SOLUTIONS DATA SHEET

DIGITAL GUARDIAN®
Formerly VERDASYS

USDHS Continuous Diagnostics & Mitigation

In 2014, the US Department of Homeland Security issued a task order for Continuous Diagnostics and Mitigation (CDM) tools. This program “moves away from historical compliance reporting toward combating threats to the nation’s networks on a real-time basis.” Initially, the program’s focus is on four functional areas: Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Management (CM), and Vulnerability Management (VUL).

The CDM initiative recognizes that information protection in today’s world requires more than simply blocking known threats. Attackers are patient and well-funded, with the resources and time required to build sophisticated attacks. Rather than blocking yesterday’s attacks, agencies must protect the data itself, wherever it resides.

DIGITAL GUARDIAN STANDS UP TO CDM REQUIREMENTS

Digital Guardian is the only solution available that detects, deters, and prevents the exfiltration of data from both insider and outsider threats. It operates at the kernel of the OS and has complete visibility to all hardware, software, data storage, and data movement. Digital Guardian can automatically classify data based on its context, content, or user descriptions, and then ensure that people and applications use data according to agency policies no matter where it moves. It can be installed on premise (as a perpetual license), as a cloud-based managed service, or in a hybrid model.

The following explains how Digital Guardian can help agencies with the first four CDM functional areas.

Tool Functional Area 1 – Hardware Asset Management (HWAM)

Discover unauthorized or unmanaged hardware on a network.

Digital Guardian provides agencies with the ability to identify and control the use of hardware on a network by user and by content, including computers, USB devices, CDROM, and shared storage. It monitors all file-related events to and from the attached devices and enforces block/allow/encrypt controls based on data type and unique device identifiers.

Digital Guardian enforces enterprise policies to block unauthorized use of sensitive data by users or software applications. Digital Guardian provides granular identification of authorized and unauthorized hardware by manufacturer, model number, and serial number. Unauthorized devices can be blocked from reading or writing data.

Tool Functional Area 2 – Software Asset Management (SWAM)

Discover unauthorized or unmanaged software configuration items in IT assets on a network.

Digital Guardian provides agencies with the ability to control which applications run in their environments and what actions those executables and processes can take with data. Upon installation Digital Guardian automatically compiles a list of all applications and data on each device.

Digital Guardian understands the function of every application. Policies can dictate the privileges of each application to prevent applications from being co-opted to perform data movements that would compromise security.

With Digital Guardian, agencies can block unknown executables and ensure that only approved applications are used. This includes blocking legitimate but undesirable applications such as peer-to-peer networking or chat applications as well as unknown software that may be malicious. Administrators can enforce the use of specific browsers with controlled settings, including funneling Internet access through the company’s network proxy or VPN.

Tool Functional Area 3 – Configuration Management (CM)

Reduce misconfiguration of IT assets, including misconfiguration of hardware devices (physical, virtual, and operating system) and software.

Digital Guardian provides agencies with the ability to block changes to protected files and directories by unauthorized users, including privileged users such as system administrators. It can report on "approved" applications and identify those that are out of date or have unusual MD5 characteristics – indicating possible compromise.

Digital Guardian is tamper resistant and can operate in stealth mode to prevent users from bypassing security configurations. It identifies trends for individual users or computers at day-level granularity to normalize baseline behavior and detect anomalous behavior for further investigation. Administrators can set up email alerts when thresholds for certain activities are exceeded, indicating potential threats to data from privileged users or external attackers.

Tool Functional Area 4 – Vulnerability Management (VUL)

Discover and support remediation of vulnerabilities in IT assets on a network.

Advanced threats often introduce and spawn new processes to affected devices. Digital Guardian can detect these malicious processes, block execution or access to protected data, and alert incident response teams in near real time. Digital Guardian's endpoint agents allow agencies to identify, monitor, and control all actions on endpoints, whether from users or processes.

Digital Guardian's kernel-level agent is the key to its effectiveness and low overhead. The kernel manages all requests and system calls from applications to the CPU, memory, and input/output devices (e.g. mouse, keyboard, disk, and USB drives). By integrating at the kernel, agents monitor and control data from within the operating system. They maintain awareness of all operations and data and can apply appropriate policies to each data item prior to allowing execution of an operation. When a user accesses data, endpoint agents take action based on the classification of the data, context of the action, and applicable policy(s).

COMPLETE DATA PROTECTION AGAINST INSIDER AND OUTSIDER THREATS WITH ONE AGENT

Digital Guardian provides agencies with a proven, scalable solution to protect sensitive information from malicious insiders and external/cyber threats. By protecting the data directly, Digital Guardian provides complete visibility to data movement and use, even if a user attempts to hide actions by copying data into other formats, compressing files, or using screenshots. Operating at the kernel provides "always on" visibility and evidentiary-quality auditing, on and off the network. Data can be shared securely with trusted partners and monitored to ensure proper use. Unauthorized actions by users or applications can be blocked while providing immediate alerts to incident response teams.

ABOUT DIGITAL GUARDIAN

At Digital Guardian, we believe in data. We know that within your data are your company's most valuable assets. The sum total of innovations, plans and potential. We protect your company's sensitive information like it's our own so you can minimize risk without diminishing returns.

For over 10 years we've enabled data-rich organizations to prevent data loss at the endpoint. Our expert security team and proven Digital Guardian platform radically improve your defense against insider and outsider threats.

Hundreds of customers across a wide range of industries rely on Digital Guardian to protect their critical information at the point of risk. Seven of the top ten IP holders and five of the top ten auto companies trust us with the integrity of their most valuable and vulnerable data. We take pride in knowing that, at this very moment, Digital Guardian agents are securing the sensitive data of the world's most inventive, influential companies.

SHARE