



eEye Digital Security®

## Central Florida Educators Federal Credit Union Switch to Blink

### The Challenge: Finding Strong Endpoint Security that Doesn't Hinder End Users

The Central Florida Educators Federal Credit Union (CFE) was having problems with its endpoint security. CFE has 16 branches in four central Florida counties. Each branch has 15 plus workstations that connect back to servers at the CFE headquarters in Lake Mary.

At the time, their existing endpoint security from Symantec was causing problems. First, CFE end users noticed that their machines were increasingly slow. A quick check of the Task Manager showed high CPU usage tied to Symantec.



#### Customer:

Central Florida Educators  
Federal Credit Union

#### Fast Facts:

Headquartered in  
Lake Mary, Florida

16 branches across  
Central Florida

700+ end nodes, 100  
servers

Transitioning to desktop  
virtualization along with  
dumb terminals at several  
branch locations

#### Key IT Challenge:

finding an integrated  
security suite that protects  
robust endpoints, such as  
workstations, while protec-  
ting servers and virtualized  
computing environments

[www.mycfe.com](http://www.mycfe.com)

Next, when the software was updated, old installations often failed to uninstall and created software conflicts, with many unrelated applications failing to work. Finally, Symantec burdened end users with alerts and false alarms.

For a small IT staff, these constant problems took too much time away from other IT projects. For instance, CFE is in the process of rolling out a desktop virtualization effort. At one of CFE's smaller branches, they have already installed dumb terminals connected back to hosted desktops, but constant security troubleshooting has kept them from being as far along on this project as they would like.

Hosted desktops promise to lower capital and operating expenses, while also giving IT greater control over desktop management. While hosted desktops are currently used at one location, CFE is hoping to convert more branches to this computing model soon.

Aside from simply finding time for this project, moving to hosted desktops adds yet another concern: security. Security for hosted desktops must absolutely protect against zero-day threats. Otherwise, an infection on a single server could cripple an entire branch or even the entire organization.

#### The Selection Criteria:

##### Boosting Security without Breaking the Budget

CFE decided it was time to upgrade their security. Moving to new computing models meant that the security of the past just wouldn't keep up. However, if they were going to sink their resources into a full-scale switch of security vendors, they decided they should make it a priority to get more security features per dollar.

The first additional feature CFE wanted was the ability to gain visibility into what was happening on end devices. Since the banking industry is heavily regulated, they also wanted a security suite that would simplify reporting and auditing for compliance.



CFE didn't want to overlook its initial concerns of resource consumption, interoperability and false positives in order to get added features. In addition to the new features, the existing features needed to be in place and handled better than before.

Finally, CFE wanted to move away from signature-based security. With all of the computing changes happening at the organization, CFE needed zero-day protection.

With the criteria in mind, CFE first considered staying with their existing security vendor, Symantec and updating to the newest security suite offering. This option was quickly dismissed because it didn't offer the range of features they sought. Next, they considered Cisco's endpoint security. While Cisco offered improved endpoint security and a broader feature set, the software was simply too expensive.

CFE then investigated the Blink Endpoint Security solution from eEye Digital Security.

## The Answer: eEye's Integrated Threat Management Solution

eEye's Blink Endpoint Security is a comprehensive security suite that was able to offer everything CFE was looking for: zero-day protection, centralized and behavior-based management, rather than signature-based, protection - all at a much lower price than competing solutions.

"We tested security suites head-to-head," said Ian Thompson, network specialist for CFE. "We looked at cost, speed, security strength, the feature set, and more, and eEye came out ahead in every category. For instance, we tried to exploit systems with malware. Other vendors allowed some types of malware to slip through to the endpoints. eEye Blink, on the other hand, stopped everything we threw at it."

Blink protects client devices by identifying behaviors, not signatures. Offering integrated multi-layered endpoint protection, Blink is a single, lightweight client that replaces multiple security agents, protecting against known exploits, zero-day attacks, and all other attack vectors.

"In this economy, everyone has a tight budget. Blink, with its many advanced security features and low price point, is the perfect fit for us. With Blink we get strong, flexible security that goes beyond traditional signature-based protection. Being a financial institution means you're a prime target for cyber-criminals. If you rely on signatures, you're vulnerable to whatever new attacks those criminals think up. We could no longer risk trusting signature-based security," Thompson said.

### The Hidden Benefits of Blink

Once in place, Thompson noticed some less obvious benefits of Blink in addition to the ones they were initially looking for. While eEye offers a full-blown network vulnerability assessment tool, smaller organizations often make use of the endpoint vulnerability scanner built right into Blink, which then coordinates those findings back to REM, the security management console from eEye.

## Key Benefits:

Zero-day protection

Quarantining of suspicious machines

Policy creation and enforcement

Antivirus protection

Visibility into endpoints

Centralized security management

Reporting and auditing



eEye Digital Security®

To learn more, please visit [www.eeye.com](http://www.eeye.com)  
or call 866.282.8276





“Staying current with client-side applications is a major concern. We knew we needed a better way to look at applications and determine whether they needed to be updated or patched,” Thompson said. “With Blink we get detailed information about which vulnerabilities are the most pressing, and in the meantime, we know we’re protected until we update and patch.”

Blink offers a number of protections against application vulnerabilities. Blink provides system protection, giving IT control over which applications are allowed to function by authorizing or denying program file execution. Blink also protects at the registry level, preventing specific registry settings from being modified, thus stopping malicious programs from infecting or modifying systems.

Blink also leverages a host-based intrusion prevention engine that dynamically collects and incorporates new threat data in real-time.

This protection gives IT professionals like Thompson the ability to prioritize the vulnerabilities that require the most immediate action and the confidence that endpoints are protected until patching is completed. “The fact that a client vulnerability assessment tool is built into Blink was icing on the cake,” Thompson said. “I figured we’d be paying for an entirely separate product to get that capability.”

### **Moving Security away from End Users to IT**

With traditional endpoint security, end users are responsible for much of their own protection. CFE’s employees, for instance, often received alerts from Symantec when something was amiss.

“We didn’t gain anything by alerting end users other than scaring them,” Thompson said. “Now, with Blink we are able to run it in silent mode for end users. When something triggers an alert, IT checks it out first.”

With IT taking control of security, end users have the beneficial experience of not having security get in the way of their normal workflows. “Blink is pretty transparent for end users,” Thompson said. “Even for our power users, they barely notice Blink. The only thing they notice is that security is taken care of for them, and they can go about their business without being afraid of viruses, phishers and other security threats.”

***“Blink, with its many advanced security features and low price point, is the perfect fit for us. With Blink we get strong, flexible security that goes beyond traditional signature-based protection.”***

***- Ian Thompson, network specialist,  
Central Florida Educators Federal Credit Union***

## **Other Key Benefits:**

Automated notification when problems occur

Streamlined incident response

Transparent to end users

Centralized security management that provides a single point of visibility into and control over the network

Offers remote administration features, so updates don’t require manually visiting each PC

Ability to apply policies to USB storage devices



eEye Digital Security®

To learn more, please visit [www.eeye.com](http://www.eeye.com)  
or call 866.282.8276

