# Case Study: Clal Insurance

## About Clal

Clal Insurance Enterprise Holdings is Israel's leading insurance, pension and financial services group. Founded in 1987, it owns insurance agencies, pension funds, provident funds and study funds. It has over 4,500 employees and works with over 2,000 insurance agents.

Along with the rest of the banking and insurance industry in Israel, Clal is subject to strict government regulation regarding data security and privacy. Clal must ensure that customer data is segregated from the internet, to prevent data privacy breaches. At the same time, it is essential for Clals' thousands of employees to use the internet daily in order to provide quality customer service.

## The Challenge

Clal's IT organization needed a solution for secure internet access that complied with the industry regulations. Clal's employees are a highly diverse group with different internet requirements and technical skill levels, so it was essential to find a solution that was transparent to the end user. At the same time, there were a number of endpoint configurations at various sites, so it was also important that the solution be easy to deploy, configure and manage centrally.

In the past, Clal segregated the internet from the local network using a local virtual machine image that ran on every user endpoint. Employees could only access the Internet through the virtual machine. This solution suffered from poor performance, high maintenance and costly replication of software licenses. The user experience was slow and awkward, and at times the PC did not behave as expected, resulting in IT support calls. So Haim Inger, Chief Technology Officer at Clalbit Systems, started looking for another way.

## The Solution – BUFFERZONE Advanced Endpoint Security

In 2012, Clal was introduced to BUFFERZONE Advanced Endpoint Security. BUFFERZONE uses patented virtual container technology to segregate applications that are accessing the internet from the rest of the endpoint and the network.

At Clal, employees browse the internet from inside the BUFFERZONE container. If they accidentally download malware, the entire exploit is confined to the container and cannot get out. But for Clal's employees, BUFFERZONE is invisible. Users can browse the internet normally, and do not feel any degradation in performance as they did with the old solution.

BUFFERZONE protects users from common viruses as well as advanced exploits such as drive-by downloads, malvertising and zero-days that take advantage of Java, Flash and other browser plugins. BUFFERZONE also provides network separation capabilities to ensure that on each endpoint, the internet communications are fully segregated from the corporate network. It runs locally on each endpoint and is centrally managed using the BUFFERZONE management server or a standard enterprise security management platform.



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

> We are aware of more than one targeted attack aimed at the financial sector in Israel that we avoided, most likely thanks to BUFFERZONE.
>
> Haim Inger,
> CTO, Clalbit Systems

"BUFFERZONE proved to be the optimal solution from both the IT and the end-user perspective," said Mr. Inger. "To our diverse user community, the solution is practically invisible and does not interfere with the way that they work. From the IT perspective, it is both easy to manage and cost-effective in comparison to the alternatives and it meets all of our security and compliance requirements. We are aware of more than one targeted attack aimed at the financial sector in Israel that we avoided, most likely thanks to BUFFERZONE."

Clal performed a rigorous pilot as well as penetration testing. They then immediately proceeded to a full roll-out on all 4,500 user endpoints. "The BUFFERZONE support team was always available to assist us," he added.

"Email is now our biggest attack surface," says Mr. Inger. Clal uses the latest solutions to scan email attachments for malware, but for companies in the financial services sector, that is not enough. "Insurance companies are victims of targeted attacks and that means our users are vulnerable to sophisticated social engineering. We have started using BUFFERZONE to contain email attachments from outside the company."

## Next Steps

Clal is starting to virtualize some of their endpoints and enable access from personal devices using Virtual Desktop Infrastructure (VDI). But just like physical endpoints, virtual endpoints are vulnerable to malware. Criminals access the VDI through internet applications like browsers, Skype, or email attachments, and from there, spread throughout the network. As a next step, Clal is planning to deploy BUFFERZONE on the VDI server to secure Internet access.

## BUFFERZONE Benefits for Clal

- Safe browsing and email attachments for over 4,500 employees
- Compliance with government security standards, including network segmentation, for insurance companies
- Protection from advanced malware, zero-day exploits and targeted attacks
- Transparent user experience and fast performance increased productivity
- Simple and cost-effective to deploy and manage saved hundreds of thousands of dollars compared to alternate solutions



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