Gigamon®

EXECUTIVE SUMMARY

Enhancing PCI DSS 4.0 Compliance with Gigamon AMI

Leveraging Deep Observability for Secure Payment Processing

Gigamon Application Metadata Intelligence (AMI) offers organizations a robust solution to meet PCI DSS 4.0 requirements. By delivering detailed network-derived application metadata, AMI complements existing security measures, facilitating effective segmentation of systems processing credit card transactions and ensuring continuous compliance monitoring.

The Payment Card Industry Data Security Standard (PCI DSS) 4.0 mandates stringent measures for protecting cardholder data, emphasizing the need for both physical and electronic segmentation of systems handling processing credit card information. Traditional security tools often rely on metrics, events, logs, and traces (MELT) data, along with endpoint detection and response (EDR) systems. Gigamon introduces a third pillar—network metadata through its Application Metadata Intelligence (AMI)—to enhance visibility and compliance efforts.

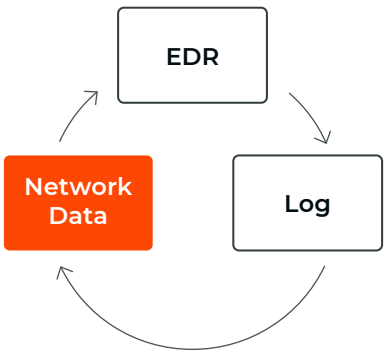

Figure 1. The three pillars of PCI.

How Gigamon Application Metadata Intelligence Assists in PCI Compliance

Gigamon AMI supports compliance across a range of PCI DSS requirements (R1 through R12) by:

- **Enabling continuous visibility**
  Provides real-time insights into system interactions, aiding in accurate scoping and segmentation of PCI environments
- **Reducing deployment time**
  Enhances understanding of system communications, streamlining planning and implementation of security controls
- **Verifying control operations**
  Ensures ongoing effectiveness of security measures, even in dynamic network environments

For example, AMI can detect outdated ciphers and monitor certificates, addressing PCI compliance requirements that include:

- **4.2.1**
  Use of strong cryptography and security protocols
- **4.2.1.1**
  Maintaining an inventory of trusted keys and certificates
- **4.2.2**
  Securing the primary account number (PAN) with strong cryptography during transmission

- **8.3.2.c**
  Ensuring authentication factors are unreadable during transmission
- **12.3.3**
  Documenting and reviewing cryptographic cipher suites and protocols in use

Additionally, AMI identifies vulnerable protocols and specific ports, supporting requirements like:

- **1.2.6**
  Defining and implementing security features for all services, protocols, and ports considered insecure
- **6.2.4**
  Detecting vulnerable protocols in bespoke and custom software

TLS Versions
Lookout for SSLv2, SSLv3, or TLS1.0

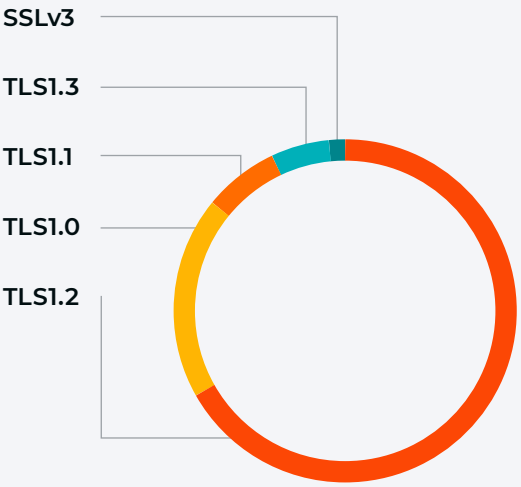

Figure 2. Certificate inventory in Gigamon dashboard.

Insecure Protocol/Service/Port
Services, protocols, or ports that transmit data or authentication credentials (for example, password/passphrase) in clear-text over the internet.

Examples of insecure services, protocols, or ports include but are not limited to:

- FTP
- IMAP
- Telnet
- SNMP v1 and v2
- POP3
- SMB v1 and v2

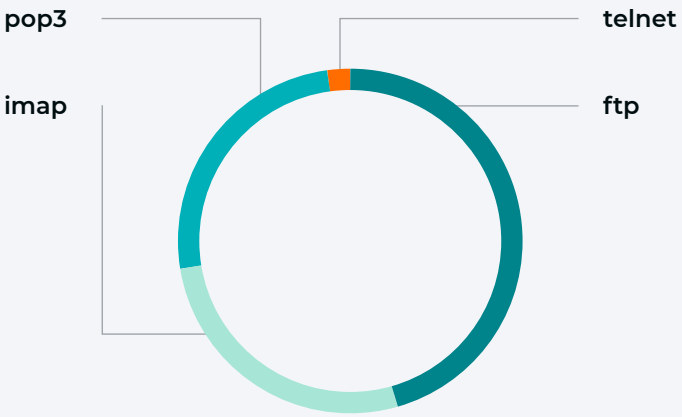

Figure 4. Visibility into insecure protocols.

Server IP	Gigamon Application Name	Days_To_Expiration	Expiration_Time
34.254.182.186	ubuntu	36	2024-06-05T09:27:54-05:00

Figure 3. Certificate expiration status.

Other Considerations

Beyond PCI mandates, organizations must address factors such as performance and shadow IT:

- **Performance**
  Gigamon, as a network packet broker, can detect sources of network slowdowns by observing conversations across various network segments, helping organizations achieve and maintain service level objectives (SLOs) or service level agreements (SLAs) for transaction processing.

- **Shadow IT and AI**
  While not directly addressed in PCI DSS, unauthorized applications—including AI applications—can introduce significant, unmeasured risks. Unauthorized applications, for example, file sharing applications, can undermine PCI DSS controls, while AI applications introduce the risk of information being leaked into public Large Language Model (LLM) databases.

  The Gigamon Deep Observability Pipeline helps organizations identify and mitigate both Shadow IT and AI risks by identifying the digital signatures of these applications and the protocols they use.

Conclusion

Gigamon AMI provides a critical third pillar of visibility, complementing MELT and EDR data. By delivering detailed network-derived metadata, AMI assists organizations in effectively deploying and verifying PCI controls, ensuring secure and compliant processing of credit card transactions.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

07.25_02