FIREEYE™

CUSTOMER STORY

Denver Public Schools Utilizes FireEye to Protect Students' Prestine Identities

DENVER PUBLIC SCHOOLS
Discover a World of Opportunity™

FACTS AT A GLANCE

INDUSTRY

Education

SOLUTIONS

- FireEye Network Security
- FireEye Email Security
- FireEye Endpoint Security

BENEFITS

- Enhanced security through cross-platform communications
- Integrated solutions provide multi-vector protection
- Savings from operational efficiencies
- Support for district-wide BYOD initiative

CUSTOMER PROFILE

The Denver County School District No. 1 — generally known as Denver Public Schools — serves 92,000 students in 199 schools across the city and county of Denver, Colorado, and it employs almost 12,000 staff. Of the nearly 300 school districts in the United States with at least 25,000 pupils, Denver Public Schools has had the second-highest academic growth.

Denver Public Schools' (DPS) IT department manages 24,000 Microsoft Windows computers, as well as a similar number of Chromebooks. It supports Google Apps for Education to provide students with the ability to collaborate and share information, while Microsoft Office is maintained for the use of faculty and staff.

In addition to the large network of district-owned desktop and laptop computers, DPS permits students, faculty, and staff to connect their own smartphones and tablets to its network, under a 'bring your own device' (BYOD) policy. On an average day, the network handles 25,000 individually-owned devices, bringing the total endpoints managed to over 73,000. Correspondingly, email volumes generated and received by the enormous number of devices run into multiple millions of messages each month.

The Shock of Being Breached

In 2014, many DPS employees received a phishing email directing them to a credential harvesting website that tempted unsuspecting visitors to provide passwords and other login details. A few users inadvertently responded, allowing the attackers to use the stolen credentials to breach the district's human resources system. The criminals were able to hijack the direct deposit routing for the payroll of a number of employees, resulting in a loss of almost $30,000 for the district.

> "FireEye alerts are almost always valid, and that accuracy is important in keeping us efficient in our remediation of attacks."
>
> — **Robert Losinski,** Manager of Information Security, Denver Public Schools

Reeling from this breach, and knowing that the massively popular BYOD program had the potential to inflict vulnerabilities anywhere in its network, DPS began looking for more advanced threat prevention tools to safeguard its infrastructure. The district's attention quickly focused on FireEye because of its reputation for threat prevention across multiple domains.

Robert Losinski, DPS' Manager of Information Security, recalled, "We were looking for solutions that would protect our network, email and endpoints. We also needed tools that would elevate our incident response capabilities."

Losinski consulted with each of the five other school districts in the Denver area and with the IT department of a nearby county. It soon became clear that FireEye was the leading security-as-a-service vendor for all of them.

Comprehensive Coverage

The district elected to install an integrated FireEye suite comprised of FireEye Email Security, FireEye Network Security and FireEye Endpoint Security. FireEye worked with DPS IT personnel during a week-long engagement to integrate the solutions into DPS' infrastructure. "They were very knowledgeable about the implementation and it went very smoothly," noted Losinski.

"A big advantage of having all the components from FireEye is that one of them will create an alert and publish that information to the others," said Losinski. "The proliferation of intelligence between solutions really makes a big difference to the effectiveness of our protection."

DPS is conscious of the fact that students generally have unblemished online identities. "A 12-year old's identity is a blank canvas, making it an extremely attractive target for cyber criminals," commented Losinski. The FireEye suite of solutions helps DPS protect students from these attacks.

When FireEye Endpoint Security detects a threat, the IT staff can rapidly isolate it from the network, and FireEye Network Security is configured in blocking mode to deliver protection from threats arising from BYOD tablets and phones. "We typically receive around 40 threats that originate from Android devices on any given day," observed Losinski. "Once they are blocked, we help students remove the infection and try to teach them how to prevent a reoccurrence. FireEye alerts are almost always valid, and that accuracy is important to keeping our attack remediation efficient."

Some of the threats witnessed can originate from students. For example, some have downloaded denial-of-service software in order to disguise their absence from class. Enterprising students have pushed the envelope of digital security encryption by attempting to install Bitcoin miners on district servers. FireEye Network Security immediately identified and alerted the IT staff of these attempts. "After we catch the students we talk to them to try and help them become responsible 21st century Internet citizens," Losinski reflected.

Accurate and Timely Data Delivered Economically

Losinski values FireEye innovation and its commitment to the cloud platform. "FireEye is a leader in the threat prevention market: FireEye Dynamic Threat Intelligence gathers threat-related information from its millions of endpoints and shares it globally with all FireEye users. This benefits our school district because we always have the latest, high-quality threat intelligence coming into our system to protect our network," emphasized Losinski.

He concluded, "Any investment in technology is an investment that comes out of the classroom, so we appreciate the cost-effective solutions that FireEye provides to protect both district assets and devices brought from home."

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™