



Brocade and ForeScout Create a Secure Visitor Network for ITOCHU

“ Brocade said ForeScout would plug right in and play nicely in their switch environment, automate my entire visitor network ... and ‘then some’. They were right. The ForeScout product installed in a day, and immediately began to deliver value. ”

John Budek,
Infrastructure Manager
ITOCHU North America

Objective

- Create a reliable, secure visitor network to connect ITOCHU’s nine North America branch offices and third-party partners

Solution

- Brocade FastIron Edge switches with out-of-band ForeScout CounterACT network access control appliances

Results

- Visitor network improves security and reliability while decreasing IT management time costs
- Automated health checks and security software updates bring managed laptops into IT-compliance
- Plug-and-play deployment ensures ForeScout appliances install in Brocade-based network in less than a day

ITOCHU is a huge financial and industrial conglomerate based in Japan.

And grow they have. Today, ITOCHU ranks as one of Japan’s largest companies and is among the largest companies in the world. ITOCHU has over 1000 subsidiaries and associate companies worldwide which altogether employ over 45,000 people. ITOCHU has holdings in everything from food to photovoltaic farms.

ITOCHU’s growth-through-acquisition strategy has resulted in some interesting IT challenges.

SUMMARY

How do large companies such as ITOCHU who grow through mergers and acquisition ensure that their various businesses remain interconnected and collaborative? The answer for ITOCHU is to provide a network that combines flexibility with security. The network needs to support employees who travel from office to office across business units and to allow guest access by authorized third-party partners.

To support employees visiting its North American offices, ITOCHU North America added ForeScout CounterACT appliances to its Brocade network. The ForeScout appliances identify the visitors when they plug into the network, allowing them to access the Internet without risking the security of the North American network. The visitor network has been automatic, seamless, and easy to implement. And many other security benefits have also been realized.

Why ForeScout?

ITOCHU North America asked Brocade for a suggestion, and Brocade recommended ForeScout CounterACT network access control (NAC) appliances.

According to ITOCHU North America Infrastructure Manager, John Budek: “Brocade said ForeScout would plug right in and play nicely in their switch environment, automate my entire visitor network ... and ‘then some’. They were right. The ForeScout product installed in a day, and immediately began to deliver value.”

Budek explains: “All I expected ForeScout to do was add the visitor network piece. Was I surprised! ForeScout CounterACT gave me a lot more than I asked for – all in one simple integrated package.”

In 2009, Budek and his IT staff of three rolled out ForeScout CounterACT appliances to its nine North American offices. Every installation had a very low impact on the network:

- All appliances sit out-of-band, which means no latency or points of failure
- 100% clientless which means no software to install
- Non-intrusive to users
- Works with Windows, Linux and Mac
- Integrated seamlessly with the Brocade Switch environment, so no need to replace hardware or reconfigure anything
- Completely compatible with all third-party products

The resulting implementation includes: Two CounterACT appliances are located in the New York office – one at the core and one at the distribution layer - to give complete visibility and control over all devices in New York. Each branch office has a Layer 3 Brocade switch with a smaller CounterACT appliance to give complete visibility and control over devices at each of the nine remote sites.



How ForeScout Helped

Brocade-ForeScout have given ITOCHU North America a network that facilitates its strategy to grow through acquisition. Results went far beyond their original objectives:

- Enhanced productivity by automating visitor network access without compromising network security.
- Reduced helpdesk costs by automating health checks for all visitor laptops
- Improved security through automatic detection and remediation of endpoint vulnerabilities
- Reduced risk of infection by blocking malware and attacks inside the network
- Improved security by blocking P2P and instant messaging applications – closes “back doors” to the network
- Automatic “update-audit” reports – shows which endpoints have the latest Windows SUS updates

The Brocade-ForeScout solution has paid for itself within just a few months by helping ITOCHU North America find and disable resources that waste company time and money or that open up “back doors” to the network.

Explains Budek: “Our corporate policy disallows the installation and use of peer-to-peer and instant messaging applications. Within minutes of installing ForeScout CounterACT, we found a slew of machines that were in violation of this policy. ForeScout helped me identify and block those machines. We then sent alerts to remind users about our corporate policy. They were required to remove the applications and, if they cared to protest, were asked to submit a department authorization/resource justification form.”

Budek went on to describe another benefit of their network:

“As a network diagnostic tool, ForeScout CounterACT has proven to be worth its weight in gold. About a month ago, users began complaining about a slow network. We ran CPU utilization summaries, and we discovered that an Active Directory (AD) server was being bombarded with CPU requests. To fix the problem, I needed to know which endpoint computers were behaving badly. I had been told that ForeScout CounterACT was a ‘super sleuth’ that could help us discover almost anything about our endpoint computers, so I decided to try it. In almost no time, CounterACT was able to tell me that twenty machines were causing the traffic.”

“With a little more sleuthing, I discovered that these twenty machines were all new systems that came with preinstalled services. One of these was an unnecessary RPC service that was flooding our AD server with CPU requests. Using ForeScout CounterACT, I blocked and disabled the twenty machines – almost instantly. We removed the RPC service on each machine, and had our network back up to full bore in minutes. In the past, diagnosing similar consumption issues could have taken me hours – even days, resulting in a huge loss in productivity.”

ITOCHU-North America continues to enjoy seamless operation of its ForeScout and Brocade joint solution. The solution delivers high availability and network performance with minimal downtime and the least amount of disruption. Both organizations continue to work together to help ITOCHU maximize its investment in their solutions.

For more information about ForeScout’s CounterACT appliance, visit www.forescout.com/counteract.