

THINK

Endpoint Security

Data mobility is at an all-time high through the use of data sharing applications and removable devices, but in an age where information is constantly a target, federal agencies must look beyond traditional security solutions to better guard against data leakage at the endpoints.

Most security breaches and attacks – inadvertent or intentional – occur at the endpoint and are generated internally. Unmanaged removable media and applications can easily open the floodgates for data to escape into the wrong hands. For example, thumb drives that contained intimate details on everything from US soldiers to secret informants were sold in Afghanistan by teenagers for \$40 a piece.

Recent security violations have sparked the OMB to issue the M-06-16 Mandate that requires agencies to establish safeguards for sensitive data on laptops and workstations. While most government agencies have established security policies that guide what applications and removable devices can be employed by end users, they do not have the capabilities to enforce these policies. Many users continue to run unauthorized software, remove data from organizational networks – when they travel or work at home – and download infected or inappropriate files, which can expose vulnerabilities that enable the theft or loss of critical information.

In the face of such high-profile breaches and growing pressure by regulators to ensure that data is secured, agencies require an endpoint security solution that proactively enforces

application and device control to prevent data leakage.

To date, traditional solutions such as anti-virus software have fallen short of expectations because of their reactive approach that provides security patches only after a vulnerability has been exposed – and these patches are not produced in real time. This blacklist approach blocks known security threats from targeting vulnerabilities, but offers no security against unknown threats originating from unmanaged applications and removable devices.

A more secure approach such as whitelisting, protects against the insider threat and enables quick identification and authorization of specific applications and devices, where only those authorized applications and devices are allowed to run or connect to the network. Everything else is automatically denied by default. And thanks to innovations from SecureWave, such a solution is easy to implement.

SecureWave Sanctuary: A World Apart

With more than 1,200 customers and 1.8 million licenses worldwide, SecureWave brings a wealth of data security expertise and innovation to bear for federal agencies. SecureWave Sanctuary provides policy-based application and device control that proactively secures federal agencies from data threats, including data leakage, malware and spyware. By employing a whitelist approach, Sanctuary is uniquely capable of enabling only authorized applications and devices to run on a network, laptop

or PC – facilitating security and systems management, while providing necessary flexibility to the agency.

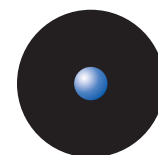
Sanctuary also assures and proves compliance with the landslide of regulations governing privacy and accountability. In particular it helps agencies become compliant with the OMB mandate by providing the necessary controls to manage the data flowing to and from network endpoints and audits the use of applications and devices. Sanctuary maps directly to DCID 6/3 by providing a full audit trail of files written to authorized media devices on organizational networks and in the SCIF environment. No longer will a government entity be vulnerable to data theft or data leakage through the use of unmanaged applications and removable devices.

Sanctuary helps federal agencies:

- Prevent unauthorized I/O devices from connecting to endpoints;
- Protect against malware;
- Prevent network security breaches;
- Enable the transmission, integrity, confidentiality and retention of data without disruption, corruption or loss;
- Prevent unwanted applications and devices from burdening network bandwidth;
- Enable faster computing resources on networks, laptops and PCs;
- Minimize the amount of necessary security patch updates;
- Minimize security crisis response.

For more information about Sanctuary, contact SecureWave at www.securewave.com, or call Robert Monine at (703) 793-3964.

Think



SecureWave
Safeguarding Tomorrow