FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint Threat Protection for Linux®

UNCOVER MALWARE WITHOUT SIGNATURES TO REDUCE ATTACKER DWELL TIME

FEATURES AND BENEFITS

- **Enables** visibility into the state of software in memory on Linux systems
- **Detects** malware using a unique integrity verification approach
- **Seamlessly** integrates alerts and data into Security Information and Event Management (SIEM) systems
- **Includes** an extensive collection of reference software (kernels and applications)
- **Easily deployable** via integration with standard SSH remote management/ administration infrastructure
- **Scalable** to thousands of systems and to systems with hundreds of gigabytes of memory
- **Provides quick access** to detailed results through easy-to-use interfaces
- **Supports** all Linux distributions on 32- and 64-bit x86 systems
- **Capable** of monitoring mission-critical systems with minimal overhead and no impact to uptime

INCREASED USAGE OF LINUX

Linux is everywhere in the modern enterprise—in cloud deployments, web infrastructure, and many business-critical back-end services. A recent Linux Foundation report indicates that 80% of respondents planned to increase the number of Linux servers within their organizations over the next five years.

ESCALATED ATTACKS ON LINUX

As Linux is used more, it is increasingly attacked—at mass scale by cybercriminals and in targeted operations by motivated attackers. The past year has seen the discovery of more and bigger Linux malware campaigns than in any previous year. Yet as quickly as security researchers publish information and indicators for the malware, attackers update their tools and techniques.

ADDRESSING THE THREATS TO LINUX SYSTEMS

Forcepoint Threat Protection for Linux addresses advanced Linux threats by providing a signature-less attack detection capability based on memory forensics and integrity verification. Memory forensics eliminates reliance on the operating system and other software on potentially compromised hosts, giving Forcepoint Threat Protection for Linux a trustworthy view of system state. Integrity verification means that Forcepoint Threat Protection for Linux ensures Linux systems are running unmodified software from known sources – making malware instantly visible.

MEETING THE NEEDS OF LINUX SECURITY TEAMS

Linux system administrators and security teams require the ability to ascertain whether their systems are

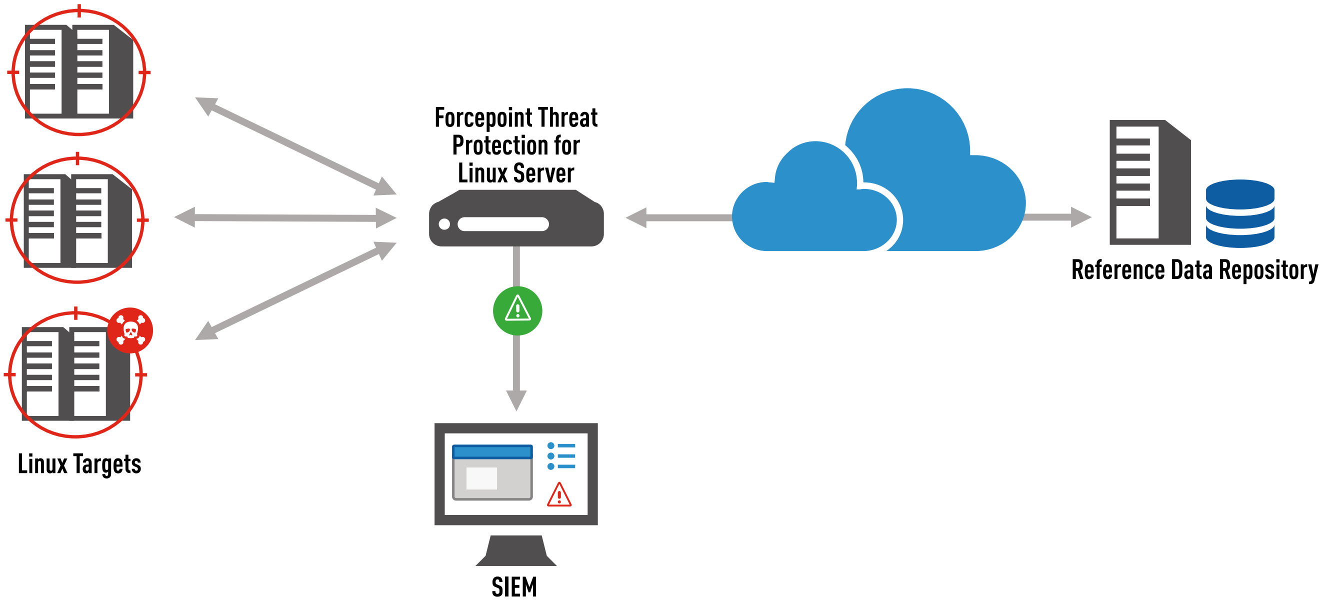
Forcepoint Threat Protection for Linux Server
Reference Data Repository
Linux Targets
SIEM

Figure 1. Forcepoint Threat Protection for Linux Architecture

compromised or not. The most effective way to make such a determination is to understand what software systems are supposed to be running, and to verify they are running precisely that software and nothing else. Such a capability is invaluable for proactive detection of intrusion, determining the scope of a breach, and validating the success of remediation. With Forcepoint Threat Protection for Linux, Linux administrators and security teams can gain confidence in their systems' security, be ready to respond to security incidents, reduce attacker dwell time, and improve the overall effectiveness of their operations.

CONCLUSION

The rising trend in malware campaigns and incidents targeting Linux systems, combined with the ability of modern Linux malware to avoid common security measures, make the advanced Linux threat detection and response capability of Forcepoint Threat Protection for Linux vital for any organization that depends upon the security of its Linux systems. Forcepoint Threat Protection for Linux provides unparalleled visibility and assurance of the software in memory on Linux servers and workstations, from the kernel to system services and applications. There is no more effective tool commercially available for detecting rootkits, backdoors, unauthorized processes, and other indicators of compromise on Linux systems.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_FORCEPOINT_THREAT_PROTECTION_LINUX_EN] 100040.031117