CEQUENCE

The PCI DSS 4.0 Compliance Countdown

A Surge in Attacks Signals Urgent Action

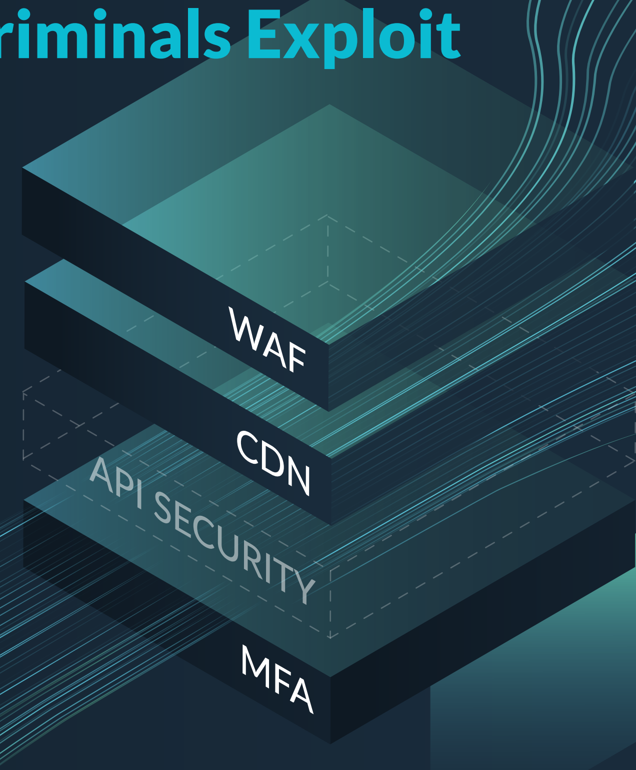
With the PCI DSS 4.0 deadline fast approaching, businesses handling cardholder data face increasing pressure not just to comply but to defend against a relentless wave of cyber threats. Attackers are targeting APIs as a primary attack vector, bypassing traditional defenses with automated fraud, credential stuffing, and payment system abuse. APIs are now the default method of connectivity in modern applications, but they also introduce new security risks. Without proper visibility and protection, attackers can exploit vulnerabilities to steal cardholder data, manipulate transactions, and drain financial accounts while remaining undetected.

Retailers and financial institutions remain top targets as fraudsters take advantage of security gaps in payment infrastructure. While PCI DSS 4.0 introduces stronger protections, addressing API security and automated threats remains a critical challenge for many organizations.

This report uncovers how cybercriminals are exploiting today's payment landscape—and what security leaders must do to protect their organizations.

The Bigger Picture: Cybercriminals Exploit Compliance Gaps

While PCI DSS 4.0 aims to modernize security requirements, many organizations are still playing catch-up. Attackers are capitalizing on:



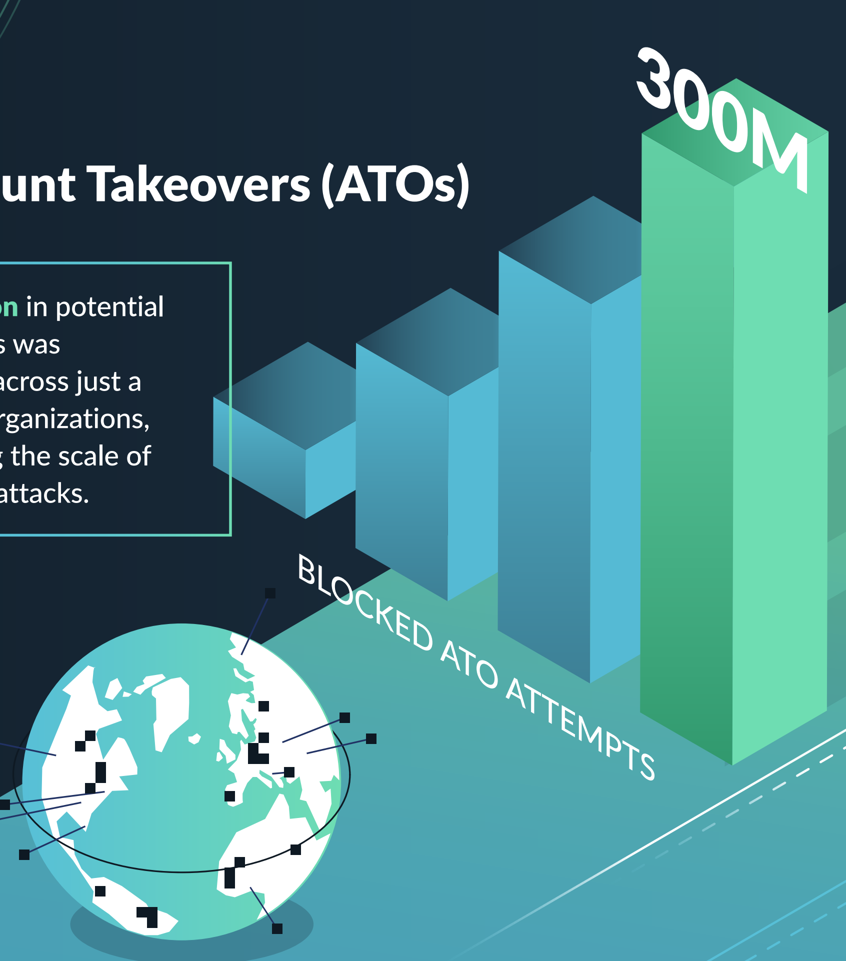
API Security Blind Spots

With an average of over **800 APIs per organization**, attackers are leveraging bot-driven abuse, credential stuffing, and token exploitation to infiltrate payment systems.

Retail's High-Stakes Battleground

Retailers bore the brunt of attacks, accounting for 66.5% of all malicious traffic. This is a clear indication that fraudsters see these businesses as easy targets due to high transaction volumes and fragmented security postures.

The Scale of Account Takeovers (ATOs)



Over 300 million ATO attempts were blocked in the last 12 months, highlighting the scale of automated credential stuffing attacks.

$121 million in potential fraud losses was prevented across just a subset of organizations, highlighting the scale of attempted attacks.

This trend aligns with a broader industry shift. Stolen login credentials remain the number one method attackers use to bypass defenses, outpacing malware-based intrusions.

Beyond ATOs: Attackers Diversify Their Strategies

While account takeovers remain the dominant threat, our data also reveals a rise in new and evolving attack techniques designed to exploit every stage of the digital payment process.

Loyalty Rewards Abuse

Over 22M attempts blocked
Attackers are treating loyalty points like cash, draining customer rewards accounts because they're easier to cash out than stolen credit cards, and often go unnoticed until it's too late.

Product Search & Pricing Abuse

822M attempts blocked
An overwhelming 89% of non-ATO attacks came from bots scraping product pricing to manipulate competitive algorithms, enable scalping tactics, and undercut legitimate retailers in real time.

Shopping Cart & Inventory Abuse

About 6M attempts blocked
Fraudsters are weaponizing automation to hoard high-demand products, creating artificial scarcity that drives up prices, then reselling at a markup. This deprives real customers and fuels black-market resellers.

Credit Verification Fraud

Over 69M attempts blocked
Criminals are mass-testing stolen card details through small, low-risk transactions before making bigger fraudulent purchases, putting millions of stolen credit cards into circulation.

The common denominator is APIs. Attackers are bypassing traditional security layers, targeting API endpoints that process cardholder data, which is a critical but often under protected attack vector.

PCI DSS 4.0 is The Wake-Up Call for Payment Security

Next Steps for Security Leaders

Many of the new PCI DSS 4.0 requirements are security 101 such as "creating and maintaining an infosec policy" and "tracking and monitoring network access." However, there are also some that either build on previous requirements or are completely new, and we cover some of the most important ones here, and how API security and bot management can help ensure compliance.

Ensure all Primary Account Number (PAN) information is encrypted when transmitted over open, public networks. Organizations should:

- ☐ Identify all API endpoints that transmit PAN
- ☐ Ensure those API endpoints are only transmitting encrypted PAN

Inspect custom application code for vulnerabilities prior to production. Use automated tools to help:

- ☐ Inventory all APIs (internal, external, third-party, etc.) and associated risk
- ☐ Test APIs and applications to identify misconfigurations or vulnerabilities prior to production
- ☐ Monitor applications and APIs for anomalous and malicious behavior

"Shift left" to avert or reduce the impact of common attacks and vulnerabilities in custom software. The proper automated software can help:

- ☐ Test APIs in pre-production and at runtime
- ☐ Shield right by proactively blocking attacks and business logic abuse in real time while you shift-left to fix vulnerabilities

Use automated, preventative controls to assess and prevent vulnerabilities in public-facing web applications and APIs from being exploited. Employ a solution that:

- ☐ Prevents both conventional attacks as well as business logic abuse and sensitive data exposure
- ☐ Identifies and proactively blocks bad traffic before it even gets to your applications

Implement change control for all production components. APIs can be harder to manage since you can't "see" them like you can regular applications. Organizations should employ tools that:

- ☐ Ensure that proper API documentation exists and is current.
- ☐ Enable easy, automated testing of any API code changes/updates in pre-production environments.

The transition to PCI DSS 4.0 is more than just a compliance milestone—it's a necessary evolution in payment security.

Attackers are adapting, and businesses must do the same. With API security blind spots, automated fraud, and credential stuffing on the rise, organizations need to move beyond compliance checkboxes and take proactive steps to protect their payment infrastructure.

Are you ready for PCI DSS 4.0?

Ensuring compliance is just the beginning. Securing APIs, mitigating bot-driven attacks, and protecting customer data require real time, automated defenses that go beyond traditional security measures.

Get a Free API Security Assessment

Understand where your vulnerabilities lie and how to strengthen your defenses before attackers exploit them. Our complimentary API security assessment provides valuable insights into your API attack surface, identifying risks and gaps in compliance with PCI DSS 4.0.

PCI DSS 4.0 & API Security: What You Need to Know

Request Your Free API Security Assessment

For tailored guidance on strengthening your API security and bot mitigation strategy, contact us today.

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai

Cequence-PCIDSS40Infographic-20250325