How to Quickly Comply with PCI DSS 4.0

Navi Gill, Senior Product Marketing Manager, F5
Jay Kelley, Senior Manager, Security Product Marketing, F5

Book A Meeting With Us!

A webinar exclusive offer...

BOOK A MEETING

Bluetooth Tracker

Book a meeting with our Connections Agent, Ella Jimenez at (e.jimenez@f5.com) and receive an F5 Bluetooth Tracker!

COMPLETE A MEETING

JBL Speaker

Complete a meeting with the F5 Account team and receive an F5 limited edition JBL speaker!

Agenda

What is PCI DSS?

What is PCI DSS v4.0?

PCI DSS and WAFs

F5 & PCI DSS

F5 WAF

Comprehensive PCI DSS Coverage from F5

Conclusions & Takeaways

Q&A

What is PCI DSS?

What is PCI DSS?

PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide

Payment Card Industry (PCI) Data Security Standard (DSS) defines security requirements to protect environments where payment account data is stored, processed, or transmitted

Sets the minimum technical and operational security requirements for compliance for organizations storing, processing, or transmitting payment card data

PCI DSS compliance can be expensive, but it's necessary

A breakdown of potential costs to obtain PCI DSS certification

Preparation costs

Employee training , infrastructure upgrades, etc.

Audit costs

Self-Assessment Questionnaire (SAQ): $5,000 to $20,000; or a Report of Compliance (ROC): $35,000 to $200,000 – annual recurring costs

Vulnerability scans

Quarterly vulnerability scans internally or by a PCI DSS-Approved Scanning Vendor (ASV): ~up to $200 per IP annually

Penetration tests

Penetration testing required for most orgs: $3,000 to $30,000, depending on org size

Compliance fees

Card service providers may charge between $70 to $120 annually to recover compliance-related expenses

However, PCI DSS non-compliance can cost even more

The costly consequences of **not** complying with PCI DSS

Non-compliance fees
~$5,000 - $100,000 **per month**!

Increased transaction fees
Up to $90 **per transaction**!

Loss of merchant license
Losing license to accept credit cards =
Serious business impact

Cost of a data breach
Investigations & legal expenses

FTC audits

Cardholder notifications

Affected customer compensation

Requirement to meet Level 1 compliance
(additional $50,000 - $200,000 annually)

And this is all before factoring in loss of reputation and revenue losses due to a breach!

What is PCI DSS v4.0?

What is PCI DSS v4.0?

PCI DSS v4.0: Developed with global industry collaboration

3
Request for comment (RFCs) on draft content

6,000+
Items of feedback received

200+
Companies provided feedback

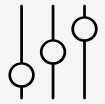
- Updates firewall terminology to network security controls to support broader range of technologies
- Requires multi-factor authentication (MFA) for all access into cardholder data environment
- Increases flexibility to demonstrate how different methods in use achieve security objectives
- Adds targeted risk analyses to allow flexibility to define how frequently certain activities may be performed

Out with the old, in with the new

PCI DSS v.3.2.1		PCI DSS v4.0
Prescriptive controls and standard requirements	→	Focused on security outcomes (custom and risk-based approach to meet security objectives)
Focused MFA for admin access to cardholder data environments	→	Expanded MFA requirements across use cases
Encryption requirements limited to certain data transmissions and storage scenarios	→	Broader requirements for encryption to address emerging threats and technologies
Standardized testing process with fixed templates	→	More robust and flexible testing procedures (targeted risk analysis and validation)
Reporting is primarily compliance-focused	→	Reporting focuses on security outcomes and continuous improvement

Source: pcisecuritystandards.org

Detailing some of the new changes in PCI DSS v4.0



Customized approach

Orgs can use alternative methods if they prove security objects are being met

Stronger passwords

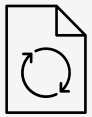
Updates password rules: longer passphrases, no forced changes unless compromised

Targeted Risk Analysis

Promotes risk analysis for adaptive security controls

Enhanced awareness and training

Adds frequent updates to training on phishing and social engineering



Monitoring and logging improvements

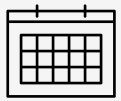
Requires continuous monitoring and automated log reviews to enhance threat detection

Cloud and third-party security

Adds cloud security and third-party service requirements

Encryption key management enhancements

Tightens encryption key and cryptographic process controls



Implementation timeline

Transition period until **March 31, 2025**

Source: pcisecuritystandards.org

PCI DSS v4.0 has 12 requirements that include security, access control, vulnerability management, and data protection

1. Implement & maintain controls for network security
2. Apply secure configurations to all system components
3. Protect stored account data
4. Protect cardholder data with strong cryptography during transmission over open, public networks
5. Protect all systems and networks from malicious software
6. Develop and maintain secure systems and software
7. Restrict access to system components and cardholder data by business need to know
8. Identify users & authenticate access to system components
9. Restrict physical access to cardholder data
10. Log & monitor all access to system components & cardholder data
11. Test security of systems & network regularly
12. Support info sec with organizational policies & programs

Why PCI DSS v4.0?

Continue to meet the security needs of the payment industry

Promote security as continuous process

Add flexibility for different methods

Enhance validation methods

Organizations now required to maintain compliance

Add new or extend existing security solutions to comply with PCI DSS v4.0

Required:
Vulnerability security assessment tools

Required:
Automated detection and prevention for web-based attacks

Required:
Client-side attack defense

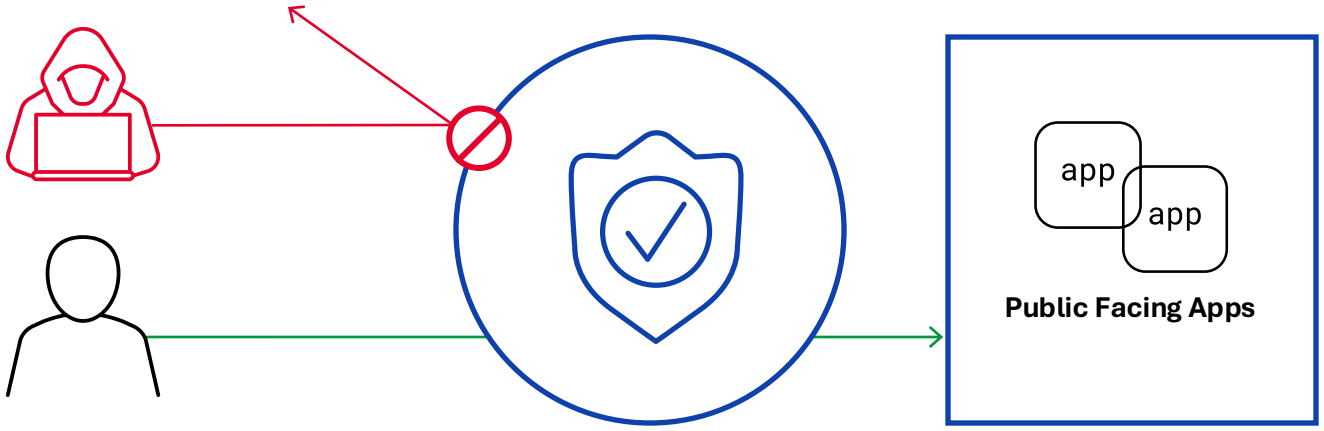
Required:
Stricter access controls & stronger auth

Required:
Anti-phishing mechanisms

Required:
Intrusion detection and/or prevention

PCI DSS and WAFs

WAFs and PCI DSS v4.0 compliance



Mandatory deployment

Requires a solution in front of public-facing web apps to detect, prevent, & alert on web-based attacks

The role of WAF

A WAF fulfills requirements by monitoring & filtering app traffic

Comprehensive protection

WAFs defend against app layer attacks like exploiting un/known vulns in code, libraries, & build tools

Broader security

WAFs mitigate risks from config flaws & automated attacks targeting payments, credentials, & installed apps

How a WAF can help attain PCI DSS v4.x compliance

Protect cardholder data

Prevent SQL injection, XSS attacks

Monitoring and logging

Enhancing encryption

Mitigating DDoS attacks

Automates updates

Source: pcisecuritystandards.org

F5 & PCI DSS

F5 is a PCI DSS v4.0 Certified Service Provider

Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data.

Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.

If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).


PCI Security Standards Council

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: F5, Inc.

Assessment End Date: 07/28/2023

Date of Report as noted in the Report on Compliance: 07/28/2023

F5 WAF

BIG-IP Advanced WAF

Distributed Cloud WAF

NGINX App Protect

F5 delivers the most comprehensive and flexible market leading WAF solution delivered wherever your apps reside

Available in different deployment models and form factors to meet any app and API security requirement

Available in multiple delivery models

Appliance, software, SaaS, and edge

Supports most deployment types

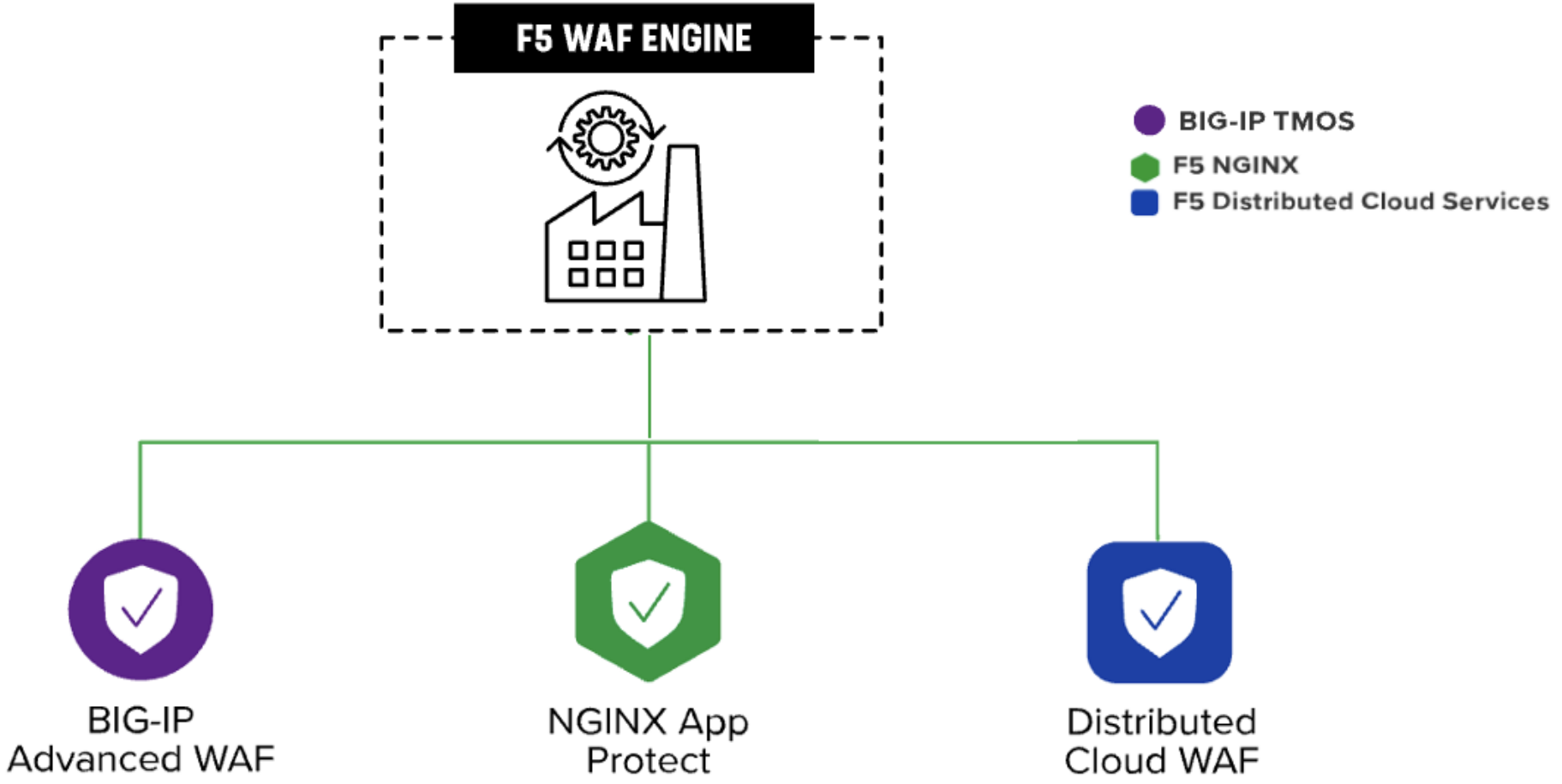
Hybrid, multicloud, on-premises/data center, VM, public cloud, private cloud, edge, and containers (Kubernetes)

Designed to protect all types of apps

Traditional, multicloud, hybrid, cloud-native, modern containerized, and microservices

All F5 WAFs share the same WAF engine

Platform-agnostic app security for distributed architectures from edge to cloud



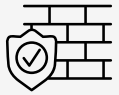
** Required after 3/31/25*

PCI DSS v4.0: Protecting web apps from attack

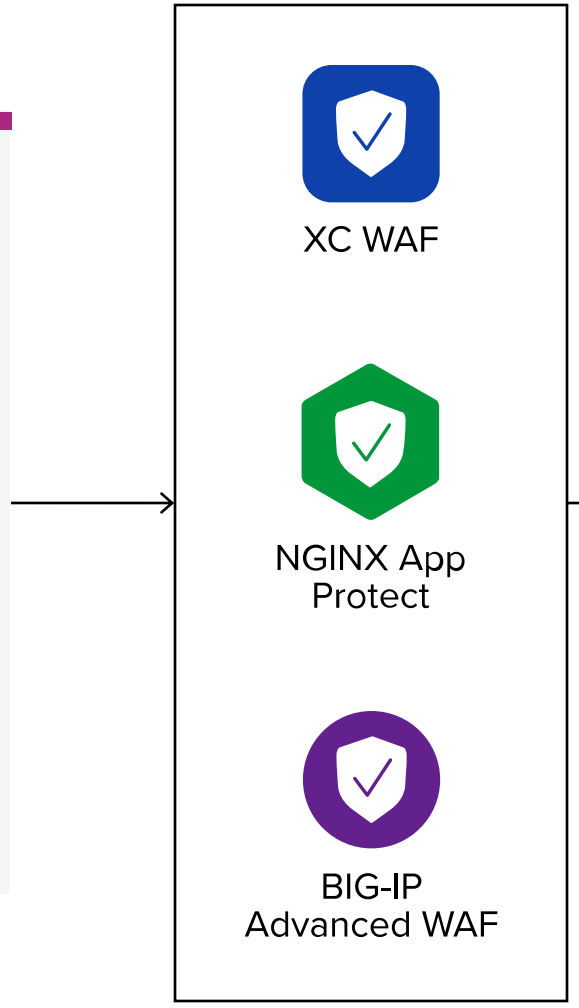
BIG-IP Advanced WAF, Distributed Cloud WAF, NGINX App Protect

3.4.1
Mask primary account number (PAN)

6.2.4
Mitigate common software attacks & vulns in software development



6.4.1, 6.4.2*
Install automated solution that continually detects & prevents web-based attacks



- AI/ML powered detection
- Signature-based attack detection
- Behavioral analysis
- User behavioral analytics
- Secures against OWASP Top 10
- CI/CD pipeline ready
- Bot mitigation
- DDoS attack protection
- IP Reputation
- Automated updates
- Rate-Limiting
- CAPTCHA
- Comprehensive logging & reporting
- Integrates with Web App Scanning

Comprehensive PCI DSS Coverage from F5

Distributed Cloud Client-Side Defense
Distributed Cloud API Security
Distributed Cloud Web App Scanning
Distributed Cloud Mobile App Shield
BIG-IP APM
BIG-IP SSL Orchestrator
BIG-IP AFM
Distributed Cloud Bot Defense
Mobile App Shield

** Required after 3/31/25*

PCI DSS v4.0: Detect & Prevent Skimming

Distributed Cloud Client-Side Defense

6.4.3*

Confirm all payment page scripts authorized

Assure integrity of payment page scripts

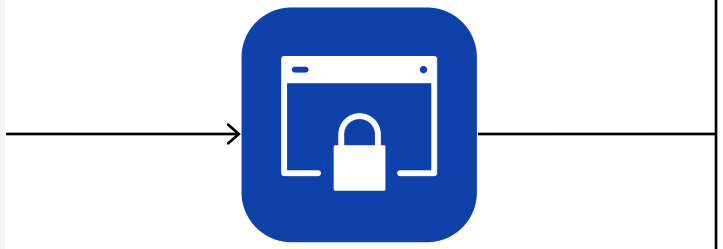
Keep inventory of scripts & justify need

11.6.1*

Alert personnel to unauthorized HTTP headers & payment page content changes

Configure to evaluate received HTTP header & payment page

Perform at least once every 7 days or periodically



XC Client-Side Defense

Prevents skimming and formjacking

Monitors client-side code for continuous and comprehensive protection against malicious JavaScript

Apply all necessary measures to safeguard personal data

Uncover suspicious data exfiltration patterns with advanced machine learning algorithms

Provides actionable alerts on unauthorized modifications via emails, SMS, Slack, & more

** Required after 3/31/25*

PCI DSS v4.0: Securing APIs

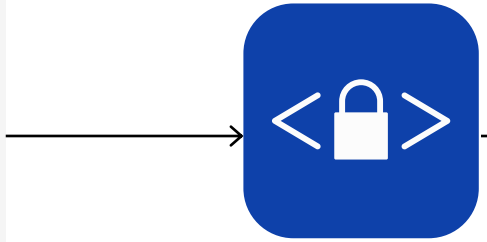
Distributed Cloud API Security

6.2.3
Pre-production or -release testing of bespoke/custom software including APIs

6.2.4
Mitigate common attacks & vulns using software engineering or other methods

6.3.2*
Maintain inventory of bespoke software & components including APIs

6.4.2*
Install automated technical solution to continually detect & prevent web-based attacks



XC API Security

- Comprehensive API discovery
- Robust API testing[1]
- Runtime protection
- Continuous monitoring & anomaly detection

[1] *Roadmap, anticipated delivery in Q2 CY25*

** Required after 3/31/25*

PCI DSS v4.0: Understanding the attack surface

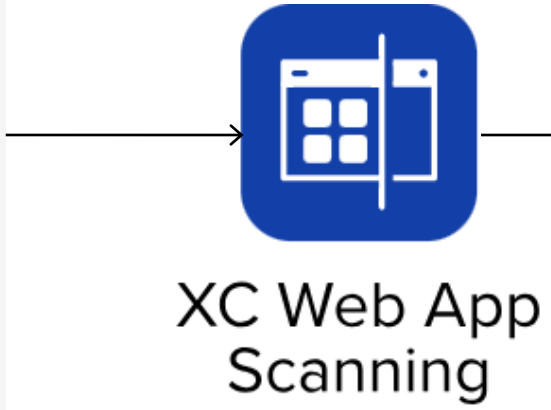
Distributed Cloud Web App Scanning

4.2.1
Maintain an inventory of software & components

6.4.1
Regular reviews for new threats & vulns in public web apps using automated app vulnerability security assessment tools

11.3.1*
Perform internal vulnerability scans & rescans as needed

11.4.1
App-layer pentesting to at least identify vulns listed in 6.2.4



External attack surface management

Automated penetration testing

Continuous visibility & vulnerability detection

* Required after 3/31/25

PCI DSS v4.0: Authentication, authorization, & securing access to cardholder data

BIG-IP Access Policy Manager (APM)

4.2.1*, 8.3.2
Strong cryptography and security to safeguard PAN over open, public networks & make all auth factors unreadable during transmission

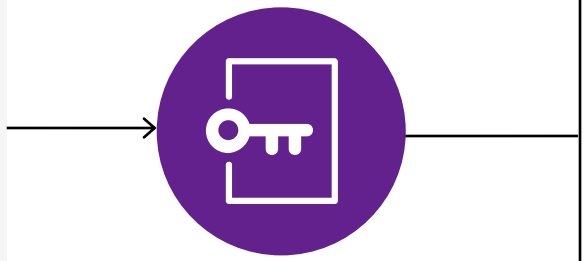
7.2.5*
Use-based & least privilege access

7.2.6*
Deploy an access control system & limit cardholder data (CHD) access

8.2.7, 8.2.8
Time-based, monitored third-party access & idle session timeout & re-auth

8.3.9
Analyze account security posture before allowing access

8.4.2, 8.4.3
Support for MFA for non-console & remote access



BIG-IP Access Policy Manager

- Zero trust application access/Identity Aware Proxy
- Use- and role-based access controls
- Least privilege access
- Policies based on time, day, inactivity, etc.
- Dynamic security posture assessment
- Secures in-transit data
- MFA & step-up authentication support

* Required after 3/31/25

PCI DSS v4.0: Addressing critical control system failures

BIG-IP SSL Orchestrator

5.4.1*
Processes & automated mechanisms in place to detect & protect against phishing attacks

10.7.2*
Detect, alert, & address failures of critical security control systems

10.7.3*
Prompt response to critical security control system failures & quick restoration

11.5.5.1*
For service providers only: Detect IDS and/or IPS techniques, alert on/prevent, & address covert malware communication channels

BIG-IP SSL Orchestrator

Orchestrate traffic through the security stack

Monitor health of security stack solutions

Mitigate impact by active bypass of offline solutions

Address security service changes/insertions by seamless traffic transfer without interrupting traffic flow

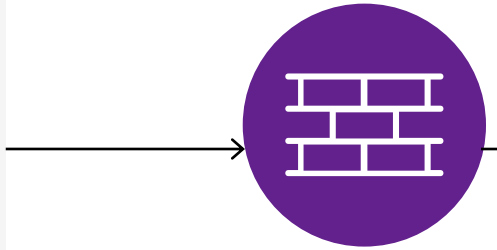
Defend against outbound traffic dispersing malware, exfiltrating data, or communicating with command-and-control (C2) channels

* Required after 3/31/25

PCI DSS v4.0: Addressing critical control system failures

BIG-IP Advanced Firewall Manager (AFM)

11.5.1*
Intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network



BIG-IP Advanced Firewall Manager

Performs Layer 5 - 7 inspection of all incoming traffic to adhere to protocol standards & match against known attack signatures

Protects DNS infrastructure against protocol attacks and exploits

PCI DSS v4.0: Securing mobility

Distributed Cloud Bot Defense & Distributed Cloud Mobile App Shield

XC Bot Defense

F5 Distributed Cloud Bot Defense

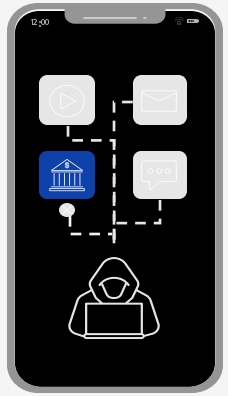
Significantly reduce bot attacks

Protect APIs

Reduce login attacks by 96%

Reduce app fraud costs by 30%

XC Mobile App Shield



F5 Distributed Cloud Mobile App Shield

Prevent repackaging

Stop runtime attacks

Meet compliance requirements

F5 helps you meet and maintain compliance with PCI DSS v4.0

Add new or leverage your existing F5 investments for quick, comprehensive compliance!

XC Web App Scanning

Required: Vulnerability security assessment tools

XC WAF

XC API Security

BIG-IP Advanced WAF

NGINX App Protect

Required: Automated detection and prevention for web-based attacks

XC Client-Side Defense

Required: Client-side attack defense

BIG-IP Access Policy Manager

Required: Stricter access controls & stronger auth

BIG-IP SSL Orchestrator

Required: Anti-phishing mechanisms

BIG-IP Advanced Firewall Manager

Required: Intrusion detection and/or prevention

Key Takeaways

The 3 things to remember!

If you don't remember anything else from this session, this is what you need to remember

1. **The time is now!!**
   Deadline: March 31, 2025!
2. **Strengthen payment security & validation**
3. **F5 helps you address PCI DSS v4.0 compliance!**

Book A Meeting With Us!

A webinar exclusive offer…

BOOK A MEETING

Bluetooth Tracker

- Book a meeting with our Connections Agent, Ella Jimenez at (e.jimenez@f5.com) and receive an F5 Bluetooth Tracker!

COMPLETE A MEETING

JBL Speaker

- Complete a meeting with the F5 Account team and receive an F5 limited edition JBL speaker!

Q&A