DATASHEET

ADVANCED EPDR FOR LINUX

KEEPING THREATS OFF LINUX

The Linux system already represents 15-20% of the server market and is used in approximately 40% of website servers. Its presence in company infrastructures continues to grow, while cyberattacks on these systems are becoming more frequent and severe. Therefore, protecting Linux-based servers and workstations is critical to businesses.

WatchGuard Advanced EPDR simplifies the security practices for Linux systems by allowing centralized management of all endpoint security and full protection of businesses of any size, industry, or sophistication.

Security and management capabilities on WatchGuard Advanced EPDR for Linux are built from the ground up and optimized solely for Linux. They are powered by Linux-first features to answer the needs of security teams, ranging from performance to prevention, detection, and automated response to threats.

The single **lightweight agent** of WatchGuard Advanced EPDR supports most Linux distributions while using **minimal resources, reducing its impact on the system itself.**

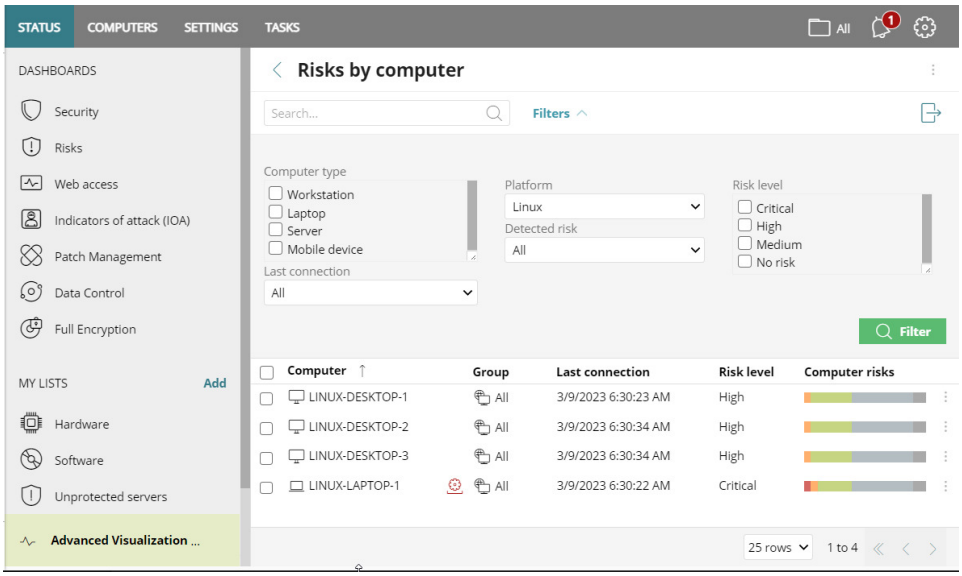

Figure 1. WatchGuard Advanced EPDR centralizes and reinforces the security of all endpoints, including Linux O.S.

Cybercriminals have targeted the Linux operating system

There are two types of attacks on Linux endpoints that companies should be most concerned about:

Ransomware attacks on virtual machines

Ransomware has become one of the primary sources of income for cybercriminal groups. Not only do they act indiscriminately against Windows machines, but when it comes to attacking organizations' assets, many groups have begun to develop techniques to encrypt deployments based on Linux, which is the operating system that is mostly found in company on-premises and Cloud servers.

Cryptojacking

Cryptojacking (hacking systems to use a machine's resources to mine cryptocurrency) is one of the most widespread cyberattacks on Linux systems. It allows attackers to gain direct benefits and can go relatively unnoticed by victims, who only start to worry when the loss of performance of their machines becomes evident.

WatchGuard Advanced EPDR delivers - without the need for costly infrastructure - central management and advanced security functions that bring the following benefits.

Operational Efficiency:

- Centralized management – ease of use in mixed IT environments: Windows, Linux, macOS, Android, and iOS
- Flexible Deployment: supporting even bastioned or isolated environments leveraging the "no-deps" version and native proxy capabilities
- Continuous risk assessment considering endpoint security status
- Individual or group security settings of workstations, servers, and customers for MSPs
- Email alerts in the event of infection and discovery of unprotected endpoints
- Hardware and software inventory
- High performance – specifically designed to have a minimal impact on other programs and the system's general performance

Superior protection and detection against zero day and ransomware attacks:

- Preventative antivirus (AV) against known malware by looking at WatchGuard's up-to-the-minute Cloud-based threat knowledge, the Collective Intelligence (CI)
- WatchGuard's CI is automatically enriched from multiple threat intel sources. One source is the WatchGuard's Zero-Trust Application Service, which is fed by millions of protected endpoints around the world
- Context-based detection of malwareless attacks
- Threat Hunting Service that automatically detects indicators of attacks (IoAs) related to living-off-the-land techniques
- IoAs mapped to the MITRE ATT&CK framework
- Automated containment and remediation by removing malware
- IoAs and suspicious behaviors investigation area
- Access enriched telemetry where MITRE ATT&CK tactics and techniques are mapped to suspicious events

Reduced time to response:

- Automated malware removal
- On-demand and scheduled scans from the single Cloud-based console
- On-demand computers restart
- Remote Shell to manage processes and services, file transfers, command-line tools, get dumps, pcap, and more

REDUCE THE ORGANIZATIONS' ATTACK SURFACE. PROTECT THE LINUX SERVERS AND WORKSTATIONS

Supported systems and distributions within the Endpoint Security Platform for Linux:

WatchGuard Advanced EPDR

Linux System Requirements

Supported Linux Distributions

[i] According to Fortune Business Insights, https://www.fortunebusinessinsights.com/server-operating-system-market-106601, Linux has a 21.8% share of server operating environments, and based on W3techs, Linux is used by 38.8% of all websites: https://w3techs.com/technologies/comparison/os-linux,os-windows

[ii] https://www.watchguard.com/wgrd-resource-center/feature-brief/zero-trust-application

US SALES 1.800.734.9905 EMAIL strategic.accounts@watchguard.com WEB www.watchguard.com WatchGuard Technologies, Inc.