

Navy Mine Warfare Training Center Prevents Data Leakage Explosions with Safend Protector

Ensure the Integrity and Security of Sensitive Data

“In my opinion, Safend should be considered the industry standard for endpoint data leakage prevention technology. As an information technology director, when you find a tool that you can't break - no matter how hard you try - that's a tool you keep in your tool box indefinitely.”

-Herb Armstrong, Director of Information Technology, The Navy Mine Warfare Training Center's

The Organization

The Navy Mine Warfare Training Center is the only training center that trains sailors for shipboard mine counter measures. While technology has a large part of the training the hands on sections bring home the safety and hazards to the forefront. The protection of data both in the areas of integrity and security are paramount to the training of American sailors.

The Challenge

The Navy Mine Warfare Training Center's Director of Information Technology Herb Armstrong anticipated the risk that portable devices such as USB thumb drives posed to the Center's security. "The last thing we need is to have data on mine warfare falling into the wrong hands. In our training classrooms for sailors, it is essential to ensure the integrity and security of the sensitive data used for instruction. Even one incident of data leakage would be disastrous for us," said Armstrong.

Herb knew he needed to find a solution that would enable him to seamlessly control data access via portable devices without impeding on instructors' abilities to access data for teaching purposes.

The Solution

In order to make the most informed decision, Armstrong set out evaluating 17 endpoint security solutions, including products from Symantec, McAfee, Microsoft and DeviceLock. After extensive testing, one solution stood out amongst the masses: Safend Protector. Says Armstrong: "Safend was the no-brainer choice to meet the Navy Mine Warfare Training Center's needs. Of the 17 products we tested, it was the only one that could not be bypassed because it is loaded at the kernel and since it is not loaded as a service, users can't shut the software off and circumvent the protection. The product was also very granular, making it easy to control access based on everything from device type to serial number. We found that it's impossible to beat from our testing - you know you have found the right solution when no matter how hard you bang on it, it won't break."

Safend also stood out from the pack because of the stellar level of individual, hands-on service it offered. "When you are evaluating - and ultimately deploying new technology - it's important to have a true partner there to support you along the way," explains Armstrong. "Safend's support technicians were there whenever I had a question. The level of service Safend offers was a major differentiator."

The Results

Armstrong and his team purchased 350 licenses of Safend Protector to guard against data leakage on nearly 850 ports throughout the Navy Mine Warfare Training Center. In addition to securing the USB port access that Armstrong originally intended the product for, he has also used Safend to secure WiFi, FireWire and game ports.

Since deploying Safend, the Navy Mine Warfare Training Center has not had a single incident of data leakage and has stopped unauthorized devices from accessing the network 285 times.

“From an information technology standpoint, one of our most crucial directives is to protect the sensitive data we work with on a daily basis but it’s impossible for me and my team to be everywhere, all of the time, monitoring endpoint access,” adds Armstrong. “Safend has become my eyes and ears at the point of impact across the organization. Any time someone tries to access data using an unauthorized device, they are automatically denied and I receive a detailed report documenting the incident. Safend also provides me with explicit logs of approved data access so I can see who downloaded what file from what endpoint, and when.”

In Conclusion

“In my opinion, Safend should be considered the industry standard for endpoint data leakage prevention technology,” comments Armstrong. “As an information technology director, when you find a tool that you can’t break no matter how hard you try, that’s a tool you keep in your tool box indefinitely. Safend has absolutely become an indispensable tool for the Navy Mine Warfare Training Center and I am excited to see the latest developments from the company.”

About Safend

Safend is a leading provider of endpoint data leakage prevention (DLP) solutions that protect against corporate data loss by offering comprehensive solutions for data encryption and port and device control. The Safend DLP Suite encrypts internal and external hard drives, removable storage and CD/DVDs and provides granular port and device control over all physical, wireless and removable media devices. Safend ensures compliance with regulatory data security and privacy standards. Safend solutions are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe. For more information, visit www.safend.com



Safend Ltd. 32 Habarzel Street Tel-Aviv 69710, Israel. Tel: +972.3.6442662 | Fax: +972.3.6486146
Safend Inc. 2 Penn Center, Suite 301, Philadelphia, PA 19102, USA. Tel: +1.215.496.9646 | Fax: +1.215.636.0251
Safend S.A. 5, Avenue Gaston Diderich L-1420, Luxembourg Tel: +352 26 87 08 67, Fax: +352 26 87 08 68
Toll free from the US (to US and Israel): 1.888.225.9193 | info@safend.com