WHITE PAPER

Next Generation Linux Server Security

Provide clear visibility, deliver comprehensive context & allow for complete control

cmd.com
1.604.262.9123
sales@cmd.com

Traditional Linux security is fractured

As more and more applications are migrated into cloud environments, the world's most powerful organizations are relying on Linux to run their servers. However, strategies to secure the information stored on these Linux servers often fall dramatically short of the ideal state due to gaps in the tools available.

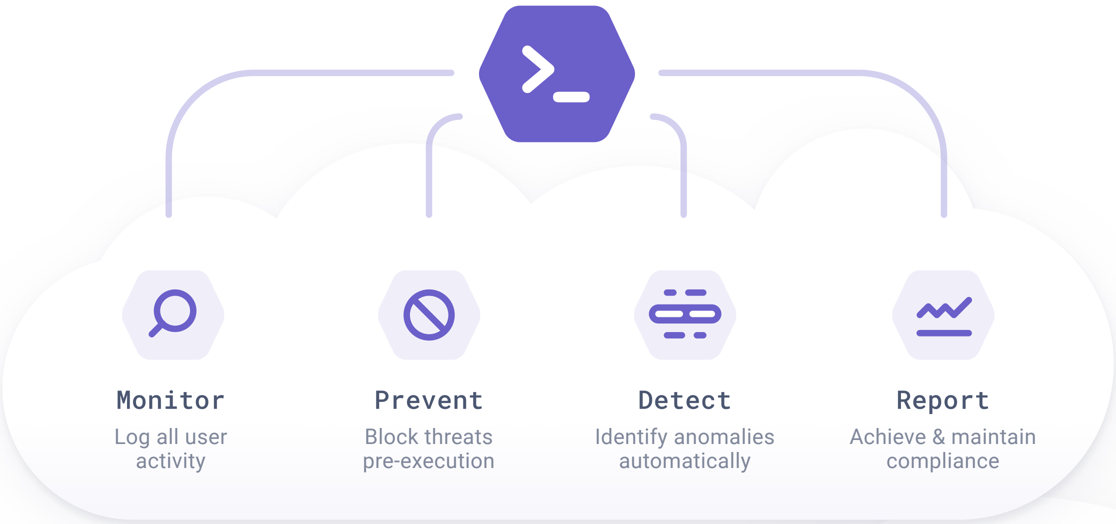
Many of these tools weren't designed with Linux in mind, resulting in solutions that are either too slim to offer reliable protection or too cumbersome and expensive to feasibly roll out and maintain. Further complicating matters, the DevOps and SecOps teams within an organization are locked in an unwinnable battle of warring motivations. This often leads to cutting security corners in order to keep business operations from slowing to a crawl. Day after day organizations roll the dice, leaving themselves exposed to the possibility of a crippling breach.

We believe it's about time things changed. Cmd is a proactive security solution built specifically for Linux servers that offers organizations native user control. Because keeping your sensitive data out of harm's way shouldn't be left up to chance.

Benefits of Cmd

- Watch user activity in real time and react live
- Lock down privileged accounts without blocking business
- Optimize investigation efforts with intuitive, yet comprehensive logs
- Intercept syscalls and block commands pre-execution
- Maintain an agile security strategy that delights DevOps and SecOps alike

	Competitors	Cmd
Policy / Rule management (Two-factor, approval)	✗	✓
Logs encrypted at rest, and in transit	✗	✓
Machine learning / Anomaly detection	✗	✓
Process level monitoring	✓	✓
User level monitoring	✗	✓
Tamper proof agent / listener	✗	✓
Custom user notifications on error / policy violation	✗	✓
File-diff on change	✗	✓
Command execution prevention	✗	✓



Monitor
Log all user activity

Prevent
Block threats pre-execution

Detect
Identify anomalies automatically

Report
Achieve & maintain compliance

Establish your internal baseline and understand user behavior with Cmd Monitor_

Cmd begins by comprehensively logging all user activity within your Linux environment as soon as you run Cmd's 60-second installer. The Cmd agent runs within user space, collecting valuable information for every action performed regardless of user privileges.

Enjoy unprecedented visibility

Cmd goes far beyond simply showing you the commands that a user typed, showing you the executions underneath scripts and binaries, too. If a user writes and executes a script with multiple commands nested underneath, you'll get to see those executions. You'll even be able to see what's happening under sudo shells or other unusual executions that might never be captured any other way.

Monitor the logs in real time or months down the line

Watch user activity as it happens with live monitoring. Enjoy the option to react live and end high-risk sessions on the fly.

Have you ever needed to comb through logs from three months ago? A year ago? It probably made you want to pull your hair out. Our intuitive UI transforms the process of sifting through logs from impossible chore to attainable task. Cmd makes it easy to find the information you need, fast. Cmd protects your logs against tampering regardless of user privilege level, ensuring that the integrity of your audit trail remains intact.

Stop threats, pre-execution with Cmd Prevent_

Cmd's customizable access control capabilities allow you to lock down your Linux environments at the command level. Build bespoke triggers that align to the specific security policies present within your organization to secure your environments, your way.

Control privileged user access beyond the rigid Allow/Deny binary

Successfully safeguarding your Linux servers requires a defense-in-depth strategy, one that allows you to stay two steps ahead of malicious-minded attackers. Cmd allows you to move past the outdated mindset that setting and forgetting a few generic rules to grant or block access will leave your organization protected.

Prompt for dual authentication

Not all access control is black and white. This is where Cmd truly shines: provide clarity to those "maybe" cases by introducing agile follow-up actions, such as:

- **Multi-factor authentication** — Do your users access your Linux servers with shared or root keys? Prompt for dual authentication to attribute user activity to a specific individual.
- **Manager dual authentication** — Ask users to enter a reason for executing a sensitive command. Cmd will send the command request to a manager's mobile phone so that they can approve, deny, or end the session on the fly.
- **Peer-to-peer dual authentication** — Skip the CISO and send low-risk requests to a Slack channel. A fellow engineer can approve these commands instead, saving your engineers valuable time and reducing alert fatigue in one fell swoop.

Whitelist or blacklist commands with granularity

Choose to allow, deny, or end sessions based on a custom mix of trigger queries. Choose from criteria such as IP address, location, job title, day of the week, or even first-time executions.

Enforce new rules in seconds

Cmd's position outside of the kernel means that new triggers are enforceable within 30 seconds of enforcing in our console. This makes it easy to create an emergency lock down, block a user from completing actions on the fly, or grant temporary access to a group of users tasked with putting out a fire outside of their typical jurisdiction without requiring a restart.

Identify and stop suspicious, risky commands automatically with Cmd Detect_

Based on your custom triggers, Cmd will begin flagging potential threats within your environment. Cmd's machine learning capabilities help mitigate potential human blind spots, ensuring no risky behaviors go unnoticed.

Identify indicators of compromise early and efficiently

Once threat actors gain a foothold, they can easily move through networks by leveraging administrator tools. Cmd allows you to detect adversarial TTPs (Tactics, Techniques and Procedures) early, block actions that seem unusual, and prevent escalation of attacks in real time.

Cmd's machine learning acts as a policy force multiplier

What types of suspicious activity will Cmd detect? Our machine learning identifies anomalous users, detects intruders, classifies known malicious binaries, and even flags activity that it deems potentially unknown malware. To arrive at these conclusions, Cmd analyzes behavior and command analysis of all users, regardless of the user's native access level.

Stay one step ahead of malicious actors

Coupled with Cmd's detailed visibility features, alerts generated by Cmd's machine learning capabilities will help you uncover the latest techniques attackers are using to commit zero-day attacks. Use this valuable information to build new triggers, adding extra layers of protection around your sensitive data.

Automatically fine tune your signal-to-noise ratio

By default, Cmd's machine learning will trigger an alert when it comes across a perceived threat. These threats are categorized by perceived risk level, viewable by the Cmd user on the web app.

The Cmd system is optimized to keep false positives to a minimum in an effort to prevent alert fatigue. However, nothing is set in stone. You can adjust the signal strength of alerts until you reach your organization's ideal state.

Maintain accountability and achieve compliance with Cmd Report_

Ensuring that your security operations comply with regulatory standards can seem like a daunting task...but it doesn't have to be. Combining the powers of added visibility and bespoke triggers, Cmd streamlines the process of achieving and maintaining compliance, according to all major standards.

Here's a high-level look at how Cmd's capabilities map to a few common regulatory standards:

PCI

- Provide a comprehensive audit log of all server activity, accounting for every user action performed.
- View and manage application and binary deployment across your network. Blacklist unknown and/or potentially risky commands.
- Attribute any root login to a specific user in a way that cannot be bypassed.

SOC 2 TYPE II

- Protect the integrity of your files. Restrict who can access certain files, track log file diffs, and more.
- Monitor and log all interactions with the system terminal, including interactive commands and tools such as Screen, vim, Nano, tcpdump, etc.
- Control privileged access. Every user action is logged using tamper-proof methods, regardless of the user's existing permissions.

GDPR

- Limit a user's ability to access PII based on qualifications such as job role, company position or user login location.
- Automatically scrub sensitive information from logs.
- Customize the level of detail logged for sensitive servers from specific users or accounts.

NIST

- Ensure all user activity is recorded. Logs cannot be obfuscated or deleted, regardless of user's access level.
- Automate dual authentication requirements or multi-tier approval for commands.
- Restrict the use of shared accounts, requiring individuals sharing keys to dual-authenticate, and monitor suspicious activity therein.

Cmd integrates seamlessly with your existing toolchain

Infrastructure compatibility

Cmd's architecture works with virtually all enterprise environments and maintains compatibility across all major Linux distributions.

- Debian 7 (wheezy)
- Debian 8 (jessie)
- Debian 9 (stretch)
- Ubuntu 14.04 (Trusty Tahr)
- Ubuntu 16.04 (Xenial Xerus)
- Ubuntu 18.04 (Bionic Beaver)
- CentOS 6
- CentOS 7
- Amazon Linux (2017.09+)
- Red Hat Enterprise Linux 7.4
- And many more

One centralized events dashboard

Connect Cmd with the SIEM product your team utilizes to analyze the Cmd events alongside your other security solutions within one centralized dashboard.

Identity verification in a snap

Our MFA capabilities can be configured to work with many of the tools your team already know and love. Ensuring the identity of your users has never been this easy.

...and so much more

Between our direct integrations, API, webhooks, and the direct integrations in our pipeline to build, the possibilities are endless. Contact us to inquire about specific integrations.

Ready to accelerate your organization's security strategies from reactive to proactive? **Email us to schedule a live demo** to experience Cmd's capabilities for yourself.