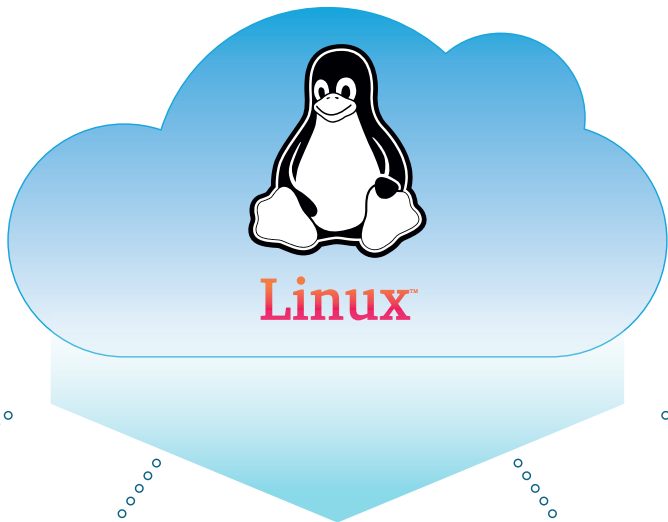


Linux Is the New Ransomware Battleground



THE PREVENTION-FIRST MODEL

Automated Moving Target Defense (AMTD)

Breaks the attacker's assumptions at runtime.

Memory Shielding

Stops fileless and in-memory ransomware cold.

High-Value Decoy Traps

Force ransomware to reveal itself early.

Zero-Noise Protection

Lightweight, deterministic defense built for Linux performance.

Cloud, DevOps, and Container-Ready

Secure CI/CD pipelines, containers, VMs, and Kubernetes without friction.

REAL-WORLD ATTACK MOMENTUM

"Helldown" ransomware expanding attacks to VMware + Linux hosts.

"BERT" ransomware leveraging weaponized ELF files.

Cryptojackers running **undetected for months** in Linux systems.

Attackers blending **AI-driven reconnaissance + credential theft**.

Supply chain attacks abusing trusted open-source ecosystems.

THE NEW RANSOMWARE PLAYBOOK

Double-Extortion by Default

Encrypt the data. Exfiltrate the data. Maximize the pressure.

Fileless & In-Memory Execution

No files. No artifacts. Nothing for EDR to scan.

Living-off-the-Land (LotL) Attacks

Bash, cron, system...attackers use your own tools to stay invisible.

Polymorphic Payloads

Constantly morphing code that evades signature-based detection.

Cloud-Aware Ransomware

Tailored for containers, Kubernetes, and cloud workloads.

THE WAKE-UP CALL

80% of public cloud workloads run Linux.

96% of the top 1M web servers run Linux.

Ransomware operators are now building Linux-native payloads, not ports.

Attackers go where the mission-critical data lives – and that's Linux.

WHY LINUX IS UNDER SIEGE

Fragmented Environments

Too many distros. Too many custom builds. No consistent defense.

Unpatched & Legacy Systems

Old kernels and outdated libraries create long exploitation windows.

Misconfigurations Everywhere

Open SSH ports. Weak permissions. Exposed services. Easy entry points.

Cloud & DevOps Acceleration

Misconfigured pipelines, containers, and orchestration expand the attack surface fast.

HIDDEN WEAKNESSES IN YOUR LINUX STACK

Weak identity controls (SSH key reuse, no MFA).

Container misconfigurations that allow breakout or privilege escalation.

Open-source supply chain exposure from tampered packages and libraries.

IoT, IIoT and edge devices running outdated, unmonitored Linux builds.

Inconsistent logging and monitoring across distros and environments.

WHY DETECTION FAILS ON LINUX

Fileless malware leaves **no disk artifacts**.

Memory-resident attacks bypass behavioral detection.

Polymorphism breaks signature and IOC-based tools.

Resource-constrained Linux servers can't handle heavy agents.

By the time detection fires... the data is already gone.