



CyberGatekeeper: The Verdict Is In

When this legal services not-for-profit started assessing the NAC market, it seemed all of the solutions were costly and cumbersome to deploy and manage. Fortunately, further investigation proved otherwise.

If you live in Georgia and are in need of legal advice but can't afford representation, one of the first places you'd turn for help would be to the Georgia Legal Services Program. Georgia Legal Services provides legal services and counsel to low-income individuals and families from 11 offices throughout the state. Its lawyers and paralegals offer the help that reflects the community's values of fairness, equality, and responsibility to assist those in need. Some of the special legal projects this nonprofit undertakes include the statewide Domestic Violence Project, the Landlord/Tenant Housing Helpline, the Migrant & Seasonal Farm Workers Helpline, the Homeless Legal Assistance Project, and many others.

To fulfill its mission, Georgia Legal Services makes a variety of legal software applications and e-mail access available for its employees and guests. Not surprisingly, many of its users, who include numerous legal students, access these services remotely through a virtual private network (VPN). With such a diverse and decentralized group of workers accessing its systems from essentially anywhere, making certain that its network, applications, and sensitive client data remained secure was growing more essential.

Georgia Legal Services also had users accessing its network from unauthorized personal and home computers. "Managing our remote users was becoming more of a priority for us," says Joseph Mays, director of IT, Georgia Legal Services. "Many of these remote systems were not being kept compliant with our security policies and we had students running various applications, such as peer-to-peer and instant messaging clients, that we wanted to control and block to prevent malware from seeping in," he says.

That's no minor task. The threats from Web and Internet-borne viruses, spyware, and other forms of malware aren't slowing.

EXECUTIVE SUMMARY

Corporate Overview

Georgia Legal Services Program

Scope

Georgia Legal Services Program provides access to justice and opportunities out of poverty for Georgians with low incomes

Business

Not-for-profit

Size

Twelve locations throughout state of Georgia

Business Problem

Ensure remote user systems accessing primary network were authorized, within security policy, and clean of infection.

Solution

CyberGatekeeper with Dynamic Network Access Control (DNAC)
CyberGatekeeper Remote

Investigating the NAC Alternatives

When considering ways to protect the organization's network, Mays concluded that Network Access Control (NAC) held promise. Through a NAC solution, remote systems could be vetted before being granted access over the VPN. Through NAC, Mays hoped, Georgia Legal Services could enforce that certain security applications such as anti-virus were up-to-date, patch levels were recent, and that risky applications such as P2P networks and messaging clients were not installed.

Unfortunately, when Mays began investigating potential NAC options, the concept – at first – looked as if it would be better in theory than in practice. "One of the first things that threw us was that they required substantial network configuration changes, including switches having to be installed at each remote location," he says. "That was obviously quite cost prohibitive for us."

As a not-for-profit, Georgia Legal Services can't make mistakes on its IT investment: every purchase must count. "We needed something that was affordable, easy to manage, and wouldn't require big changes to our network," he says.

The Jury Has Its Verdict

That's when, through its study of the market, Georgia Legal Services came across InfoExpress, Inc. and its CyberGatekeeper with Dynamic Network Access Control (DNAC) and CyberGatekeeper Remote solutions. "It seemed as if CyberGatekeeper would provide exactly what we needed, at a cost that was significantly lower than all of the others we looked at," he says. "With CyberGatekeeper, everything fell into place. It was cost-effective, we didn't have to alter our existing network, and it would achieve the level of control over our security policies that we wanted," he says.

"CyberGatekeeper is one of those products that once it's implemented, you really don't have to do anything. You create the policies, make sure they're enforced, and forget about it."

– Joseph Mays, director of IT, Georgia Legal Services

Once the decision to select CyberGatekeeper was made, Georgia Legal Services was able to quickly deploy the CyberGatekeeper solution, relying on only remote support from InfoExpress. "The technical support team was extremely responsive and helpful throughout the deployment process," says Mays. Other vendors required an on-site engineer to be dispatched to set up their product, as well as up to three days of billable training. With CyberGatekeeper DNAC and Remote, that training and on-site support was optional. "We were able to install centrally, without having to travel to our remote offices. Once the policy servers were in place and the policies created, it was literally as simple as putting the CyberGatekeeper Agent onto a couple of endpoints on each subnet and pushing the policy out to the two policy servers," Mays explains.

"We then watched to see that all the endpoints were compliant and then we enforced the policy," he adds.

CyberGatekeeper Proves Its Case

Because CyberGatekeeper DNAC requires zero network changes, it's many times easier and faster to deploy than other NAC alternatives. CyberGatekeeper offers centralized management, flexible policies, granular quarantining and monitoring, and remediation of unhealthy systems. As a result, Georgia Legal Services' remote and internal systems are maintained today to a much higher level of security. For instance, CyberGatekeeper Remote audits all networked systems continuously for policy compliance. Systems that don't meet Georgia Legal's level of compliance are denied access to the network, and directed for remediation. At the same time, the CyberGatekeeper Server monitors the network for threats and non-compliant systems, and quarantines unauthorized devices while also providing automated and interactive remediation.

Once installed, the Georgia Legal Services IT team isolated a considerable number of systems that were placing themselves and the non-profit at risk. "We had many applications that lowered security that we just didn't know about," Mays says. CyberGatekeeper revealed that 60 percent of Georgia Legal Services' systems were out of compliance. "Previously, we just had no way to peer into the infrastructure and look," he adds.

CyberGatekeeper also has proven itself to increase security by immediately stopping attacks. "We had several instances when fake anti-malware applications were downloaded. That software managed to disable the anti-virus software on the computer, but CyberGatekeeper identified the threat and safely quarantined the desktop off of the network," he says. In addition, users can't access Georgia Legal Services' network from their home-based, or other untrusted, PCs: only Georgia Legal Services sanctioned devices gain entry.

Today, all of the systems that access Georgia Legal Services' network are checked to make certain that they're permitted and up to policy, and that they're not infected with malware and have in place the proper security settings – patch, anti-virus levels, and others. They also can ensure that systems aren't running banned applications, such as peer-to-peer clients. "It's just incredible now that we can keep that stuff off of our network," he says.