SOLUTIONS DATA SHEET

DIGITALGUARDIAN™ for Linux

FILLING THE LINUX SECURITY GAP

Linux adoption continues to soar, with the platform consistently earning a reputation for high reliability. However, as Linux has become more widely deployed, its success has made it a bigger target for outside attackers and malicious insiders. The number of Linux vulnerabilities requiring patches is growing, yet there is a limited set of security solutions available. Most organizations have limited visibility into all of their active applications and user activities on Linux desktops and servers.

National Vulnerabilities Database

ENTERPRISE READY

Digital Guardian is the leading data protection solution for securing data on the endpoint, with millions of agents successfully deployed worldwide. 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. The system proactively tags and classifies your most sensitive data and automatically blocks transmission of proprietary information based on the data's context. Monitoring, real-time prompts, and blocking of suspect actions gives you complete data visibility and control. This protection is software-based, can be installed on Linux servers and desktops, and is achieved with a minimal software footprint.

Unique Benefits for Linux

FULL VISIBILITY INTO LINUX DATA MOVEMENT

Digital Guardian monitors all file movement at the endpoint using a non-invasive approach. This gives you real-time visibility of all data movement and data transmission methods across online, offline, physical and virtual environments, including email, cloud storage, removable media, print and FTP.

BETTER VISIBILITY MEANS BETTER CONTROL

The enhanced visibility provided by Digital Guardian enables effective management of data loss risk. It provides fast, flexible policy implementation based on data, user, and event context. Security policy starts by controlling "known threats" (e.g., prevent source code from going to USB). Full visibility exposes the risk of "unknown threats" (e.g., the Dropbox process synchronizing sensitive data to the cloud).

ADVANCED DATA PROTECTION WITHOUT SLOWING THE PACE OF BUSINESS

Digital Guardian automatically blocks and controls only those behaviors that pose a threat to your organization based on the user, event and data type. This unique contextual awareness and non-invasive approach lets you minimize risk without slowing the pace of your business.

Unique Features for Linux

Because the Digital Guardian platform takes advantage of kernel and user mode visibility, it provides the following unique features:

UNMATCHED PROTECTION

All file types, applications, and data movement are monitored. Even if a user writes their own custom script to manipulate data, policy will still be applied based on the user role and usage rights to the data.

TAMPER-RESISTANT SECURITY

Digital Guardian software cannot be removed or tampered with, ensuring that protection is active at all times, whether on or off the network.

PRIVILEGED USER MONITORING

Linux systems are typically maintained by administrators that have root access (full local administration privileges). Digital Guardian applies policy equally to regular users or privileged users, independent of the Linux security model in place. This means that administrators may have unhindered access to a system for administrative purposes, but Digital Guardian will monitor their actions and block their access to sensitive data.

DIGITALGUARDIAN™ by VERDASYS

For more information, visit
www.digitalguardian.com

CASE STUDIES

INTELLECTUAL PROPERT PROTECTION

Digital Guardian helps companies with Linux infrastructure protect their intellectual property. This includes CAD drawings, source code, and other data residing in structured or unstructured formats.

A financial services firm uses Linux to create the source code that powers their financial platform. Digital Guardian monitors users as they check out the source code and allows them to work on the data on a local machine, and then check it back in again. Protection includes knowing when, where, and how source code is used, and using this visibility to prevent users from removing the source code via removable devices, internet uploads, or any other method. The system logs and audits events to streamline forensics and incident response.

PRIVILEGED USER MONITORING AND CONTROL

An IT Service Provider outsources its Linux servers. Using Digital Guardian, the company provides monitoring and control of privileged administrator access to those servers, and assures its clients that no unauthorized data access occurs.

ITAR COMPLIANCE

Digital Guardian helps companies with Linux infrastructure comply with export control regulations. By monitoring access to controlled information, Digital Guardian assures companies that no foreign nationals ever gain access to it.

A US-based chip manufacturer needed to comply with Export Administration Regulations where foreign nationals could not access export-controlled chip components. All chip designs were accessed through complex source control and CAD applications. The company needed to make sure that any policy applied to a foreign national would enforce the controls but also not break the function of those applications. Digital Guardian provides user-level controls that identify foreign nationals and blocks their view to the chip components while still allowing them to use the applications to perform their function.

HIPAA (PHI) COMPLIANCE

For a healthcare provider, Digital Guardian ensures compliance with HIPAA PHI regulations. Linux web servers are used to serve health information to customers. Digital Guardian prevents administrators from accessing the server data stores and performing unauthorized sensitive data transmissions.

Digital Guardian supports many of the major distributions of Linux including Red Hat, Oracle Linux and SUSE.

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