overseas) by employees who make a difference in our members' lives.

Air Academy Federal Credit Union is guided by our core values – integrity, quality, service, and community – we are committed to corporate social responsibility and to improving the quality of life in the communities in which we operate and to our members. With comprehensive financial products and services, exceptional lending rates, and automated and on-line financial management systems, Air Academy Federal Credit Union is the only "bank" you'll ever need.

ABOUT THE USER

Jeremy Taylor worked in the IT department at Air Academy Federal Credit Union for 16 years. He's held many different roles before taking the Network Services Manager position seven years ago. Jeremy has a Bachelors of Biology with a minor in Computer Science from the University of Colorado.

ABOUT THE INTERVIEWER

John Pescatore, SANS Director of Emerging Security Trends

Mr. Pescatore joined SANS in January 2013 with 35 years' experience in computer, network and information security. He was Gartner's lead security analyst for 13 years, working with global 5000 corporations and major technology and service providers. Prior to joining Gartner Inc. in 1999, Mr. Pescatore was Senior Consultant for Entrust Technologies and Trusted Information Systems, where he started, grew and managed security consulting groups focusing on firewalls, network security, encryption and Public Key Infrastructures. Prior to that, Mr. Pescatore spent 11 years with GTE developing secure computing and telecommunications systems. Mr. Pescatore began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems. He holds a Bachelor's degree in Electrical Engineering from the University of Connecticut and is a NSA Certified Cryptologic Engineer. He is an Extra class amateur radio operator, callsign K3TN

SUMMARY

Annual penetration testing convinced a medium-sized credit union that they were vulnerable to attacks from unauthorized devices on their network. Using NAC features of their networking equipment proved NAC had value but also showed they needed broader capabilities, integration to other security processes and better support. After evaluating several solutions, they chose Great Bay Software. The credit union is still early in the deployment cycle but has already seen security and business value, as well as learned lessons that will ease the broader rollout.

Q Tell us a little bit about who you work for and what your role there is, your position?

A I'm the Network Services Manager for Air Academy Federal Credit Union. We have a fairly small team with eight people in our IT department. I manage a Network Engineer, a Network Admin and two Developers. We also have a Help Desk with three people who handle the entry level calls and the core banking services.

Q Since it is a credit union, is it a central facility and branches? How many different locations are you involved with?

A We have nine locations. Our primary site, Corporate Headquarters, is also our primary data center. We have a co-location facility for our disaster recovery. All the branch locations connect back to the primary data center for connectivity.

Q What kinds of problems were you looking to address that eventually led you to using Great Bay's products?

A We're firm believers in testing our security, so annually we have a third party come in and perform penetration tests and vulnerability assessments to point out what our weaknesses are, and what we need to work on. One of the companies we started using about three years ago was really focused on network access control; we can do some limited type of security using just built-in features on our networking gear such as sticky Mac addresses, but, it wasn't a full-fledged NAC (Network Access Control) solution, so we were never really happy with it. It checks the box, but it's not as good as it could be. After a couple of years with them, we decided that we could get funding for a true NAC solution, and looked at Pulse Secure and Great Bay, and it looked like Great Bay had a better product. Great Bay's sales team was much better prepared, and gave a much better presentation. We decided to do a proof of concept, so we got it set up in a small environment, and what really sold us was the profiling ability. We set up a device that was spoofing the MAC (Media Access Control) address of an approved HP printer, and within about seven minutes, the Beacon software detected it wasn't a printer and shut down the port for us.

Q To understand the environment a little bit, you have a mix of wired and wireless networks in use?

A Yes, that is correct. We have wired and wireless networks.

Q How about BYOD? Is that part of what you needed NAC for, or do you try to use NAC to say no BYOD, and we want to find things and disconnect them?

A We maintain a separate guest network for BYOD, so any corporate resources an employee may need access to via BYOD are made accessible from our guest network. We were looking at NAC to address unauthorized devices on our corporate network; find them and shut them down.

Q You said you convinced management to fund this. Were the results of that consult or third-party recommendations in the pen testing enough to do that, or were there security incidents or other things that demonstrated the need for this to management?

A It was just the results. Being a small team, there's only so many major projects we can take on in a year. We freed up some time and dedicated ourselves to getting something that would fulfill that need.

Q You mentioned you did an evaluation that detected a printer device with a phony MAC address. What other sort of features or requirements were you looking for in a product to do NAC for you?

A We were definitely looking for asset inventory to make sure we knew exactly what's on our network. But more so, it was the ability to profile devices to know that they are what they appear to be and to disable those that are not.

Q Using that scenario as an example, how did you go about removing them or quarantining them?

A The Beacon solution works with the switching device to shut off the port that it's connected to. So, it basically terminated access for that device. We then we had to manually go in and clear the event so that the real printer could go back online.

Q Can you walk through how you installed Great Bay? Is there an appliance that goes on the network and is scanning it or watching DHCP requests? How does Great Bay Beacon find things on your network?

A It definitely required a lot of changes on our part. Most of our IP addressing was static with a very limited deployment of DHCP. To take advantage of the profiling abilities of Beacon we needed to broaden our implementation of DHCP and change the naming scheme for our devices. In the long run, it made us stronger.

Q Physically speaking, was it an appliance?

A It's a virtual appliance, yes.

Q So, it runs on a VMware or on a virtual server and listens on the network?

A Correct.

Q You mentioned you had to manually clear things. Is it alerts that are coming or consoles that warned you or one of your team to look at? If so, how do you get alerts when something happens?

A Since it was a test we were able to monitor the console and watch it happen. We were also able to leverage our SolarWinds SIEM to generate alerts based on RADIUS (Remote Access Dial In User Service) authentication. Alerts were not yet native to Beacon but they are on their roadmap.

Q How long have you been using Great Bay?

A It's been three months. We're still going through and restructuring.

Q What percent of your environment is covered by Great Bay?

A I would say 20 percent right now.

Q How has it been from a false positive perspective or miscategorizing things?

A Our network is not really that exciting since we don't allow BYOD; therefore, it hasn't been an issue on false positives. Our network engineer has spent a lot of time working with Great Bay support to tune that.

Q How about VoIP phones?

A We have two models of Cisco VoIP, so it makes it easy to tune.

Q Is it Cisco switches that Great Bay is interfacing to?

A We are interfacing to Juniper, and our wireless LAN to Aerohive.

Q So, you have a heterogeneous environment?

A Yes, we're a diverse environment.

Q You mentioned some tuning. One of the things I always like to focus on is lessons learned. If you had known some things when you got started, are there things that you would have approached differently.

A We weren't standardized as well as we should have been with naming schemes on devices, so that's made it more difficult – having to go through and rename devices. Being a credit union, the software that we use for banking is name-based, which makes it easier to set up profiles on device locations; however, because of that, it slowed us down significantly.

Q Was your network flat enough that everything was visible where Great Bay could see things? I suppose if you were doing it through the RADIUS or DHCP, you could monitor from a single instance of Great Bay, and you could monitor everything?

A Yes it was visible. In addition, we also had a lot of static addressing, which was a leftover from our credit union banking software.

Q Was it straightforward to interface to the Juniper switches with 802.1X and RADIUS? Did that take a while to do?

A It took a little while to figure out the proper way to do that. I'm sure it would have been much easier if we were standardized on a single vendor.

Q Is this operational at your headquarters location and branches as well, or is this strictly done in your headquarters facility?

A It's centralized at headquarters, but it is also working at branches.

Q So, it can have the visibility and communicate out and do the same quarantining-type actions out there?

A Yes. We had our third-party auditors onsite, and the Great Bay software was able to shut down a LAN Turtle. There will be a WiFi Pineapple test next.

Q The auditors brought in a LAN Turtle to see if you could detect it and see what would happen?

A Yes.

Q So, when they did that, did Great Bay identify it as, "hey, there's a LAN Turtle," or what did it show up as?

A I only saw the RADIUS alerts that it was a unauthorized device and shut down because of the way we're configured. The devices are added to active directory via their MAC address. I saw the notice that it was pulled, but I did not see the console on Great Bay to see what it said.

Q You mentioned the wireless printer previously that was masquerading as a printer. Was seven minutes a similar timeframe for this detection?

A I want to say this was even faster. It took about three minutes.

Q What happens when legitimate new devices are added to your network? How do you keep from getting flooded with alerts or new info from Great Bay Beacon?

A Once we're fully deployed, it is an on-boarding process, so we'll have to on-board new devices. Being a small organization, we can do that. I could see where huge organizations would have a hard time with that.

Q So, you on-board them into Great Bay as an admin action?

A Yes.

Q Often, sometimes with NAC, you discover things that are against policy that you then have to allow. BYOD is one thing, other wireless devices you didn't know were there that you end up having to allow. Are you running into that, or have you been able to quarantine anything that shouldn't be there?

A We haven't run into any unauthorized devices. Having the policy of Bring Your Own Device and setting it on our guest network, nobody tries. So, at this time, I have no good examples.

Q What are your plans for expanding it out to full coverage of your network?

A It's ongoing and we're gradually pulling new branches into the solution.

Q I assume the LAN Turtle was a nice piece of data to show management, but how do you convince management that it's worth continuing and/or expanding?

A Fortunately, our management team is strongly behind security, and being a credit union, that's pretty easy to sell. Definitely having the LAN Turtle show up in the assessment as a successful test was great.

Q As you've worked with Great Bay, are there any requirements or feature requests you'd like to see added or feature requests you've made of Great Bay?

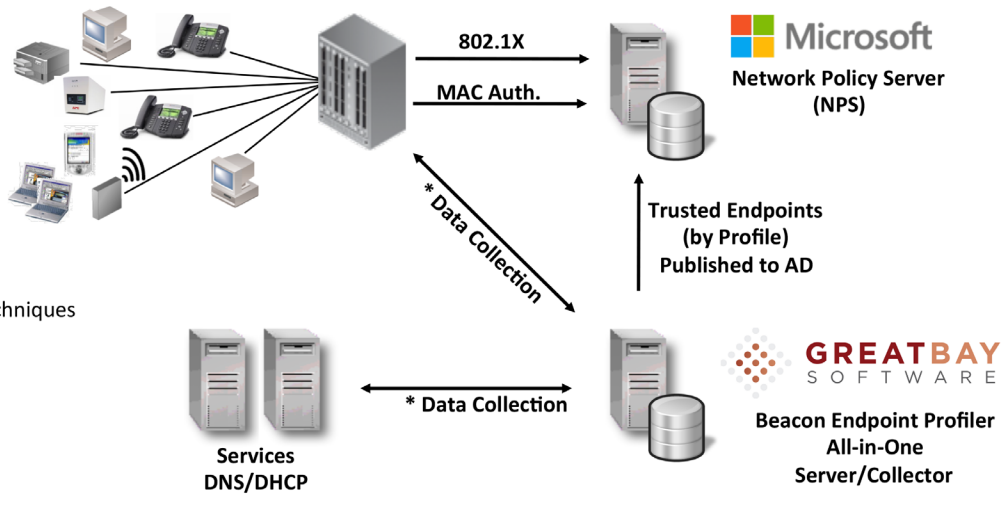
A They do prefer to use a physical appliance, and the way we're architected for disaster recovery, we prefer to virtualize as much as possible. I was able to get support for going virtual all the way.

Q How do you grade Great Bay on the tech support you've gotten from them?

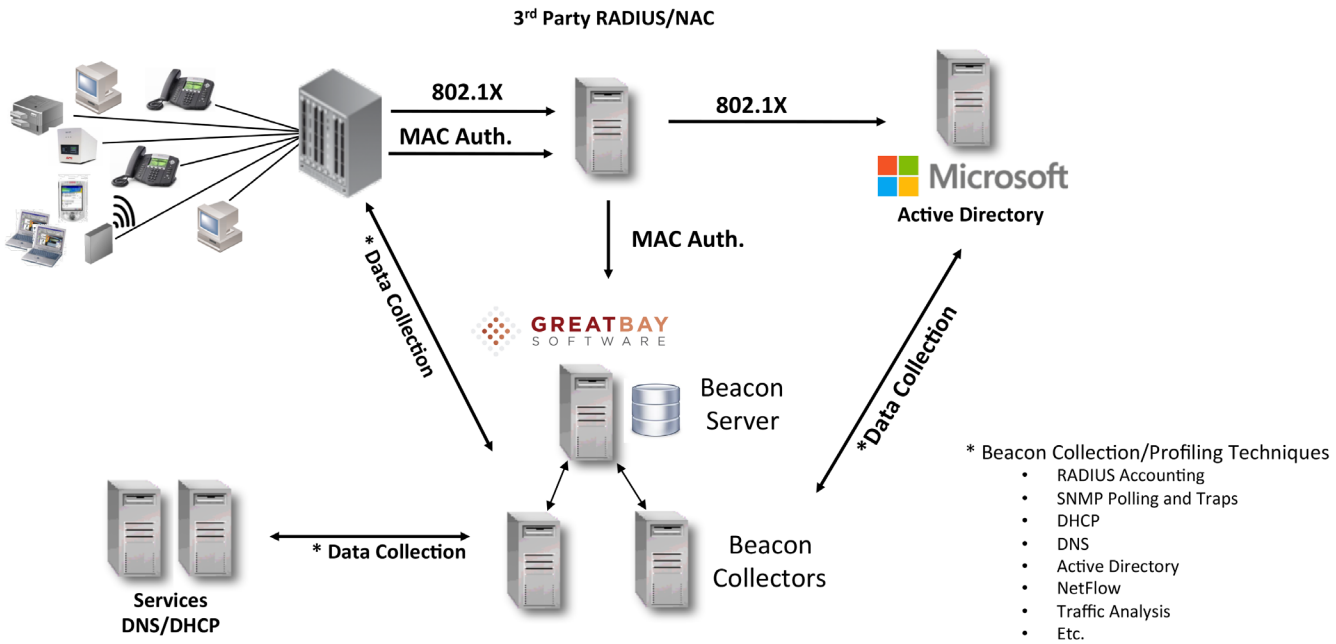
A The support from Great Bay has been very good.

GREATBAY SOFTWARE

Beacon Endpoint Profiler NPS Integration

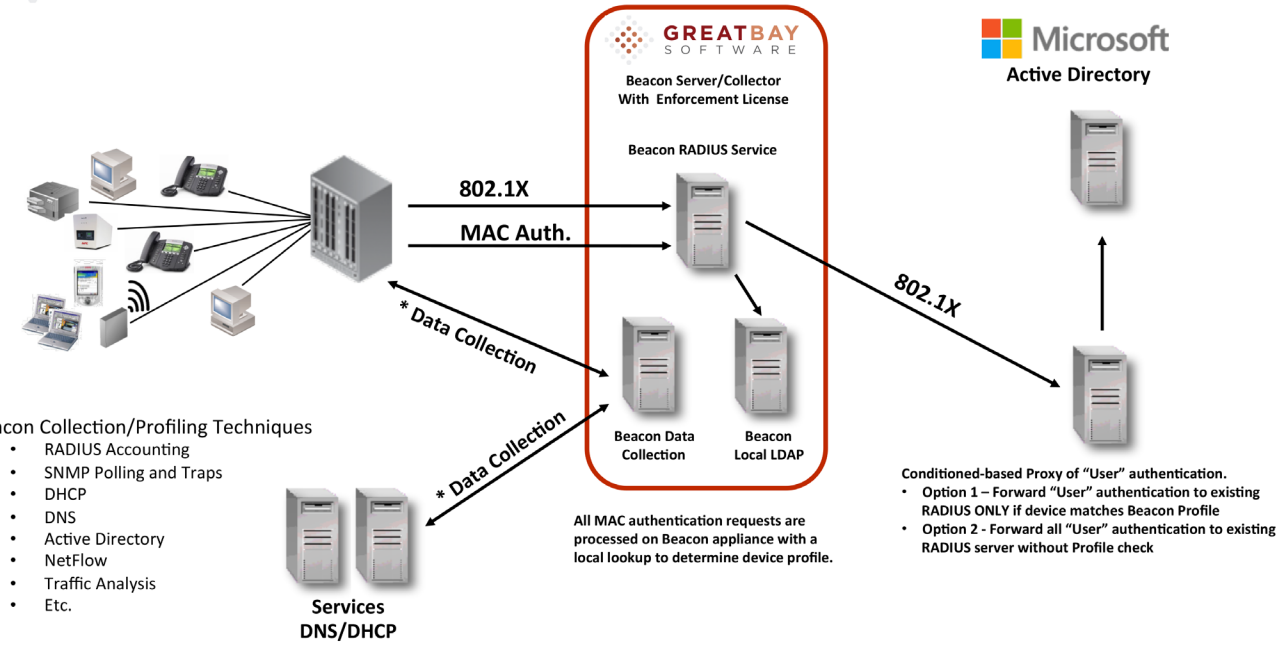


Beacon Endpoint Profiler Architecture



* Beacon Collection/Profiling Techniques
- RADIUS Accounting
- SNMP Polling and Traps
- DHCP
- DNS
- Active Directory
- NetFlow
- Traffic Analysis
- Etc.

Beacon Endpoint Enforcement Architecture



* Beacon Collection/Profiling Techniques
- RADIUS Accounting
- SNMP Polling and Traps
- DHCP
- DNS
- Active Directory
- NetFlow
- Traffic Analysis
- Etc.

All MAC authentication requests are processed on Beacon appliance with a local lookup to determine device profile.

Conditioned-based Proxy of "User" authentication.
- Option 1 – Forward "User" authentication to existing RADIUS ONLY if device matches Beacon Profile
- Option 2 - Forward all "User" authentication to existing RADIUS server without Profile check