Case Study: Town Police Department

Background

A police department needs to secure the computers used by police officers at the department and in their patrol cars.

Officers' laptop computers are used mostly in their patrol cars, for filing incident reports, for handling citizens' documents, and for sending and receiving emails and attachments. From the patrol cars, the computers connect to the department network via VPN.

These laptops have experienced cyber-attacks in the past.

The Challenge

Officers need to be able to securely connect to the internet, and to handle citizen documents received via email or USB.

The police officers' laptops connect from their patrol cars to the department network VPN, which is enforced. However, the department's information security office knows from experience that this does not ensure security to the laptops themselves, and the connection to the department network risks sensitive systems as well. A more secure solution is required.

At the same time, the desired solution cannot disrupt important, time-sensitive police activity in the field. Officers need to be able to receive documents by USB and email and to maintain them in police systems.

The Solution

The Police Department Chief Information Security Officer (CISO) investigated several security solutions, including BUFFERZONE®.

BUFFERZONE provides automatic containment and isolation of processes that access data from unsecure sources, including browser downloads, email attachments from external sources, and removable storage (USB). BUFFERZONE also includes SafeBridge™, allowing content to be extracted from the container via a secure process of Content Disarm & Reconstruction (CDR), so that only sanitized content can reach the rest of the computer operating system and sensitive department systems and resources.

The CISO decided to deploy BUFFERZONE to the department laptops. BUFFERZONE will enable officers to freely access the internet, receive emails and attachments, and copy files from removable storage devices. Any possible malware, including zero-day attacks, will be isolated and periodically wiped from computers; needed documents will be sanitized by SafeBridge. And officers do not need to change the way they work.

Benefits for PD

- Safe browsing
- Safe email and attachments
- Safe removable storage (USB)
- Protects from malware including ransomware and zero-day exploits
- Transparent user experience
- Low resource consumption, fast performance
- Easy to deploy
- Cost effective