Case Study: Global Semiconductor Manufacturer

Background

A global semiconductor manufacturing and design company, one of the world's largest, needs to secure its endpoints across the enterprise.

In addition to security concerns similar to those of other enterprises, such as the dangers of ransomware, zero-day exploits and other types of ransomware arriving via browsing sessions and email, the manufacturer has a specific need to securely download files, such as blueprints, from cloud storage via FTP. Documents are received also via unsecure USB removable devices and network shares. These too need to be securely accessed.

The Challenge

Enterprise employees need to be able to securely and comfortably connect to the internet, and to handle documents received via FTP, email, USB, and network shares. Those documents then need to be securely uploaded to organizational network resources.

Detection-based solutions are of course present, but the enterprise security officers know that these solutions effectiveness is limited, as they are dependent upon signatures from known malware variants and a limited set of identifiable behavior patterns. A more secure, proactive solution is required.

At the same time, the desired solution cannot disrupt important, time-sensitive business. Employees need to be able to receive documents via FTP, USB and email without interruption to regular work processes and to safely maintain them in organizational systems.

The Solution

BUFFERZONE® meets most of the enterprise's requirements naturally. BUFFERZONE provides automatic containment and isolation of processes that access data from unsecure sources, including browser sessions and downloads (Safe Browsing), email attachments from external sources (Safe Mail), removable USB storage, and network shares. Browsers can automatically switch between contained and uncontained sessions according

to site trust status.

BUFFERZONE also includes SafeBridge®, allowing content to be extracted from the container via a secure disarming process, so that only sanitized content can reach the rest of the computer operating system. The disarmed files can subsequently be securely uploaded to sensitive organizational systems.

For the secure FTP download requirement, BUFFERZONE recommended performing the FTP downloads via browser. In that context, the download becomes a regular browser download, and is secured by BUFFERZONE Safe Browsing.

Benefits for enterprise

- Safe Browsing
- Safe Mail
- Safe removable USB storage and network shares
- Protects from all types of local malware including ransomware and zero-day exploits
- Seamless user experience
- Low resource consumption, fast performance
- Easy to deploy
- No need for security expertise and event handling