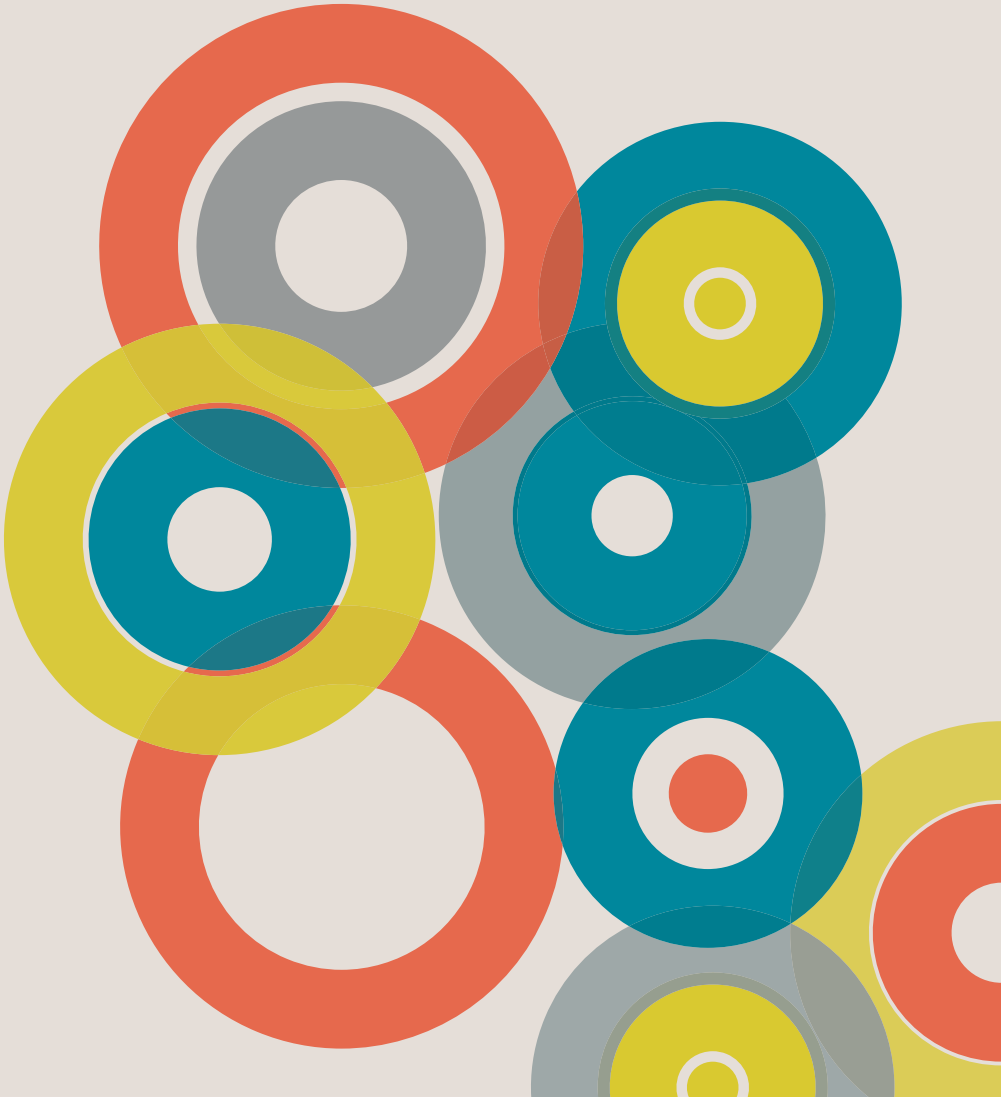
CAPSULE8

Capsule8 for PCI Compliance

Solution Brief



Securing Credit Card Data across Linux Environments

For many organizations, payment card information is the lifeblood of the business. As card usage surges globally, cardholder data have become attractive targets to cyber criminals.

To push merchants, payment processors, financial institutions and service providers to protect cardholder data, the leading payment card brands partnered to create the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI DSS defines a broad range of measures, spanning people, process and technology, every company must enact if they store, process or transmit cardholder data. Compliance is required and businesses face fines for failing to deploy appropriate controls.

Protecting payment card data and complying with the PCI DSS is daunting. The scope is broad—all systems included in or connected to the cardholder data environment are impacted. This becomes particularly challenging for companies with complex IT infrastructure, including Linux production environments, which needs to be protected but must also perform at optimal levels at all times.

While the challenge is real, there is hope. As businesses look to comply and, more importantly, protect cardholder data across Linux-based environments whether in the data center or cloud, Capsule8 delivers. Capsule8 Protect is a single platform that addresses PCI requirements in such areas as intrusion detection and prevention systems (IDS/IPS), file integrity monitoring (FIM) and anti-virus (AV). Thanks to an exhaustive review by DirectDefense, a leading provider of PCI and security assessment services for PCI DSS, customers are confident knowing that they can shift from multiple legacy controls to a single, simple solution from Capsule8 that performs well even on the busiest workloads and networks.

Securing Cardholder Data with Capsule8

Given the breadth of environments in-scope of the PCI DSS requirements, companies often see cardholder data touch Linux-based infrastructure, such as bare metal systems, containers, and virtual machines. Further, this infrastructure may be found within the data center or cloud environments; often both. Therefore, Linux – and the security of Linux systems – must be at the forefront of any effort designed to protect cardholder data.

Capsule8's Protect platform works across all Linux production environments – whether containerized, virtualized or bare metal. Capsule8 Protect has a powerful policy-based protection capability that solves security exception management problems that have long plagued host-based policy solutions. As a result, Capsule8 performs well even on busy servers and networks that previously were too mission-critical for agent-based security solutions that inevitably slow down systems. Using Capsule8 Protect, customers benefit from the ability to secure cardholder data by:

- Identifying and protecting against attacks in real-time, including zero-day threats, across Linux production environments. The Capsule8 system protects data and monitors system access in layers. In addition to traditional methods of scanning and monitoring for compromise, the core of Capsule8's offering leverages policies which identify indicators of attack, allowing your organization to disrupt and stop malicious actors prior to compromise
- Responding automatically to threats in real-time by killing connections, restarting workloads and alerting investigators
- Integrating with existing systems to ensure interoperability with backend workflows, including SIEMs, log analytics, and forensics tools

Capsule8 for PCI DSS

With Capsule8, customers facing PCI DSS compliance are able to ease the process of addressing:

PCI Requirement 5: Use and regularly update anti-virus software

PCI Requirement 6: Develop and maintain secure systems and applications

PCI Requirement 10: Track and monitor all access to network resources and cardholder data

PCI Requirement 11: Regularly test security systems and processes

DirectDefense, a leading PCI DSS assessor, validated Capsule8 as a PCI DSS compliant solution.

With Capsule8, customers can protect complex Linux production environments, simplify the security of cardholder data, reduce false positives, and remove performance risk on the most vital IT environments.

Complying with the PCI Data Security Standard

With 12 high-level requirements and dozens of prescriptive measures, the PCI DSS offers "fundamental guidance on controls to securing cardholder data." While the standard cuts across people, process, and technology, it is the application of cybersecurity controls that causes the greatest challenge for many businesses.

With Capsule8, customers are able to address many of the key technology requirements within the PCI DSS – and have the peace-of-mind knowing these controls are both appropriate and effective. To this end, Capsule8 partnered with DirectDefense to evaluate the Capsule8 technology in relation to the PCI Data Security Standard. In short, Capsule8 was found to be a compliant solution for ALL architectures that include Linux-based infrastructure.

Capsule8 was specifically found to address the following requirements within the PCI Data Security Standard:

CHALLENGE: PROTECT AGAINST MALWARE

PCI Requirement 5: Use and regularly update anti-virus software

The PCI DSS recognizes the damage that malware can cause in systems storing and processing payment data, whether giving attackers a foothold to exfiltrate this sensitive data, or otherwise compromising the integrity and confidentiality of the data. Businesses are expected to take the steps necessary to protect themselves against both known and unknown threats.

Through Capsule8, customers are able to both prevent and detect threats – from common attackers like cryptominers to zero-day attacks – across Linux environments.

Specifically, Capsule8 enables customers to address PCI requirement 5 by:

- Protecting against malware across containerized, virtualized, and bare metal environments, in public, private, or hybrid cloud environments and in data centers
- Keeping antivirus definitions current through regular and automatic updates
- Producing log entries based on indicators of attack which can be viewed in the Capsule8 console or integrated with your existing operations consoles
- Detecting attacks in real-time to prevent attackers from compromising payment card data
- Killing connections, restarting workloads, and alerting security teams automatically in the event of an attack

CHALLENGE: SECURING OF SYSTEMS AND APPLICATIONS

PCI Requirement 6: Develop and maintain secure systems and applications

Software vulnerabilities offer criminals doorways into systems and applications that store, transmit, and process cardholder data. Given this reality, the PCI DSS requires companies to monitor and patch vulnerabilities in all systems within the PCI environment.

To help address this requirement, Capsule8 Labs works to continually identify and evaluate new and existing Common Vulnerabilities and Exposures (CVEs) to ensure the sensors protect against new and emerging threats. In addition, Capsule8 enables companies to address the PCI DSS by:

- Testing continually against new exploits to ensure the effectivity of the Capsule8 platform
- Tagging alerts with risk ratings (high, medium or low) to enable triaging
- Developing and deploying custom exploits to quickly test vulnerabilities impacting customers

CHALLENGE: TEST SECURITY SYSTEMS & PROCESSES

PCI Requirement 11: Regularly test security systems and processes

Given the near-continuous stream of vulnerabilities impacting IT systems, the PCI DSS directs companies to ensure a comprehensive testing program is in place for both systems and processes.

While customers have often relied on disparate controls – such has IDS/IPS, FIM, and AV – across Linux environments, the Capsule8 platform offers a single solution to address these requirements and ease the compliance process by:

- Providing detection and prevention that leverages workload-level data and outperforms the detection capabilities of traditional IDS/IPS
- Delivering a granular file and user policy capability, including FIM and AV, to automatically respond to threats
- Enabling custom response actions to be put in place based on the compliance requirements of your organization (e.g. kill response; quarantine, etc.)
- Replacing multiple, disparate technologies with a single, integrated platform that will secure your Linux infrastructure without compromising the integrity and performance of production environments

CAPSULE8

About Capsule8

Capsule8 is the industry's only real-time, zero-day attack detection platform capable of scaling to massive production deployments. Capsule8 delivers continuous security across your entire production environment — containerized, virtualized and bare metal — to detect and disrupt attacks as they happen.

Learn more at www.Capsule8.com.