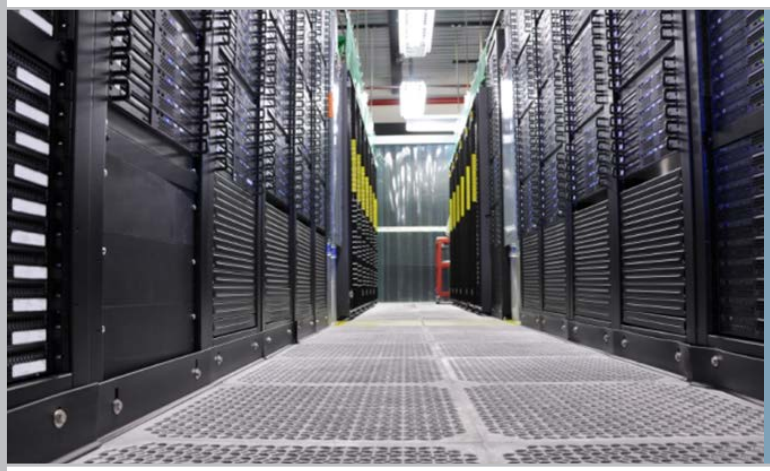
Raytheon | websense®

SureView® Memory Integrity

Advanced Linux Memory Analysis Delivers Unparalleled Visibility and Verification



Promoting trustworthy and repeatable analysis of volatile system state

Benefits

- Enables visibility into the state of systems software while executing in memory on Linux systems
- Delivers malware detection using an integrity verification approach to verify that all systems software running is known and unmodified to quickly identify threats
- Allows the integration of memory forensics into enterprise security information and event management systems (SIEMS) supporting ease of implementation
- Includes an extensive collection of reference software (kernels and applications)
- Verifies the integrity of a remote system's kernel and the integrity of the executable in all processes without doing a complete memory dump
- Scans thousands of systems with hundreds of gigabytes of memory
- Provides a configurable scanning engine for automated scans of remote systems throughout an enterprise
- Incorporates an easy-to-use GUI to quickly assess and interpret results
- Delivers output in a structured data format (JSON) to facilitate analytics
- Supports all Linux distributions, 32- and 64-bit x86 systems providing flexibility and ease of implementation
- Operates reactively or pro-actively on a single system or at enterprise scale for Linux-focused security

Increased Usage of Linux in Global Enterprises

The use of Linux is everywhere in the world. Linux is used in our stock exchange transactions, social media, network storage devices, smartphones, DVR's, online purchasing web sites, and in the majority of global Internet traffic. The Linux Foundation's 2013 Enterprise End User Report indicates that 80% of respondents planned to increase their numbers of Linux servers over the next five years[1]. Drivers include global enterprises migrating to cloud deployments, collaborative and mobile technologies, and employing Linux for mission-critical workloads.

Escalated Malware Attacks on Linux Systems

Millions of malware threat actors recognize this trend and are using advanced tactics to infiltrate Linux systems. According to the 2013 "Malware Forensics Field Guide for Linux Systems[2]," the apparent goal of these attackers is to steal all types of information. Perhaps of greatest concern are the synchronized, targeted attacks against Linux systems. For several years, organized groups of attackers (a.k.a. threat actors) have been infiltrating Linux systems and have been communicating with command and control (C2) servers and exfiltrating data from compromised Linux systems. As a matter of fact, with an increasing market share of Linux desktop users, malware authors have recently taken solid aim at this target population with banking Trojan malware.

These self-serving enemies are always going to be one step ahead of enterprises' network infrastructure security systems making it extremely difficult, if not impossible, for systems to find malware signatures and inversion of control techniques.

Despite the increasing prevalence of attacks on Linux systems, detecting them has often been an afterthought for security vendors focused on other platforms. Linux System Administrators and security experts require assurance that their enterprise systems are running the software that they are supposed to be running and nothing else. This requires a combination of memory forensics and integrity verification to uncover stealth malware and alerts on unknown or unexpectedly modified software. Too many people learn that their Linux systems are compromised only through external notification, long after the fact.

It's 10:00p.m. on Sunday, do you know what software your Linux servers are running? Today, it's a matter of "when" your system will be attacked by an unwanted perpetrator. Will you be ready?

SureView® Memory Integrity Protects Your System

SureView Memory Integrity is a tool that uses memory forensics to acquire and analyze volatile memory from Linux systems. SureView Memory Integrity provides malware detection using an integrity verification approach to validate that all software running is known and unaltered. When responding to a confirmed or potential computer security incident on a Linux system, SureView Memory Integrity will quickly determine where to focus your efforts by highlighting stealth malware, unknown, or unauthorized programs running on the system, and other potential indicators of compromise and vulnerability, saving you time, money, and loss of business.

SureView Memory Integrity for Linux Incident Response

SureView Memory Integrity Incident Response provides memory acquisition and analysis tools to help you get to the root of the problem when you're investigating a suspect system. The Incident Response edition preserves evidence in volatile memory, reconstructs the system state, and extracts artifacts from memory. It detects stealthy malware that would remain hidden from other system administration, forensic, and investigative tools. SureView Memory Integrity Incident Response is powerful and easy to use; memory acquisition is initiated via a single command and analysis results are provided via an easy to navigate GUI.

SureView Memory Integrity Enterprise Security – Protecting Entire Enterprises

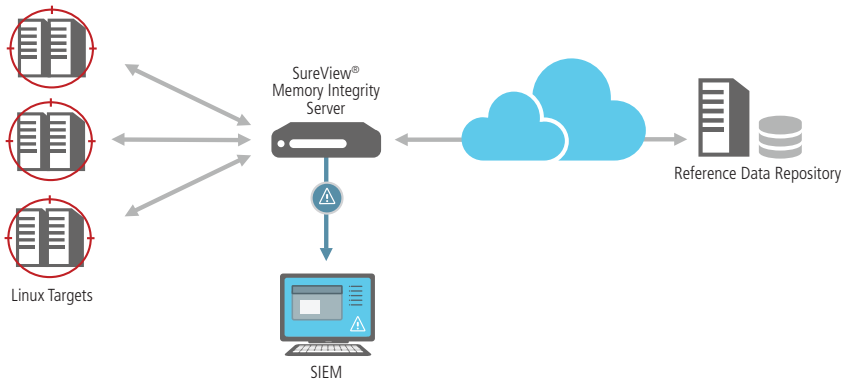
The Enterprise Security version of SureView Memory Integrity monitors Linux workstations and servers using live remote memory analysis to verify the integrity of the kernel and processes. It provides notifications to system administrators and security teams when alerts indicate a compromise has been detected and enables quick, in-depth investigation and response. SureView Memory Integrity was designed to automate Linux memory forensics on thousands of geographically distributed systems enabling system administrators and other users to meet tight performance, reliability, and timing requirements. SureView Memory Integrity Enterprise Security verifies that your Linux systems are running only authorized software whether it is vendor supplied, third-party supplied, or custom developed. It detects rootkits, backdoors, unauthorized processes, and other signs of intrusions into your critical Linux systems. Its memory forensics alerts can be easily integrated into any existing Security Information and Event Management Systems (SIEMS).

Conclusion

Rising trends in malware incidents targeting Linux systems, combined with the ability of modern Linux malware to avoid common security measures, make malware incident response and forensics a critical component of any risk management strategy in any organization that utilizes Linux systems. SureView Memory Integrity provides unparalleled assurance that the programs and libraries in memory on Linux servers and workstations, from the kernel to system services and applications, are of known origin and have not been tampered with. It's particularly useful for detecting artifacts of malware. SureView Memory Integrity is a powerful tool for detecting potential concealment techniques[2]. There is no more effective tool commercially available for detecting rootkits, backdoors, and other unauthorized processes on Linux systems.

1 The 2013 Linux Adoption: 3rd Annual Survey of the World's Largest Enterprise Linux Users.

2 Malware Forensics Field Guide for Linux Systems – Digital Forensics Field Guides by Cameron H. Malin, Eoghan Casey, and James M. Aquilina. Copyright © 2014 Elsevier, Inc.



For further information contact:

Raytheon|Websense
12950 Worldgate Drive, Suite 600
Herndon, Virginia
20170 USA
866.230.1307

www.raytheoncyber.com

All other trademarks and registered trademarks are property of their respective owners.

Cleared for Public Release. Internal Reference #IIS2014-191
Copyright © 2015 Raytheon Company. All rights reserved. - 200170.0915.

Raytheon | websense