CU t-t CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Battling Security Fatigue – Working Towards Usable Security

The security requirements of networks in financial institutions are extremely complex. Confidential customer data must be protected at all costs. Compliance with regulations must be demonstrable. And, like any business, the network must be secure and available to employees, customers and contractors. ForeScout achieves this by providing secure access to PCs and laptops, mobile devices and other devices such as Internet of Things (IoT) while giving IT personnel the tools to see, control and orchestrate network security.

Before instilling good habits, it's important that all employees understand the overarching challenges the organization faces. Those challenges include:

- Controlling access to confidential data
- Measuring effectiveness of security controls
- Identifying and securing unmanaged and IoT devices
- Guarding against targeted malware threats

Once employees know about these challenges, educational efforts should target desired outcomes.

For example, users should know that hooking up an IP-enabled camera to the network may seem harmless, but being aware of the security risks associated with introducing such a device to the network could help prevent it from happening the first place. At the same time, using ForeScout CounterACT® to accurately identify and segment these IoT devices would also provide a technological control to mitigate this particular threat.

ForeScout offers agentless visibility and control of connected devices, allowing you to better secure your financial services network, enforce device hygiene compliance and demonstrate regulatory compliance with FINRA, GLBA, PCI DSS, SOX and other mandates to auditors.

Our platform lets you:

- See, profile and monitor systems, including Bring Your Own Device (BYOD) and contractor systems, rogue devices and agentless IoT devices such as smart monitors, VoIP phones and security cameras. See how.

- Control device access to network resources, applications and network segments across financial services networks, datacenters and the cloud. Gain control.

- Orchestrate and automate security response among third-party security tools. Extend our capabilities to your tools.

In addition to the above and most importantly, a ForeScout solution can be done without network upgrades, new configurations or cumbersome agent-based deployments. So, if you have wired and/or wireless deployments, a variety network vendors, the need for security from the campus to the cloud and/or a large variety of devices, you can count on ForeScout to work within your heterogeneous environment and deliver value quickly.

Toni Buhrke
WW Director, Channel Systems Engineering

ForeScout

Toni Buhrke
is WW Director of Channel Systems Engineering at ForeScout and is a frequent speaker at various security and customer events about network visibility and access control in today's complex IT environments, including IoT.

She frequently blogs about cybersecurity and was technical advisor for the book "Definitive Guide to Next-Generation Network Access Control." During her 9 year tenure at ForeScout, she has been instrumental in helping customers address endpoint visibility, IoT, compliance, and other IT security initiatives, along with building successful system engineering teams.

Toni has over 25 years of experience in IT security in both internal IT and technical vendor roles, has an MBA, and is CISSP certified. She is an active member of many IT security groups, including ISC2 and ISSA.

Contact Info

www.ForeScout.com