



## Mitigating Mobile Access Risk

*This anti-fraud services provider needed a way to enable its mobile workforce to access the corporate network securely from anywhere they need to work.*

When thinking about fraud prevention, the word collaboration probably isn't one of the first things that come to mind. But for this fraud prevention services provider, it's the driving force. With more than two decades of experience, this company is a trusted resource for strategic fraud management for financial services organizations (FSOs) around the country. The company achieves this through the secure exchange of information between FSOs. Through this collaborative model, the organization provides a single view of fraud activity to its participants.

Keeping all of that information confidential and ensuring that it remains unchanged, with its integrity intact, is vital. To keep its systems secure, the firm follows industry security best practices and technology: firewalls, virtual private networks, anti-malware applications, and continuous vulnerability management. Yet, no matter how secure and compliant a network is maintained, Trojans, bots, keystroke sniffers – eventually can make their way onto the corporate network. In fact, a single Internet-connected system that falls out of security policy, or a remote user whose defenses are not up to grade to connect to the corporate network is all it takes for a breach.

### Secure Remote Access

That's why this security manager sought a way to ensure that only systems that should connect to the corporate network did so, and that they also were up to date and within the company's security policy. "We wanted only authorized equipment on our network," says the company's security manager. "And we wanted to be able to validate that only authorized systems, with the proper security posture, could gain access," he says.

Most of the firm's 240-plus employees are mobile and many work from home. "We operate as a very lean, high-paced company. Everybody is equipped with laptops and can access the network remotely. That's why it was so crucial to have to ability to make certain that people weren't using their home PCs, and that only equipment that was assigned and up to policy was used for remote access," he says.

### EXECUTIVE SUMMARY

#### Corporate Overview

**Scope**

International

**Business**

Provides fraud detection services to financial services and other organizations.

**Size**

240 employees

**Business Problem**

Ensure only authorized, secured devices connect to the business network

**Solution**

InfoExpress CyberGatekeeper Remote and Dynamic NAC

With those objectives in mind, the company evaluated a number of possible solutions, including the Network Access Control (NAC) offering from their network equipment provider. "We had a consultant put together a number of options, and we were going down the path of a large-scale proprietary infrastructure NAC solution. But, during our consideration, it turned out to be very cumbersome, and appeared very difficult to manage," he says. "It would have required a substantial amount of hardware and significant changes to our switches," he says. "By the time services were estimated, the total expense would have been well into six figures," he says.

That first option was more expensive than the company had planned to spend. It also called for more network configuration and management than it wanted to contend with. Another option was CyberGatekeeper Remote, for VPN enforcement and CyberGatekeeper with Dynamic NAC for LAN enforcement, both developed by network security provider InfoExpress.

**"With all of the dangers that face systems today, it's essential to have the ability to keep systems up to date and operating within security policy. Turning to CyberGatekeeper with Dynamic NAC turned out to be a great move for us."**

– security manager

### Zero Network Change Network Admission Control

CyberGatekeeper with Dynamic NAC (DNAC) is a Network Access Control solution for LAN enforcement that requires no network changes, making it many times easier and faster to deploy than other out-of-band NAC solutions. CyberGatekeeper continuously checks all devices on the network and offers centralized management, flexible policies, granular quarantining and monitoring, and remediation of unhealthy systems. CyberGatekeeper can also be installed within hours. Because there is no need to change the network or update network devices, CyberGatekeeper doesn't require expensive network upgrades. "It quickly became apparent that CyberGatekeeper with DNAC would fit our needs exactly. It was not only less expensive, but easier to manage. It didn't require reconfiguring switches and messing with port settings. CyberGatekeeper goes on the network, the system finds all of the systems, and it makes sure that they are compliant," he explains.

"The deployment went very smoothly," he says. "Essentially, it's a small agent that is installed on some of the endpoints in addition to connecting the server. I didn't have to hire a consultant, and we had it running within a day," he adds.

The InfoExpress' CyberGatekeeper Server appliance hardened the existing network by allowing access only to authorized devices and reporting and blocking rogue endpoints. Noncompliant endpoints are quarantined until remediation brings them back into compliance. CyberGatekeeper supports multiple NAC methods for managing access to the network: the CyberGatekeeper with DNAC enforcement that requires no changes to infrastructure or equipment; 802.1x NAC, which uses VLANs; and in-line NAC, which relies on a bridge to filter traffic. Users can be authenticated using 802.1x or Windows domain logon and attain automated and interactive remediation and continuous validation of endpoint compliance. All configuration changes and policy updates are managed centrally. "If I have a rule update, it's very easy to send that out to the employees," he says.

CyberGatekeeper with DNAC hardens existing networks by making some of the PCs “enforcers,” through the lightweight software agent that monitors and controls access to the network. Enforcers report and quarantine unauthorized devices, like rogue endpoints and unhealthy PCs. The unhealthy PCs can rejoin the network after automatic or manual remediation brings them into compliance.

### **Persistent Security Policy Enforcement**

Now, employee systems always are vetted for proper security posture, and only those that are at proper levels are admitted. For instance, if a user's anti-virus signatures are out of date, they're sent to a custom page for remediation. The company also now is able, through CyberGatekeeper enforcement, to make certain that all notebook drives are encrypted using McAfee SafeBoot, which also reduces the risk associated with data leaks by limiting user ability to transfer data to USB storage devices. “During the initial installation, we quickly identified a number of conditions we didn't expect, such as systems running without anti-virus software or with unencrypted drives,” he explains. “These were great catches,” he says.

Today, as a result of the deployment, the company has attained its goal of ensuring that only authorized and compliant systems connect to the network. Remote and internal systems alike are maintained to a much higher degree of security. For instance, CyberGatekeeper audits all networked systems continuously for policy compliance. Systems that don't meet an acceptable level of compliance are delayed access to the network, and directed for remediation. InfoExpress CyberGatekeeper with Dynamic NAC continuously monitors the network for noncompliant systems and quarantines unauthorized devices while also providing the firm automated and interactive remediation. In addition, security managers benefit from centralized endpoint policy management and comprehensive status reports.

“With all of the dangers that face systems today, it's essential to have the ability to keep systems up to date and operating within security policy,” he says. “Turning to CyberGatekeeper turned out to be a great move for us.”