

InfoExpress CyberGatekeeper: Anonymous Food Production Case Study

Extending Solid Network Security Practices to the Endpoint

The Background

This customer is the world's largest protein food producer based in the U.S. with over \$25B in annual sales and over 100,000 employees. Its brands are well known by consumers globally. The main point of contact for this sale was the company's Director of IT Security.

The Challenge

As with many large enterprises, mobile computing has become an essential tool for employee productivity. The customer's project focused on providing 2,000 Sales mobile employees with corporate-issued laptops that included full remote connectivity services. Mobile workers could connect to the corporate network via dial-up, broadband, standard Ethernet and wireless. The Windows-based laptops were also secured with either a standard IPsec or SSL VPN.

In recent years, the company suffered through several malicious code attacks to their network, with large-scale infections that interrupted business operations. In the aftermath of one attack, a five-person team worked over a month to clean up infected machines. The company realized that mobile devices were extremely vulnerable to such worm attacks they exploited vulnerabilities in Microsoft software. An offline unmanaged laptop could become infected, mis-configured, or fall out of policy compliance and upon re-connection to the network could spread a destructive viral payload to hundreds and thousands of systems in a matter of minutes. The cost to the company in terms of computer downtime, loss of productivity, and clean up efforts had totaled in the hundreds of thousands of dollars per each virus episode.

The bottom line challenge for this client was to get tough on non-compliant endpoints, and to make sure mobile laptops include a capability to scan, inspect and if necessary, clean systems before they are allowed onto the corporate network. Additionally, the company was looking for a solution that was easy to deploy and manage so it could be expanded rapidly to other employees.

The Solution

After ruling out personal firewalls and some basic services offered by the connection service provider, InfoExpress was invited to present CyberGatekeeper, the industry-leading endpoint policy enforcement solution.

In 45 days from when the customer was first introduced to CyberGatekeeper, the customer decided to purchase CyberGatekeeper Remote. CyberGatekeeper appliances were operational in less than two weeks after installation. CyberGatekeeper was the only solution on the market that could meet these strict customer requirements:

- Integration with the customer's remote access services provider
- Easy to deploy and manage
- Flexibility to scan machines against corporate policies governing anti-virus and Microsoft OS updates.
- Ability to quarantine and remediate them through patching of non-compliant systems.
- As part of the remediation process, the customer needed to be able to control customized messages to users. They wanted users to be able to delineate a message coming from their IT support versus a standard Windows-based message.
- Ability to monitor devices once they are connected to the network.

Results and Recommendations

The customer is 100% satisfied with their CyberGatekeeper solution. In 45 days from the time they were introduced to CyberGatekeeper, they were able to enforce policies on the 2000 endpoint laptop computers. Machines that were infected, mis-configured, or non-compliant were restricted from corporate network access. CyberGatekeeper was also used to auto remediate those machines that required software updates. With CyberGatekeeper serving as a solid base for enforcing better network security, the enterprise feels more confident in protecting their network and expanding their mobile computing practices.