halcyon

Protection for Linux with the Halcyon Anti-Ransomware Platform

Why Linux is a Target – The Reality of Ransomware

Ransomware, once largely confined to Windows environments, has evolved into a significant threat to Linux systems, as enterprises increasingly depend on Linux servers to power their critical infrastructure. These systems play a vital role in hosting backend services, databases, cloud environments, and high-value workloads. Consequently, ransomware attacks on Linux can result in devastating disruptions.

While high-profile ransomware targeting VMware ESXi hypervisors dominates the headlines, traditional Linux-based systems and endpoints are often overlooked, leaving them misunderstood and insufficiently protected. This gap in protection is a critical weakness in many organizations' cybersecurity strategies.

The Unique Halcyon Approach

Halcyon Linux is designed to address these unique challenges, providing robust protection against ransomware attacks on Linux systems when deployed with the Halcyon Anti-Ransomware Platform. Our solution is tailored to secure the unique way Linux-based environments are targeted in real world ransomware campaigns, from on-premises servers to cloud infrastructures, offering comprehensive protection and rapid response capabilities.

KEY DIFFERENCES OF RANSOMWARE IN LINUX VS WINDOWS:

- **Critical Infrastructure Vulnerability:** Linux systems are frequently used to host essential services like web servers, databases, and virtualized environments. A ransomware attack targeting these systems can cripple an organization's entire operations, leading to prolonged downtime, loss of data, and substantial financial costs.
- **Targeted Attacks on High-Value Servers:** In enterprise environments, Linux servers are prime targets due to their role in storing and processing sensitive, high-value data. Attackers exploit this to demand higher ransoms, knowing the disruption and financial consequences are far greater when Linux systems are impacted.
- **Less Emphasis on Linux Security:** While Windows systems often benefit from anti-ransomware protection, Linux environments are sometimes less fortified, leaving them more vulnerable to ransomware campaigns. Additionally, because most Linux environments are not impacted like Windows systems in a ransomware attack, the security protections that are employed aren't focused on the way in which these systems are targeted via system vulnerabilities, lateral movement, data encryption off system, and exfiltration.
- **Exploiting Linux-Specific Systems:** Though ransomware attacks on Linux are less common than on Windows, attackers are increasingly exploiting Linux-specific vulnerabilities like weak SSH configurations, exposed ports, and outdated software. These weaknesses allow attackers to infiltrate Linux systems, spread laterally, and exfiltrate or encrypt high-value data, often without directly encrypting the system itself.
- **Cloud and Virtualized Risks:** Organizations heavily rely on Linux-based virtual machines and cloud environments. When ransomware compromises these resources, it disrupts both the physical and virtual infrastructure, leading to significant operational and financial damage. Encrypted data, halted services, and lost productivity are just a few of the devastating consequences.

KEY FEATURES AND BENEFITS:

Real-Time Visibility and Detection: The Halcyon Linux agent monitors systems in real time, detecting ransomware-specific behaviors such as unauthorized access, lateral movement, or modification of critical files. This provides instant insights into potential ransomware threats before they cause significant harm.

Integrated Ransomware Response: The built-in Halcyon Ransomware Response Engine allows rapid action when ransomware is suspected or detected. Halcyon Threat Response and Services teams can engage immediately, ensuring real-time incident response is fully supported across all protected Linux systems.

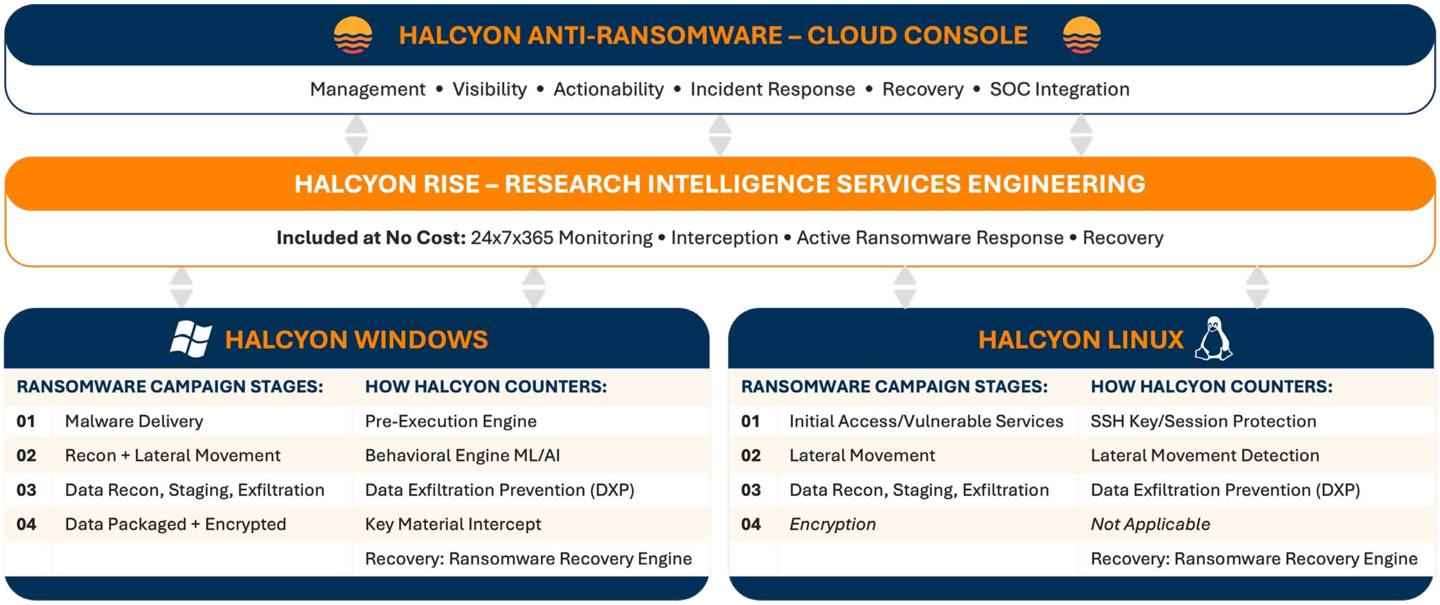
Efficient Performance: Optimized for Linux, the agent runs with minimal resource impact, ensuring that it does not hinder performance in critical environments, such as database servers or virtualized workloads.

Data Exfiltration Prevention: With support for the Halcyon DXP module, Linux environments are safeguarded against data extortion attempts, a rising concern in modern ransomware campaigns. The DXP module identifies and blocks unauthorized data transfers to protect sensitive information.

Cross-Platform Coverage: Halcyon offers seamless protection across hybrid endpoint environments. With full support for both Linux and Windows systems, organizations can secure their entire infrastructure against ransomware without gaps in defense.

24/7/365 Security Analyst Monitoring: Today's security teams are overburdened with managing technologies and responding to a cascade of alerts. The Halcyon Threat Response team supports every Linux customer by reviewing and responding to events.

How Cross-Platform Protection Works in Windows + Linux Environments:



HALCYON ANTI-RANSOMWARE – CLOUD CONSOLE

Management • Visibility • Actionability • Incident Response • Recovery • SOC Integration

HALCYON RISE – RESEARCH INTELLIGENCE SERVICES ENGINEERING

Included at No Cost: 24x7x365 Monitoring • Interception • Active Ransomware Response • Recovery

HALCYON WINDOWS

RANSOMWARE CAMPAIGN STAGES:		HOW HALCYON COUNTERS:
01	Malware Delivery	Pre-Execution Engine
02	Recon + Lateral Movement	Behavioral Engine ML/AI
03	Data Recon, Staging, Exfiltration	Data Exfiltration Prevention (DXP)
04	Data Packaged + Encrypted	Key Material Intercept
		Recovery: Ransomware Recovery Engine

HALCYON LINUX

RANSOMWARE CAMPAIGN STAGES:		HOW HALCYON COUNTERS:
01	Initial Access/Vulnerable Services	SSH Key/Session Protection
02	Lateral Movement	Lateral Movement Detection
03	Data Recon, Staging, Exfiltration	Data Exfiltration Prevention (DXP)
04	*Encryption*	*Not Applicable*
		Recovery: Ransomware Recovery Engine

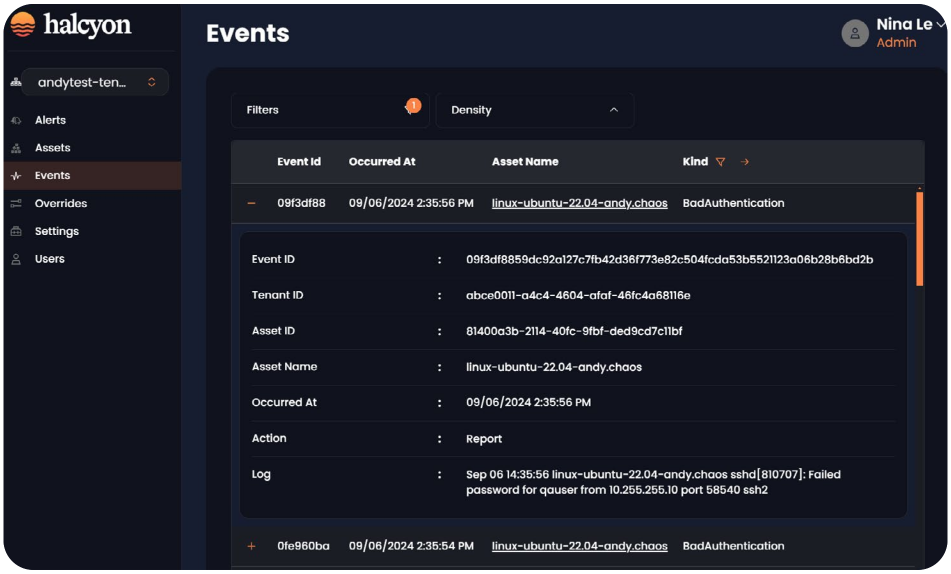
Legend - Stages of a Real-World Ransomware Campaign

STAGE 01:
Infection, Persistence, and Command & Control

STAGE 02:
Privilege Escalation and Lateral Movement

STAGE 03:
Data Recon, Staging, and Exfiltration

STAGE 04:
Payload Detonation and Extortion



	Event Id	Occurred At	Asset Name	Kind
–	09f3df88	09/06/2024 2:35:56 PM	linux-ubuntu-22.04-andy.chaos	BadAuthentication

Event ID : 09f3df8859dc92a127c7fb42d36f773e82c504fcda53b5521123a06b28b6bd2b

Tenant ID : abce0011-a4c4-4604-afaf-46fc4a68116e

Asset ID : 81400a3b-2114-40fc-9fbf-ded9cd7c11bf

Asset Name : linux-ubuntu-22.04-andy.chaos

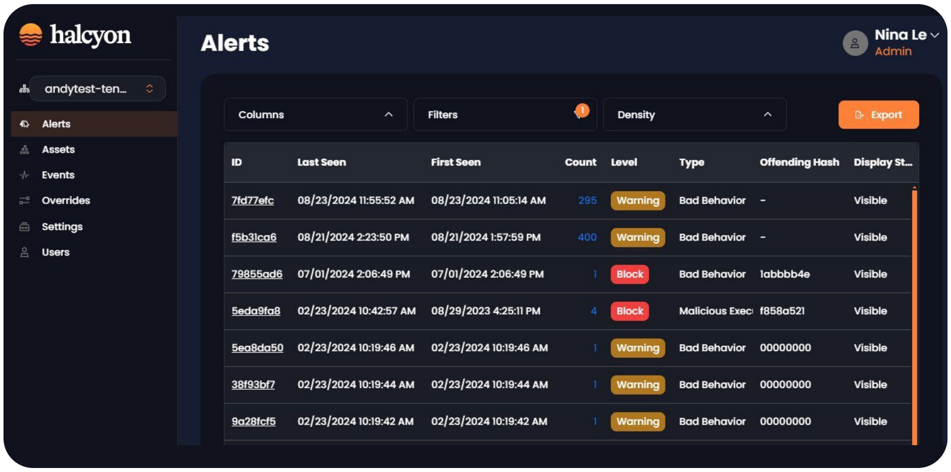
Occurred At : 09/06/2024 2:35:56 PM

Action : Report

Log : Sep 06 14:35:56 linux-ubuntu-22.04-andy.chaos sshd[810707]: Failed password for qauser from 10.255.255.10 port 58540 ssh2

	Event Id	Occurred At	Asset Name	Kind
+	0fe960ba	09/06/2024 2:35:54 PM	linux-ubuntu-22.04-andy.chaos	BadAuthentication

Fig 1: Halcyon Platform – Cloud Console showing Linux Events



ID	Last Seen	First Seen	Count	Level	Type	Offending Hash	Display St...
7fd77efc	08/23/2024 11:55:52 AM	08/23/2024 11:05:14 AM	295	Warning	Bad Behavior	-	Visible
f5b31ca6	08/21/2024 2:23:50 PM	08/21/2024 1:57:59 PM	400	Warning	Bad Behavior	-	Visible
79855ad6	07/01/2024 2:06:49 PM	07/01/2024 2:06:49 PM	1	Block	Bad Behavior	1abbbb4e	Visible
5eda9fa8	02/23/2024 10:42:57 AM	08/29/2023 4:25:11 PM	4	Block	Malicious Exec	f858a521	Visible
5ea8da50	02/23/2024 10:19:46 AM	02/23/2024 10:19:46 AM	1	Warning	Bad Behavior	00000000	Visible
38f93bf7	02/23/2024 10:19:44 AM	02/23/2024 10:19:44 AM	1	Warning	Bad Behavior	00000000	Visible
9a28fcf5	02/23/2024 10:19:42 AM	02/23/2024 10:19:42 AM	1	Warning	Bad Behavior	00000000	Visible

Fig 2: Halcyon Platform – Cloud Console showing Linux Alerts

SUPPORTED LINUX OPERATING SYSTEMS:

Linux Distribution	Versions	CPU Arch
Redhat Enterprise Linux	8	x86_64
Redhat Enterprise Linux	9	x86_64
Debian	11	x86_64
Debian	12	x86_64
Ubuntu	22.04 LTS	x86_64
Ubuntu	24.04 LTS	x86_64
AWS Linux	2023	x86_64
Oracle Linux	8	x86_64
Oracle Linux	9	x86_64
Rocky Linux	8	x86_64
Rocky Linux	9	x86_64
AlmaLinux	8	x86_64
AlmaLinux	9	x86_64

Why Halcyon?

Halcyon Linux is the first endpoint agent specifically built for proactive, real-time ransomware protection tailored to the unique challenges of Linux environments. Whether safeguarding on-premises infrastructure or cloud-based services, Halcyon provides comprehensive defense against ransomware, keeping your most critical systems secure with minimal operational impact. Protect your organization's most critical assets with advanced detection, real-time response, and minimal operational disruption.

Halcyon Linux: Built on the Anti-Ransomware and Cyber Resilience Platform

The unique Halcyon Anti-Ransomware Platform is easy to deploy, does not conflict with existing endpoint security solutions, and provides several unique levels of protection against ransomware attacks. Halcyon is the first platform to specifically target the problem of ransomware.

For more information on Halcyon Linux or the Halcyon Anti-Ransomware Platform, visit halcyon.ai and get a demo!

halcyon

Contact us at **halcyon.ai/contact** or **sales@halcyon.ai**