

InfoExpress CyberGatekeeper: StayinFront Customer Case Study



StayinFront Uses CyberGatekeeper Endpoint Policy Enforcement to Secure Remote Access

StayinFront, Inc. is a leading global provider of world-class enterprise-wide customer relationship management (CRM) applications, decision support tools, data services and eBusiness systems. Its flagship CRM platform manages and integrates all points of customer interaction including sales, marketing, customer support applications and the web. The system can be seamlessly delivered through multiple applications simultaneously; across a network, via the web or through a remote, disconnected field force. StayinFront solutions have been deployed in more than seventy pharmaceutical companies in over twenty countries in twelve languages.

Challenge: Enabling Easy but Secure Network Access

StayinFront's network operations center houses its Sales CRM, development and support servers. StayinFront remote users synchronize, and perform job responsibilities via remote access connections.

These remote users spend long periods of time off the network, often falling into varying degrees of quality from a configuration and stability standpoint leaving them vulnerable to malicious code attacks. In order to maintain control, StayinFront IT has instituted a strict security policy for all remote access users. It requires the use of an SSL VPN, updated anti-virus software and the applying of Microsoft OS security patches.

"We knew we had the right baseline security policies in place to prevent a worm outbreak via an infected laptop," said Michael Fredericks, manager of IS for StayinFront. "What we lacked was a way to enforce internal compliance measures on the laptops. It was a real challenge."

Fredericks estimated network downtime due to a mass infection could mean a loss of productivity for as many as 80-90% of StayinFront's employees. Not a risk StayinFront management was willing to take; they quickly moved to find a tool that could plug this potentially disastrous security hole.

Solution: CyberGatekeeper Remote Appliance

Research into an enforcement tool led StayinFront to InfoExpress and the CyberGatekeeper Remote solution.

"We read an InfoExpress customer case study and saw the situation was similar to ours," said Fredericks. "CyberGatekeeper was one of the first products we evaluated. We plugged it in, and it quickly demonstrated it would meet all of our requirements and more."

CyberGatekeeper actively enforces policies by auditing the configuration on remote access laptops before they are allowed to connect to the network. The user of any device deemed non-compliant is notified to contact the StayinFront help desk.

According to Fredericks, "The best way we know CyberGatekeeper works is when we get a call from one of our users with an infected, misconfigured or unpatched system." He continues, "The user is quickly sent to a special remediation library where they apply the necessary updates or patches."

Results and Recommendations

Success within the sales department has prompted StayinFront to deploy CyberGatekeeper to other employees, including engineers. The technology is also being tested on several customers who access StayinFront's CRM servers. StayinFront has also acquired the CyberGatekeeper LAN solution to help secure endpoints existing inside their perimeter firewalls.

According to Fredericks, "At StayinFront, our hardware services team deploys CyberGatekeeper in all our equipment. This has significantly reduced the risk of viruses or infections attacking laptops, handheld PCs and other devices along with our servers.

CyberGatekeeper has proven to be a valuable asset to our security process, helping alleviate potentially expensive and timely disruptions to our network operations."