BUFFERZONE

Israel National Insurance Institute (Social Security)

Background

The National Insurance Institute of Israel (NII) was founded in 1953 to provide short and long-term financial support for populations in need. Today, The NII offers a wide variety of programs, such as old-age, maternity, children, work injury, general disability, long-term care, unemployment, income support, bankruptcy and liquidation of corporations.

In order to run their programs, the IT department needs to process and protect a great deal of personal information. The NII is constantly looking for ways to improve the service they provide to the public, while ensuring data privacy and the security of their network.

The Challenge

The department that reviews accident claims needed to routinely process medical information, including very large imaging files provided on removable media such as a CD or USB memory stick. It was clear that connecting removable media to computers on the NII network posed a significant security risk.

In addition, the department wanted to reduce waiting time by enabling citizens to upload personal files through a self-service kiosk. They needed to ensure that files uploaded through the kiosk did not introduce malware onto the network.

NII looked for a security solution that would enable them to accept personal files on both employee endpoints and self-service kiosks through removable media, without putting security and privacy at risk. Since there are many branches and there isn't always an IT organization on site, they needed a solution that would be as transparent as possible to users, and easy to manage throughout the country. From the IT perspective, the solution needed to support both their Windows 7 and legacy Windows XP endpoints, and be managed using Microsoft GPO without frequent signature updates.

The Solution

The NII evaluated BUFFERZONE Advanced Endpoint Security at one of their branches. Within a matter of weeks, they had installed it on the employee PCs that were used to accept data for medical claims, and on the self-service kiosks.

When an accident investigator opens a CD or USB memory stick, it opens inside the BUFFERZONE virtual container. From the employee's perspective, the files open normally. But behind the scenes, the files are opened in an isolated environment. If malware is present on the CD or USB memory – either intentionally or unintentionally – it will be downloaded to the container, where it cannot infect the rest of the endpoint or access the NII network. After the investigators complete the review, the medical files are simply deleted. There is no need to remove them from the BUFFERZONE container. With BUFFERZONE, the investigator's endpoints and the National Insurance network are protected from malware and zero-day exploits at all times.

Americas: +1 646 432 6848 | EMEA: +972 3 6444012

BUFFERZONE

> BUFFERZONE is an excellent solution for our employees – it enables them to get the job done, while keeping the network secure.
>
> Aviv Hasidim,
> Internet and IT Security Manager at NII

"BUFFERZONE is an excellent solution for our employees – it enables them to get the job done, while keeping the network secure," said Aviv Hasidim, Internet and IT Security Manager at NII.

Following the successful deployment of BUFFERZONE on the investigators PCs, NII installed it on the self-service kiosks. The self-service application runs inside BUFFERZONE so that all uploaded files are isolated from the rest of the organization. Before transferring the files to investigators for follow up, they are processed with the BUFFERZONE Bridge to ensure that they are free of malware or any active content that could be malicious.

BUFFERZONE was simple to manage on all of NII's Windows 7 and Windows XP devices using Microsoft GPO, their in-house endpoint management platform. It is part of a comprehensive security program including TrendMicro's OfficeScan. "The services team at BUFFERZONE helped us to get up and running quickly. The solution doesn't require updates and is nearly invisible to our employees, so we rarely need support," Says Mr. Hasidim.

Benefits for NII

- Enable safe use of CDs and removable storage
- Secure uploads at self-service kiosks
- Prevent malware from infecting employee endpoints and the network
- Enable investigators to work productively
- Protect both current and legacy versions of MS Windows
- Safely transfer information into the organization without compromising security
- Deployment within hours, very easy to manage
- Minimal resource utilization

Americas: +1 646 432 6848 | EMEA: +972 3 6444012