halcyon

Data Sheet

Protect the Backbone of Your Operations with Halcyon for Linux

Linux Systems Getting Targeted by Ransomware

Microsoft Windows-based systems are undoubtedly the preferred target for ransomware attacks. However, clever attackers now target Linux-based systems because they likely house data vital to the organization's operations. This increases the chance that the organization will pay a ransom to regain access to its impacted data and systems.

Comparing Windows and Linux Ransomware Attacks

While any ransomware attack intends to force the victim organization to pay a ransom, the methods used in a Microsoft Windows attack and a Linux attack are very different, as seen in the table below.

Key Features and Benefits

- Real-Time Threat Detection
- Data Exfiltration Prevention (DXP)
- 24/7 Ransomware Expert Monitoring
- Integrated Ransomware Response
- Optimized Performance for Linux
- Cross-Platform Support

How Cross-Platform Protection Works in Windows and Linux Environments

Ransomware Attack Stage	Impact on Windows OS	Impact on Linux OS
Initial Foothold	Typically gained via phishing emails, malicious attachments, or drive-by downloads exploiting Windows vulnerabilities (e.g., SMB).	May exploit SSH brute force attacks, misconfigured servers, or vulnerabilities in web applications/services.
Privilege Escalation	Exploits Windows-specific vulnerabilities (e.g., EternalBlue) or abuses built-in tools like PowerShell and WMI.	Exploits sudo misconfigurations or vulnerabilities in the kernel or commonly used services.
Lateral Movement	Leverages Active Directory to spread across the network; uses tools like RDP, SMB, or PSExec.	May exploit SSH keys, insecure network services, or NFS/SMB shares for spreading.
File Encryption	Targets common file formats (e.g., .docx, .xlsx, .jpg) and encrypts them with ransomware-specific keys.	Encrypts files on mounted directories, commonly targeting production data (e.g., /home, /var, /etc).
Persistence Mechanisms	Installs backdoors or registry entries to ensure the ransomware restarts even after a system reboot.	May install cron jobs, systemd services, or tamper with init scripts to ensure persistence.
Ransom Note Delivery	Displays a ransom note on desktop or as a startup message using Windows GUI tools or system logs.	Places ransom notes in key directories, alters terminal startup messages, or modifies shell profiles.
Ransom Demand	Ransom note demands payment in cryptocurrency, usually via a GUI popup, or browser-based instructions.	Provides payment instructions in text files, often lacking sophisticated GUI tools seen in Windows attacks.
Recovery Challenges	Recovery may require reinstalling the OS, restoring from backups, or using specialized decryptors (if available).	Similar recovery steps; however, Linux admins often rely on backups or reconfiguration of critical services.

Key Features and Benefits

Real-Time Threat Detection: Detects ransomware-specific behaviors such as unauthorized access, lateral movement, modification to critical files, and tampering with existing security controls, delivering instant identification of potential ransomware.

24/7 Ransomware Expert Monitoring: A dedicated team of ransomware experts monitors all suspected ransomware events at no charge, ensuring no threat goes unnoticed.

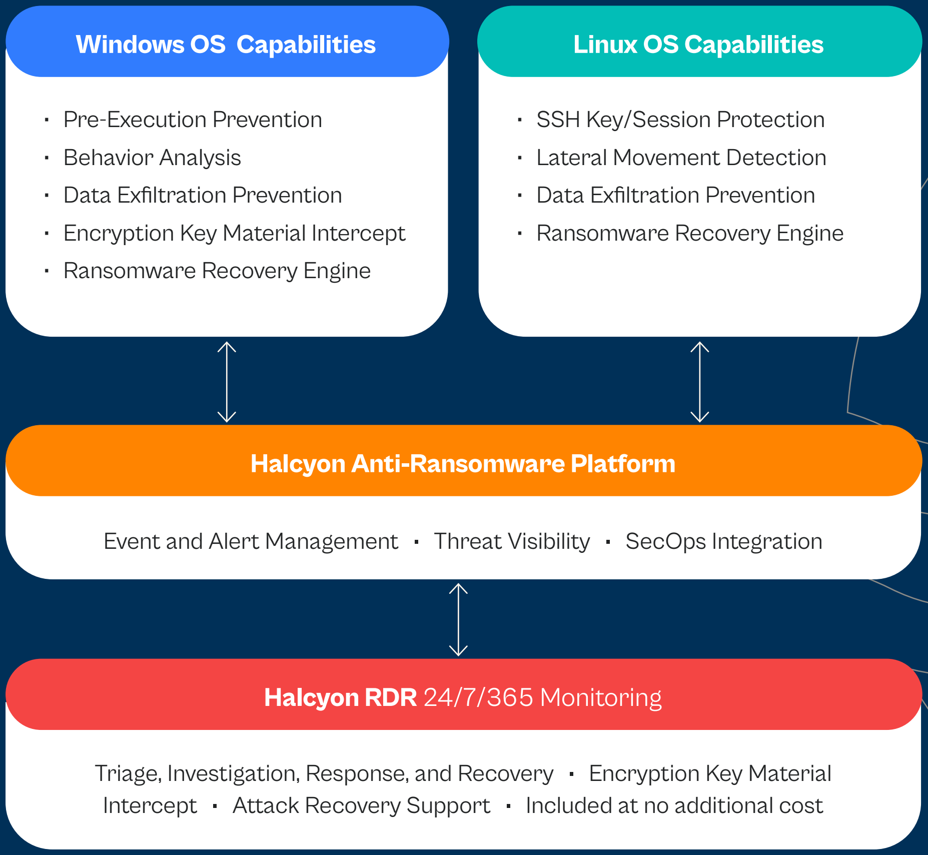
Integrated Ransomware Response: The ransomware response engine enables fast response when potential ransomware identified. With the Halcyon Threat Response team monitoring 24/7, any ransomware threat can be mitigated to ensure no disruption to normal operations.

Data Exfiltration Prevention (DXP): Ensure your vital data is safeguarded from the rising threat of ransomware attackers stealing your data before they encrypt so that they can carry out a "double extortion" attempt. With Halcyon DXP, any transfer of data to a known malicious site or any suspicious volume of data moving out of your environment is detected.

Optimized Performance for Linux: The Halcyon Linux agent runs with minimal resource impact ensuring business critical workloads operate effectively.

Cross-Platform Support: With support for Linux and Windows systems, Halcyon provides comprehensive ransomware protection across your entire environment.

How Halcyon Protects Linux and Windows Environments



Windows OS Capabilities

- Pre-Execution Prevention
- Behavior Analysis
- Data Exfiltration Prevention
- Encryption Key Material Intercept
- Ransomware Recovery Engine

Linux OS Capabilities

- SSH Key/Session Protection
- Lateral Movement Detection
- Data Exfiltration Prevention
- Ransomware Recovery Engine

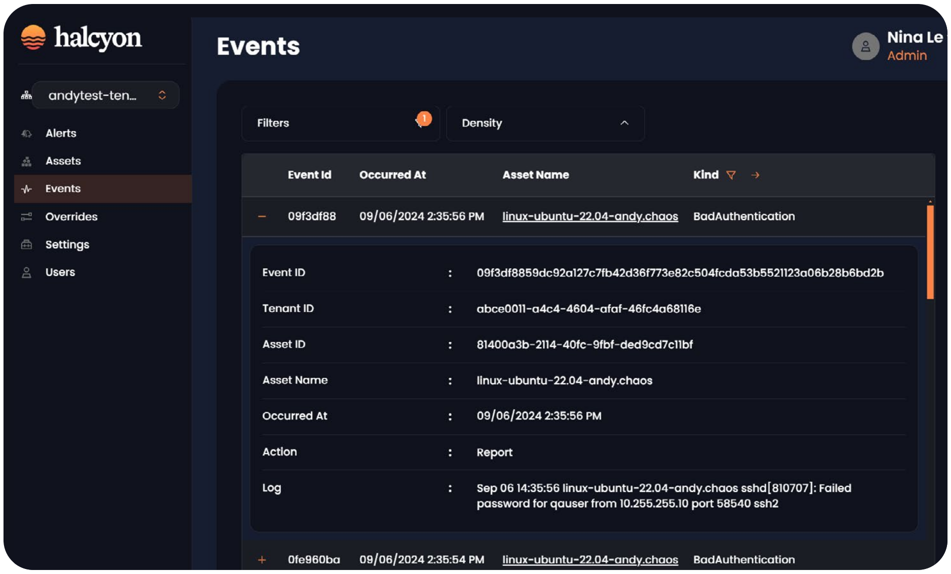
Halcyon Anti-Ransomware Platform

Event and Alert Management · Threat Visibility · SecOps Integration

Halcyon RDR 24/7/365 Monitoring

Triage, Investigation, Response, and Recovery · Encryption Key Material Intercept · Attack Recovery Support · Included at no additional cost

Halcyon is the only anti-ransomware vendor dedicated to protecting your Linux and Windows environments from the rising ransomware threat. Unlike other products that claim their ability to protect VMware ESXi Hypervisors from ransomware as Linux protection, Halcyon delivers native ransomware protection for the most popular Linux distributions. Backed by a team of ransomware experts monitoring every potential ransomware threat 24/7 at no additional cost, Halcyon delivers the Linux ransomware security you need to ensure your most vital data and systems remain secure and operational.

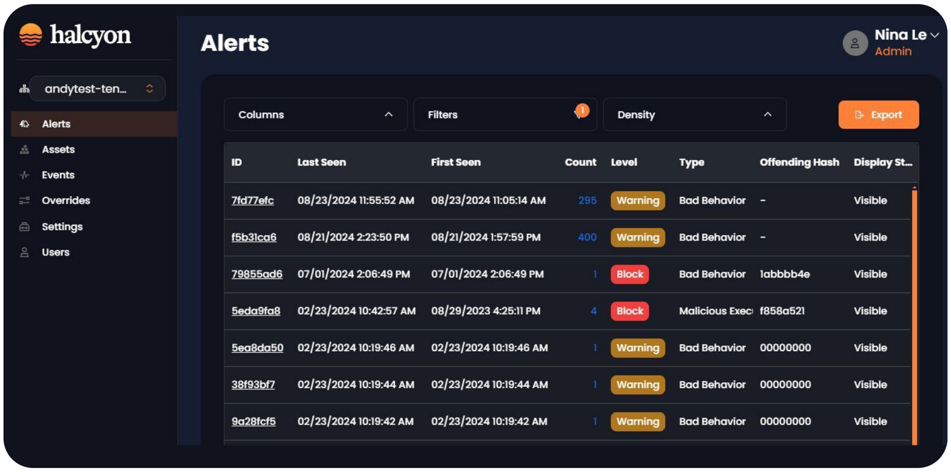


	Event Id	Occurred At	Asset Name	Kind
−	09f3df88	09/06/2024 2:35:56 PM	linux-ubuntu-22.04-andy.chaos	BadAuthentication

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

Halcyon for Linux

The Halcyon Anti-Ransomware Platform is the first security platform built explicitly 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 critical systems secure with minimal operational impact.

For more on Halcyon for Linux, or the Halcyon Anti-Ransomware Platform, visit halcyon.ai and schedule your personalized demo today.

Supported Linux Operating Systems

Distribution	Versions	CPU
Redhat Enterprise Linux	8	x86_64
Redhat Enterprise Linux	9	x86_64
Debian	11	x86_64
Debian	12	x86_64
Unbuntu	22.04 LTS	x86_64
Unbuntu	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

Get a demo at halcyon.ai/demo