

IronMail security keeps hostile code and intruders out of servers and clients, and protects in-transit emails.

Background

The Georgia Department of Technical and Adult Education (DTAE) oversees the state's system of technical colleges and the adult literacy program, as well as a host of programs that provide continuing education and customized training to the citizens of Georgia.

"We have 35 main campus sites around the state, and each site has anywhere from 500 to 5,000 students," says Geoff Catron, director of networks and security for DTAE. "We support about 35,000 work stations statewide, and the system handles over 100,000 messages daily. Email is absolutely essential. Besides our internal business communications, we do a lot of online instruction and email is the primary link between the instructors and the students."

Business Challenge

DTAE's initial problem was spam. But security quickly became a key requirement. "We couldn't afford to upsize our mail servers to keep up with the trash mail," says Catron. "And as we opened up the email problem, it raised both security and privacy issues.

For example, one factor contributing to the spam problem was the collection of email addresses through directory harvest attacks. But preventing directory harvesting requires tighter security – not spam filtering. In addition, protection for student information – which may include medical data – had to meet Federal guidelines. This means protecting email in transit as well as protecting the data when it resides on mail servers, to prevent theft. Finally, DTAE servers and workstations all needed defense against hackers and malicious code that could destroy data and cause downtime. All of these issues require email security.

Why DTAE Chose CipherTrust

"We spent a year trying to make another product work," Catron says. "There were major compatibility issues with Exchange. The thing just wouldn't work right. Our lead engineer – who had done a tremendous amount of testing on the other product – wanted to evaluate IronMail. We did, and we've never looked back."

Catron adds, "We knew in less than a week that IronMail was the solution we wanted. Besides handling spam, IronMail delivered a completely new dimension of security features not offered by the other vendor. Security became the focus of the deployment. On a project of this size, we have to have buy-in from all of our college presidents. Spam performance was critical, but security is what sold them."

The IronMail Solution

DTAE's IronMail solution has been up and running since late 2002. At each of 35 campus sites, an IronMail box sits between the firewall and the Exchange servers. The Exchange servers are isolated and protected from the outside network by the IronMail appliances.

DTAE At-A- Glance

Industry

Distance learning
and adult education

Company and Location

Georgia Department of Technical
and Adult Education; sites
throughout the state of Georgia

Business Need

- Maintain security of sensitive student information
- Protect email servers from intruders
- Protect client workstations from malicious code

Solution

CipherTrust's IronMail security
solution

Results

- Security for 35 critical email gateways
- Privacy for sensitive email content
- Protection for 35,000 networked workstations
- Blocking more than 90% of spam

Encryption provides email privacy

With IronMail, emails traveling among DTAE sites on the statewide network are encrypted for protection from unauthorized viewers.

IronMail Secure Delivery assures email privacy with a system of encryption tools, filters and email policies. Secure connections from the IronMail appliance to servers and clients use industry standard SSL/TLS encryption to provide secure, private delivery of Internet email. IronMail Secure Delivery also supports legacy systems using S/MIME and PGP technology.

Email firewall and intrusion prevention protects servers and workstations

Encryption protects email in transit, but servers and workstations still need security from attacks and malicious code. IronMail protects email servers against intrusion, and prevents contaminated email from reaching the network and infecting client workstations. Sophisticated detection techniques guard against attacks and intrusions including buffer overflow attacks, relay abuse and denial-of-service attacks.

“The IronMail box protects our email clients by filtering potentially malicious code before it can enter,” Catron says. “And the filters work both ways. IronMail helps us be good net citizens by stopping outbound contamination.”

IronMail provides web mail protection, too

Webmail systems, which let people access their email boxes through a Web browser, present their own problems. They expose organizations to vulnerabilities in Microsoft’s IIS engine, as well as in Exchange. For DTAE’s Exchange Webmail servers, IronMail defends against cross-packet attacks, directory traversal, path obfuscation, shell access, database access, directory attacks and more.

IronMail is easy to administer

“IronMail is completely transparent to the end user – and we didn’t have to go to every machine and put on software,” Catron comments. “With the power of the IronMail boxes, we could run our entire agency on just a few of them, but we opted to put an IronMail box at each main site. That gives the individual colleges complete control of their security configuration.”

“With IronMail protecting us, we also have a little more breathing room to install critical patches on servers and workstations,” Catron says. “Instead of being forced to make changes quickly, on 35 geographically dispersed sites, without a chance to test or understand the impacts on our production environment, we have the opportunity of doing real change control and choosing when to make the upgrade.”

Catron adds, “The statistical information we glean from IronMail is extremely valuable. There have been occasions where we have found problems just from scanning the nightly reports. And support is excellent. We’ve requested features that have become standard in the product within 90 days. We’ve never worked with another company with that kind of flexibility. We’re so spoiled now with IronMail, it’s hard to think about the time when we didn’t have it.”

Results

The IronMail comprehensive security solution now protects 35 critical DTAE email servers, assures privacy for sensitive email content, and guards DTAE’s 35,000 networked workstations – while providing highly effective spam reduction.

About CipherTrust

Headquartered in Atlanta, CipherTrust Inc. is a global email security company, setting new standards in the development of comprehensive security solutions for enterprise email systems. The company’s IronMail™ appliance is the only product on the market offering an integrated set of best-of-breed security solutions, including spam protection, virus prevention, intrusion detection and flexible policy controls. CipherTrust’s IronMail provides a secure email gateway for the enterprise, and earned PC Magazine’s Editors’ Choice Award for corporate anti-spam tools. For more information about CipherTrust, visit www.ciphertrust.com or call 877.448.8625.

