THE GRADES ARE IN:
ONLY SAFE NAC GETS A+ IN RISK REDUCTION

SAFE NAC ENABLES STUDENTS AND FACULTY TO STUDY AND WORK ON DEVICES OF THEIR CHOICE.

CASE STUDY | MARKET: **EDUCATION** | REGION: **NORTH AMERICA**

BUSINESS PROBLEM

Enable students and staff to bring their own devices while also maintaining a high level of security and integrity to its network.

SOLUTION

Safe NAC, a joint solution by Alcatel-Lucent and InfoExpress.

The Hamilton Southeastern School District, located in Fishers, Indiana, who's mission is for every student to reach their maximum potential, preparing students for a successful post-secondary education and to excel within a quickly evolving modern workforce. With those goals in mind, the district focuses on instilling in each student what it calls "the five C's": critical thinking, creativity, collaboration, communication, and cultural competency. The district aims to integrate technology and to take a more project-based approach to education, so that the learning experience will match the experiences its students will face in college and the workplace.

However, with technology changing so quickly – just look at the rapid adoption of tablet computers in the past two years – there's little chance any school district can accurately predict what the prevailing technologies may be in the years ahead, let alone afford to acquire devices for each student. The answer for the Hamilton Southeastern School District was similar to that of most school districts around the nation, as well as businesses for that matter: let individuals bring your own device (BYOD) to school.

“THE SUPPORT AND HELP FROM BOTH INFOEXPRESS AND MELSERNET WAS SECOND-TO-NONE. WHENEVER WE HAD A QUESTION, INFOEXPRESS MADE ITS SUPPORT TEAM AND ENGINEERS READILY AVAILABLE TO US.”
Walter Morales, Chief Technology Officer at Hamilton Southeastern School District

NETWORK ACCESS CONTROL ENABLES ORGANIZATIONS TO VET THE SECURITY OF DEVICES BEFORE THEY CONNECT TO THE NETWORK

“BYOD” REQUIRED A NEW IT SECURITY PARADIGM

The sales numbers behind mobile devices are mind-numbing. The Stamford, Connecticut-based market research firm and consultancy Gartner predicts that by 2014, 90 percent of companies will be supporting corporate applications on personal mobile devices. Also, according to Gartner, 80 percent of enterprises will soon have a tablet-equipped workforce.

However, the BYOD trend, whether a public school or a Fortune 500 enterprise, isn’t without risks. Mobile malware is on the rise. And when organizations give up control over what endpoints are allowed to connect to the network, they lose a great deal of control over how those devices are managed and secured. For instance, unlike organizationally controlled devices on which patch updates, anti-virus and anti-malware software, and system settings all can be configured to help harden systems from attack, all of those controls are lost when users bring their own devices to the network.

That’s where Network Access Control (NAC) comes in. NAC enables organizations to vet the security posture of devices before they can connect to the network and control access to network resources.

“While users bringing their own devices help make everyone happy and hopefully productive, and also helps to preserve the district’s budget, we needed a way that we could ensure that our students and faculty were not introducing malware from their personal devices onto our network,”

says Walter Morales, Chief Technology Officer at Hamilton Southeastern School District. “We believed that network access control would provide the best defense.”

Serge Melki, President of Indianapolis, Indiana-based IT solution provider Melsernet, agreed. “Network Access Control is ideal when it comes to maintaining the level of security an organization needs for devices they own and manage, as well as devices users bring on their own,” Melki says.

To succeed, Melki knew the NAC technology the district selected would have to be scalable, secure, and easily managed. In total, the school district’s 2,000 employees help to provide the education for its 19,000 students.

“We evaluated the offerings of many different NAC providers, and we tested them thoroughly,” explains Melki. “What we found, initially, wasn’t comforting. Many couldn’t be configured properly. Others didn’t provide adequate security. They focused merely on attacks such as denial-of-service (DoS), while others just didn’t provide the functionality we sought.”

The only NAC technology that met both Melki and Morales’ strict criteria was Safe NAC, made possible by a joint effort by Alcatel-Lucent and InfoExpress. The security capabilities of Safe NAC protects the public school division’s distributed network and helps its more than 30 schools offer staff and students secure access to the instructional tools and resources they need. In addition, Safe NAC’s unique visibility features gives Melki’s team a complete picture of who and what is connecting to the network.

IN-DEPTH: SAFE NETWORK ACCESS CONTROL

Safe NAC is a fully integrated NAC, designed for multi-vendor networks equipped with a variety of managed and non-managed endpoints. Safe NAC provides guest access, host integrity checks, and role-based access control to help organizations ensure compliance. Safe NAC also is backed by a global, highly-experienced multi-vendor capable professional services organization.

Safe NAC reduces costs by automating operational processes and minimizing the need for IT operator intervention during authentication. There also is simplified troubleshooting and reduced help desk costs, which enables a reduction in operational overhead and proactively ensures the health of the network.

Safe NAC is composed of InfoExpress’ CyberGatekeeper Policy Server, CyberGatekeeper Policy Management and Reporting Server, and CyberGatekeeper agents. It is integrated with Alcatel-Lucent products including the OmniSwitch platforms (AOS 6.3.4 and newer), the OmniVista Access Guardian and Quarantine Manager, the VitalQIP and OmniAccess wireless platforms.

With Safe NAC, CyberGatekeeper’s tight integration with Alcatel-Lucent enables enterprises to make certain that endpoint devices are verified to be compliant and healthy when connecting to the network. Only those endpoint devices that are compliant with enterprise security policies are allowed access to the network.

As long as an endpoint is connected to the network, CyberGatekeeper provides continuous security surveillance. Those endpoint devices that fail the host integrity check are redirected and placed into quarantine for quick remediation before being granted access.

Safe NAC is easy and fast to deploy without requiring a major network overhaul and without sacrificing security.

CUSTOMER SUMMARY

Customer Name:
Hamilton Southeastern School District

Industry:
Education, government

Number of students/staff:
19,000 students; 2,000 staff

URL:
www.hse.k12.in.us/ADM

"WITHOUT SAFE NAC, WE PROBABLY WOULDN'T HAVE BEEN ABLE TO ALLOW STUDENTS TO BRING THE DEVICES OF THEIR CHOICE ONTO THE SCHOOL'S NETWORK."

Walter Morales, Chief Technology Officer at Hamilton Southeastern School District

SMOOTH DEPLOYMENT, SUPPORT "SECOND-TO-NONE"

"The deployment went very smoothly," says Morales. "The support and help from both InfoExpress and Melsernet were second-to-none. Whenever we had a question, InfoExpress made its support team and engineers readily available to us."

For the first phase of the deployment, the district tested Safe NAC on a number of desktops, where it began enforcing the requirement that updated anti-virus definitions be in place before being admitted to the network. "That went very well," explains Morales. "Within a few weeks, we deployed Safe NAC out to the rest of the network, as well as student devices."

Should a student's or faculty member's system try to connect in a noncompliant state, it is guided to a web page containing instructions on how to bring the system to expectations set by the district's security policy. Once done, immediate network access is granted.

Building on that success, in upcoming months, the district plans to extend its Safe NAC deployment to its remaining high schools. "Without Safe NAC, we probably wouldn't have been able to allow students to bring the devices of their choice onto the school's network. Fortunately, thanks to Safe NAC, that's not a situation we have to face," says Morales.

ABOUT SAFE NAC AND CYBERGATEKEEPER

CYBERGATEKEEPER REQUIRES MINIMAL NETWORK CHANGES AND ENSURES INTEROPERABILITY IN MULTI-VENDOR LEGACY AND CURRENT NETWORK ENVIRONMENTS.

- Ensures 100 percent of network endpoints are compliant (patch levels, configurations, and application settings) or they are quarantined until remedied
- Endpoints can be plugged into phones and still be secured
- Will not interfere with existing VoIP deployments
- Keeps rogue devices off the network
- Reduces vulnerabilities, as security solutions, OS, and patches are assured to be running and up to date
- Lowers help desk costs – automatic remediation of non-compliant PCs

www.alcatel-lucent.com/enterprise

0312 NA ENG

Alcatel·Lucent Enterprise