Case Study
Global food manufacturer enlists CBTS for a network security upgrade to minimize potential risks

Client

Global food manufacturer

A global food manufacturer headquartered in Canada manages more than 100 sites globally, each with advanced perimeter security controls. The company's IT team had access to security support only from 8 p.m. to 5 p.m., creating a critical support gap.

Challenge	CBTS solutions	Results
• The food manufacturer did not want to hire full-time security experts for sporadic threats. • With over 100 sites globally, its IT team had access to security support only from 8 a.m. to 5 p.m., leaving it vulnerable to attack. • It needed an experienced security partner with 24x7x365 support without the cost of hiring, training, and retaining an entire security team.	• The company partnered with CBTS to upgrade and secure its global network. • CBTS provides around-the-clock security support for the company's IT network operations and offers an online client portal allowing the IT team to request support and address threats. • CBTS upgraded firewall management and security technology. • CBTS expanded network logging and monitoring with enterprise-grade security information and event management technology alarms.	• The company delegated its network security to the seasoned experts at CBTS, avoiding the expense of staffing full-time security support. • The online client portal allowed CBTS to immediately address dozens of potential security threats. • 99% of the network's security devices were upgrade to the latest FortiOS technology after significant vulnerabilities were identified in 40 machines.

Contact us today at 1.866.587.2287 | cbts.com

Infrastructure, covered

Challenges

The company needed an economical alternative to hiring full-time security experts to provide around-the-clock support for sporadic threats of unpredictable severity while increasing security event visibility and alerting. With a limited pool of network security expertise at its Canadian headquarters, the company manages more than 100 sites globally, each with advanced perimeter security controls.

Though network operations ran nonstop, its IT team had access to security support only from 8 a.m. to 5 p.m. This created a critical support gap—hackers do not keep regular business hours.

The company was also running a patchwork of multiple versions of their FortiGate unified threat management solution, creating substantial potential for security breaches. It needed to migrate its firewall technology to more robust software.

The client wanted an experienced security partner to ensure 24x7x365 enterprise-level security without incurring the cost of hiring, training, and retaining an entire security team.

CBTS solutions

The company partnered with CBTS to upgrade and secure its global network. The project had three primary goals: provide around-the-clock security support for IT network operations; upgrade firewall management and security technology; and expand network logging and monitoring.

CBTS developed a solution to address the company's business objectives and security challenges. CBTS initiated the project with an assessment of the company's current environment to help determine the best ways to upgrade its security while reining in IT expenses. Based on the upfront analysis, the project included:

- **An online client portal** enabling IT professionals to request support and address threats
- **Upgrading the client's network security** software to the latest FortiOS operating system and device onboarding for its FortiGate network security appliance, as well as migrating to Cisco ASA firewall technology

- **System monitoring** with enterprise-grade security information and event management (SIEM) technology alarms to alert key users of security threats and filter out network "noise," which prevents wasteful false alarms
- **Security logging enhancements** including scheduled SIEM upgrades to maintain and enhance performance

Results

CBTS completed full onboarding, including the network security upgrade, and had everything up and running within 90 days.

Here's a look at what was accomplished:

- **Online Client Portal:** In the first six months, the new portal enjoyed excellent uptake from users—77% of support tickets were opened directly in the portal, with the rest coming in via email and telephone. More than two-thirds of the 84 support tickets involved potential security threats that could be addressed immediately rather than delayed until support people were available.
- **Device Onboarding:** 99% of the client network's security devices were running gold standard FortiOS Version 5.0.1. Before the upgrade, the company's systems were running eight different versions of FortiOS, creating

substantial potential for security breaches. Significant vulnerabilities were identified in approximately 40 machines.

- **Monitoring and logging:** The new system provides 24x7x365 monitoring and reporting.
- **SIEM alarms** can be assessed, and if the risk is serious enough, it can be reported to the company's global service desk. The enterprise SIEM environment helps experts tune out "noise" that produces false alarms and helps focus on the most dangerous threats.

By joining forces with CBTS, the company delegated its network security to seasoned experts and avoided the expense of staffing a security support desk around the clock. When intruders try to break in, world-class security technology is poised to minimize the threat.