ForeScout

Solution Brief

ForeScout Benefits

- Preserves investment in infrastructure and tools
- Deploys quickly and delivers rapid time to value
- Automates hardware and software inventory and reporting
- Streamlines BYOD onboarding
- Automates device compliance and remediation
- Allows flexible deployment options
- Can be administered onsite or from district office
- Provides a single-pane-of-glass view across entire school district
- Reduces risk by blocking unwanted devices and applications
- Helps ensure security software is up to date on devices

K-12 Cybersecurity and Title I Compliance

Keeping networked devices and data secure and accounted for

Today's school districts must manage complex challenges. Aside from educating students and helping them meet academic standards, school officials must find affordable ways to accommodate digital learning, mobility and cloud computing. While these trends are transforming education, they also expose schools to increasingly sophisticated threats. ForeScout is helping educators securely embrace technological trends while complying with state and federal government mandates.

The Challenge

Title I Compliance

Nationwide, the Federal Government provides local school districts with more than $14 billion in Title I funding[1] to over 66,000 schools and over 23 million students.[2] Title I funds can be used for instructional activities, counseling, parental involvement, program improvement and IT equipment. In return, school districts must comply with accountability requirements—including maintaining an inventory of devices purchased with Title I funds. That inventory must include information on where devices are located, who is using them and how they are being used.

Specifically, most State Educational Agencies (SEAs) require Title I grant recipients to provide the following information about IT devices purchased with Title I funds:

- Description of equipment
- Cost
- Serial Number
- Date of purchase
- Location of the asset
- How the equipment is being used
- Who is using the equipment

School districts can be subject to audit and risk losing Title I funding if they are unable to properly maintain an inventory that contains this information. Title I asset control and inventory management can be challenging—especially when school officials are tasked with tracking, monitoring and protecting what they can't see.

IDC Does the Math: ForeScout Is Affordable and Cost-Effective*

IDC recently interviewed senior IT officials from seven organizations that deployed the ForeScout security platform. Based on their findings, the IDC researchers predict that these organizations will:

- Identify 24% more devices on their networks
- Experience 50% fewer network-related security breaches
- Improve overall IT efficiency by 13%
- Gain $46,040 in benefits per year per 1,000 devices on networks

> **We need to support over 200 iPads used by teachers and staff. With ForeScout CounterACT's guest networking capabilities, we can easily grant network access to staff and guests as long as they have a valid logon credential."**
>
> **— Cache County School District IT Administrator**

Cybersecurity and Prevention

One of the most formidable cybersecurity challenges school IT officials face is the necessity for students, teachers and administrators to be able to use school-owned PCs, laptops, tablets and smartphones as well as personally owned Bring Your Own Device (BYOD) endpoints. To some degree, all of these users need anytime, anywhere access to resources. That being the case, there's a need to know what systems and devices are on the network. This requires visibility so that devices can be identified and classified—and granted access to the network according to who they belong to and whether they comply with policies and regulations. Of course, all of this must be accomplished without degrading the user experience.

Another key aspect of cybersecurity is threat detection. Today's cyberthreats are more sophisticated than ever before and can evade traditional security defenses. These highly targeted attacks focus on disrupting services or acquiring sensitive personal information. Compromised endpoints and data breaches can often remain undetected for weeks or months. Consequently, there must be a mechanism in place to ferret out devices and applications on the network that are there to cause harm.

Privacy and Protection

K-12 IT security specialists must keep sensitive information on the network secure, maintain the integrity of online learning systems and resources, and sustain the free flow of information despite the fact that hacking is fast becoming a competitive sport. To protect the privacy and confidential data of students, teachers and administrators, there must be technologies and policies in place to protect devices and the network—keeping damage to equipment, theft of data and the spread of malware in check. Also, should attackers manage to penetrate perimeter defenses through phishing or other forms of social engineering, they can't be allowed to move around the network to locate targeted information.

The ForeScout Solution

Title I Compliance

ForeScout CounterACT® helps school districts comply with Title I inventory requirements by providing comprehensive visibility into the devices on their networks. CounterACT can help ensure that Title I equipment inventories are up to date and accurate, while providing inventory information in a fraction of the time and cost of current manual, labor-intensive, paper-based inventory processes. In fact, CounterACT can even alert IT staff to the misuse of Title I assets in real time—for instance, when assets are moved to areas of the school district where they should not be located.

With ForeScout, schools can:

- **Identify** computers, unmanaged personal devices, Internet of Things (IoT) devices and rogue endpoints in real time.
- **Discover and Track** software to help ensure that school districts only pay for software they actually use.
- **Collect** hundreds of attributes about devices connected to networks, including hardware and OS configuration, software versions and currently logged-in users.
- **Place** device data in a contextual database, giving schools an easy way to track information about their digital assets and how they are used.
- **Validate** that antivirus and other host-based security applications are installed, running and updated to help ensure the network is protected from cyberthreats.

> **CounterACT maximizes our network security, has already saved us time—which equates to money—and helps us to mitigate potential security breaches."**
>
> **— Steve Banyard, Network Manager, Norwich School (UK)**

Cybersecurity: The Stakes Are High

- During the summer of 2015, three teenage boys hacked into a high school records system in Long Island, New York, and altered the grades of two students and the fall schedules of about 300 students.[3]
- Nearly 800 educational institutions have experienced a data breach event since 2005 (about one educational institution per week). Nearly one-third were K-12 primary and secondary schools.[4]
- The Broward County school district faces the prospect of needing to pay back $23 million after a state audit found it improperly distributed Title I funds. A report from the Florida State Auditor General concluded that the district failed to keep track of assets owned by charter schools, among other violations.[5]

Cybersecurity through Visibility

ForeScout can help you manage mobility and BYOD trends in ways that are secure and reliable without inconveniencing students, teachers, administrators and guests. Unlike solutions that simply flag violations and send alerts to IT and security staff, CounterACT lets you automate and enforce policy-based network access control, endpoint compliance and mobile device security. CounterACT continuously scans the network and monitors the activity of the wide range of devices attempting access, as well as those already logged on. You can see the devices on your network and their security postures—including student- and teacher-owned devices as well as visitor-owned devices, rogue and IoT devices—even those devices without software agents on board. Further, CounterACT lets you classify and profile devices, users, applications and operating systems.

Network Access Control Based on Policies

Schools need to be able to keep unauthorized individuals out of places on the network they don't belong, or off the network entirely. CounterACT lets you allow, deny or limit network access based on your security policies. It can automate the process of notifying end users, administrators or IT systems about device-related security issues. CounterACT can also quarantine, remediate or block non-compliant or compromised devices—automatically, on a 24x7 basis.

In addition, CounterACT can control access to school networks by enforcing network segmentation. With segmentation, students, teachers, administrators and guests only "see" the servers and other devices that they need for completing their daily tasks—and nothing more. There is no ability to move laterally across the network for snooping, stealing private information or other malfeasance. This greatly reduces the attack surface and overall security risk while allowing appropriate, productive access.

Automation Instead of Manual Intervention

There's no getting around the fact that BYOD adds complexity and risk to the task of network protection. Unlike the old days when everything on the network was a known entity and district-owned systems and devices were tracked, controlled and locked down in every way possible, BYOD requires a much more open environment. However, with CounterACT, order can be maintained.

Aside from its ability to continuously monitor the network and limit or prevent access by rogue or non-compliant devices, CounterACT can work with key Mobile Device Management (MDM) or Endpoint Protection Platform (EPP) solutions to further automate and orchestrate network and infrastructure protection—not to mention accelerate incident response.

In combination with ForeScout Extended Modules, CounterACT can exchange information with leading MDM tools to validate device hygiene of tablets, monitor security posture and automate enforcement and endpoint remediation processes. Working with MDM solutions, the ForeScout platform can also restrict the use of blacklisted software, such as banned proxy applications on tablets and smartphones, to help prevent access to banned or inappropriate websites. The ForeScout platform can also notify users, district IT staff and local school staff of issues. As to EPP tools, the CounterACT platform can help ensure that agents from McAfee, Symantec and other EPP tools are active and up to date and can automate endpoint remediation.

For resource-constrained school districts, automation and orchestration may be the most attractive benefits of the CounterACT platform.

Seeing Is Believing

ForeScout CounterACT is sold as either a virtual or physical appliance that deploys within your existing network, typically requiring no changes to your network configuration. The CounterACT appliance physically installs out-of-band, avoiding latency or issues related to the potential for network failure. It can be centrally administered to dynamically manage tens or hundreds of thousands of endpoints from one console.

Learn more at **www.ForeScout.com**, and contact us for a free demonstration.

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

* *The Business Value of Pervasive Device and Network Visibility and Control with ForeScout*, IDC, December 2016

[1] https://www2.ed.gov/programs/titleiparta/funding.html

[2] https://www2.ed.gov/programs/titleiparta/index.html?exp=0

[3] http://abcnews.go.com/US/ny-high-school-students-accused-hacking-computer-system/story?id=34617530

[4] http://www.azcentral.com/story/money/business/tech/2015/08/21/colleges-schools-information-rich-targets-hackers/32093511/

[5] http://www.sun-sentinel.com/news/fl-broward-auditor-general-report-20160405-story.html