

Metascan® Customer Snapshot

Public Electric Utility

About the Customer

The largest electric utility in one of the western states distributes power to more than a million customers and operates thousands of miles of transmission lines and tens of thousands of miles of distribution lines. It generates more than 6 MegaWatts at capacity and operates both fossil-fuel and nuclear power plants.



Customer Challenges

An important challenge facing this undisclosed company and all electric utilities, particularly those operating nuclear power plants, is effectively defending computers from cyber intruders and acts of cyber sabotage. The company's computer systems are continually being modified, updated, upgraded and maintained using data downloaded from CDs, USB flash drives, external hard disks, memory cards, PDAs and other portable media. These external media devices are commonly used by engineers, programmers and service people in the course of their work, but are also a potential source of threats entering the organization. One important challenge for this utility was to deploy a fast, effective, and efficient solution for preventing vendors, partners, service people and visitors from bringing electronic media containing malicious malware into the company's facilities. The objective: To mitigate the risk of removable media introducing malicious code that could inadvertently or purposely infect the utility's computer systems.

OPSWAT's Solution

A crucial element of this utility's cyber security defense solution is using OPSWAT's [MetaDefender for Media](#) (MD4M) kiosks to prohibit vendors, partners, service people and visitors from bringing infected USB flash drives, CDs and other portable media into any of the company's facilities. This critical layer of security is accomplished by deploying two or more MD4M kiosks at each of the company's sites. Each MD4M kiosk is used to scan visitors' removable media quickly and reliably utilizing multiple built-in, fully licensed antivirus engines that work simultaneously to detect malicious code.

Results

Using MD4M kiosks to continually defend against infected portable media devices at its nuclear and fossil-fuel electric power plants, this utility is able to meet and exceed U.S. Nuclear Regulatory Commission regulations NEI 08-09 and NIST 800-53 for cyber security protection at its facilities. During the seven months since MD4M was implemented, the solution has been used to scan up to one thousand media devices each day at each of the company's facilities, and not one system has experienced a malware infection.



For more information please contact sales@opswat.com.