# Welcome to the TPA Webinar Series

The Payments Academy

Education, Collaboration, Leadership

May 18, 2026

# The Payments Academy

Education, Collaboration, Leadership

## Foundational Supporters

@rrowpayments

Bluefin®

CAMPUSGUARD®

J.P.Morgan

Nacha

# Scripting Attacks in Finance:

## How Cyber Threats Target Payments & What You Can Do


**Presented by:**

- Pete Campbell – Manager, Security Advisor Services
  CISA, CISSP, QSA
- Matt McGuirk, Senior Director, Global Head of Field Engineering, Source Defense


CAMPUSGUARD®

May 18, 2026

# Presenters

**Pete Campbell**
Manager, Security Advisor Services, CISA, CISSP, QSA

**Matt McGuirk**
Senior Director, Global Head of Field Engineering, Source Defense

CAMPUSGUARD™

# About CampusGuard

- Founded in 2009
- IT Security & Compliance Firm
- Customer Focused Model
- Focused on Higher Ed and other Campus-Based Environments
- RedLens InfoSec & Treasury Services

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council
APPROVED SCANNING VENDOR

# What Is E-Skimming?

**The Threat**

- E-skimming (also known as a Magecart attack) is the silent injection of malicious JavaScript into a website's payment or form pages.
- The code captures sensitive data (card numbers, names, addresses) in real time as users type and exfiltrates it to attacker-controlled servers.
- The institution and its users have no idea the theft is occurring.

**Why Higher Ed Is a Target**

- University websites are high-traffic, payment-accepting environments with complex third-party script ecosystems
- Scripts include analytics tools, tag managers, chat widgets, and donation platforms, making them attractive and difficult to defend.

# The PCI Compliance Challenge

Two new requirements, mandatory as of **March 31, 2025**, directly target e-skimming and are catching institutions off guard

**Req. 6.4.3: Payment Page Script Management** Every JavaScript file on a payment page must be inventoried, justified, and integrity-protected.

**Req. 11.6.1: Tamper Detection** Institutions must actively monitor payment pages for unauthorized script or header changes, at a minimum weekly.

**The Confusion:** Many institutions assume that outsourced payment processors or tokenization solutions remove them from scope.

In reality, any page in the payment flow that loads third-party scripts may still be in scope, which is far less clear than most compliance teams believe.

# Real-World Risks to Your Institution

**Reputational Damage**
Public breach disclosure erodes trust with students, families, donors, and accreditors

→

**Student & Donor Financial Harm**
Stolen card data hits the people your institution serves most directly—those making tuition payments or charitable gifts

↓

**Regulatory & Legal Exposure**
State breach notification laws, potential FTC scrutiny, and class action litigation can extend for years at significant cost

→

**PCI Non-Compliance Penalties**
Card brand fines, mandatory forensic audits at your expense, and in severe cases, loss of card processing privileges

↓

**Operational Disruption**
Incident response pulls IT, legal, finance, and communications into weeks of unplanned, resource-intensive crisis work

→

**Vendor Liability Ambiguity**
Attacks often originate through third-party scripts; most vendor contracts don't clearly assign responsibility, leaving the institution exposed

# ScriptSafe

- Provides real-time threat detection, protection and prevention of vulnerabilities originating in JavaScript
- Full visibility and protection
- Security and Date Privacy Assurance
- Rapid Deployment & Easy Management
- Supports compliance for PCI DSS 6.4.3 and 11.6.1
- Powered by Source Defense

ScriptSafe

# Protecting Data at the Point of Capture


Rounding out web security at the client-side

Protecting against theft *and* inadvertent data leakage

Addressing a majorly overlooked area of third-party risk management

Supporting zero-trust initiatives

Supporting compliance with PCI DSS, HIPAA, FFIEC and more

# Leading the Industry to Combat Fraud

## PCI BOARD OF ADVISORS

Guiding and shaping PCI DSS Standards as part of 2025-2027 Board. Working alongside VISA, Mastercard, Discover, and AmEx

## PCI PPO

Premier sponsor of PCI Security Standards Council, exclusive access to Executive Committee setting the PCI DSS Standards

## eCOMMERCE GOVERNANCE TASK FORCE

Source Defense was a core part of the team asked to clarify the new PCI DSS 4.X standards for easy and rapid adoption

## SMALL MERCHANT TASK FORCE

Source Defense was asked to take a leadership position ensuring solutions for the unserved SMB market

## PCI COMPLIANT

PCI Compliant Service Provider under SAQ-D with an Attestation of Compliance provided by IBM

## Leading the Industry Together

verizon — Co-author, 2024 Verizon PSR

fiserv. — Reselling Source Defense

VIKINGCLOUD — OEM Source Defense for Level 3 and 4

INTERSEC WORLDWIDE — Cyber Threat Intel, PFI Partnership

## Engaged with the Brands

AMERICAN EXPRESS, VISA, MasterCard, DISCOVER

# Mastercard's Global Partner in Digital Skimming Defense

source DEFENSE

Securing the backbone of eCommerce against eSkimming attacks

Driving down risk and fostering trust in digital commerce

Identifying active campaigns, disrupting fraud schemes, enriching global threat intelligence

# JavaScript:

## The Root Cause of Client-side Security Problems

source DEFENSE

**Client-Side security, specifically data leakage prevention and eSkimming protection starts with JavaScript**

**JavaScript can perform any action and behave in any way it wants on any site where it is running (over 97% of all websites)**

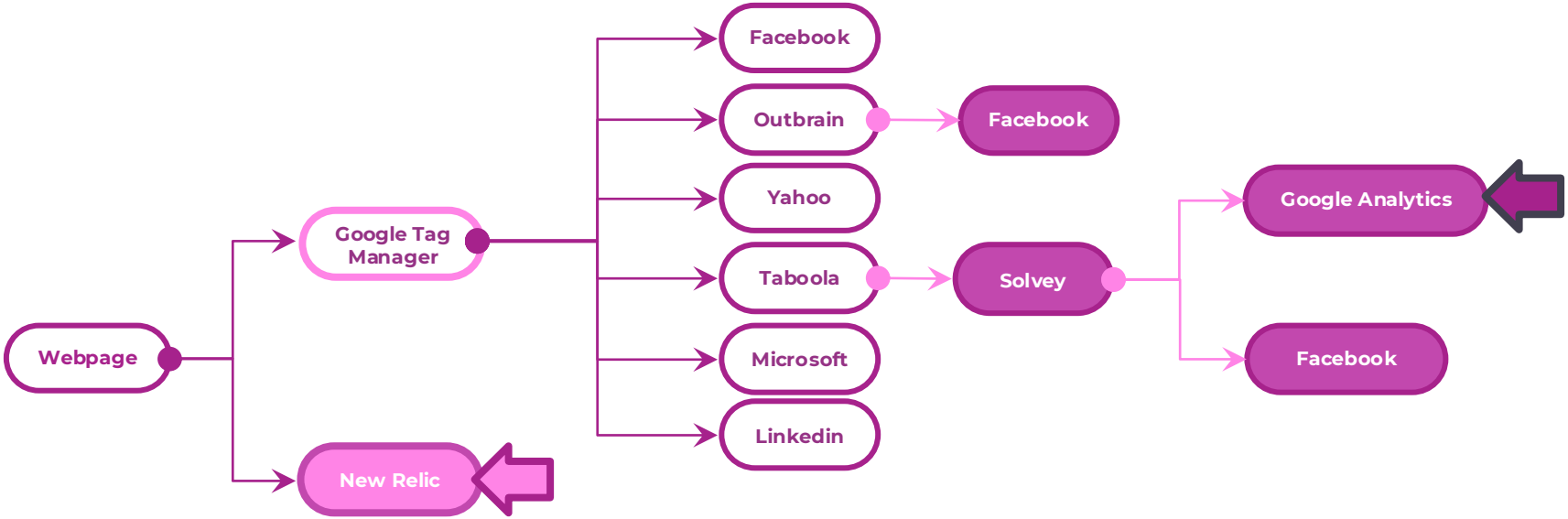
**JavaScript has no native security controls**

**Attacks that use JavaScript**

- Magecart (brand name)
- eSkimming (PCI terminology)
- Digital Skimming (Mastercard terminology)
- Formjacking, Credential Harvesting, etc.

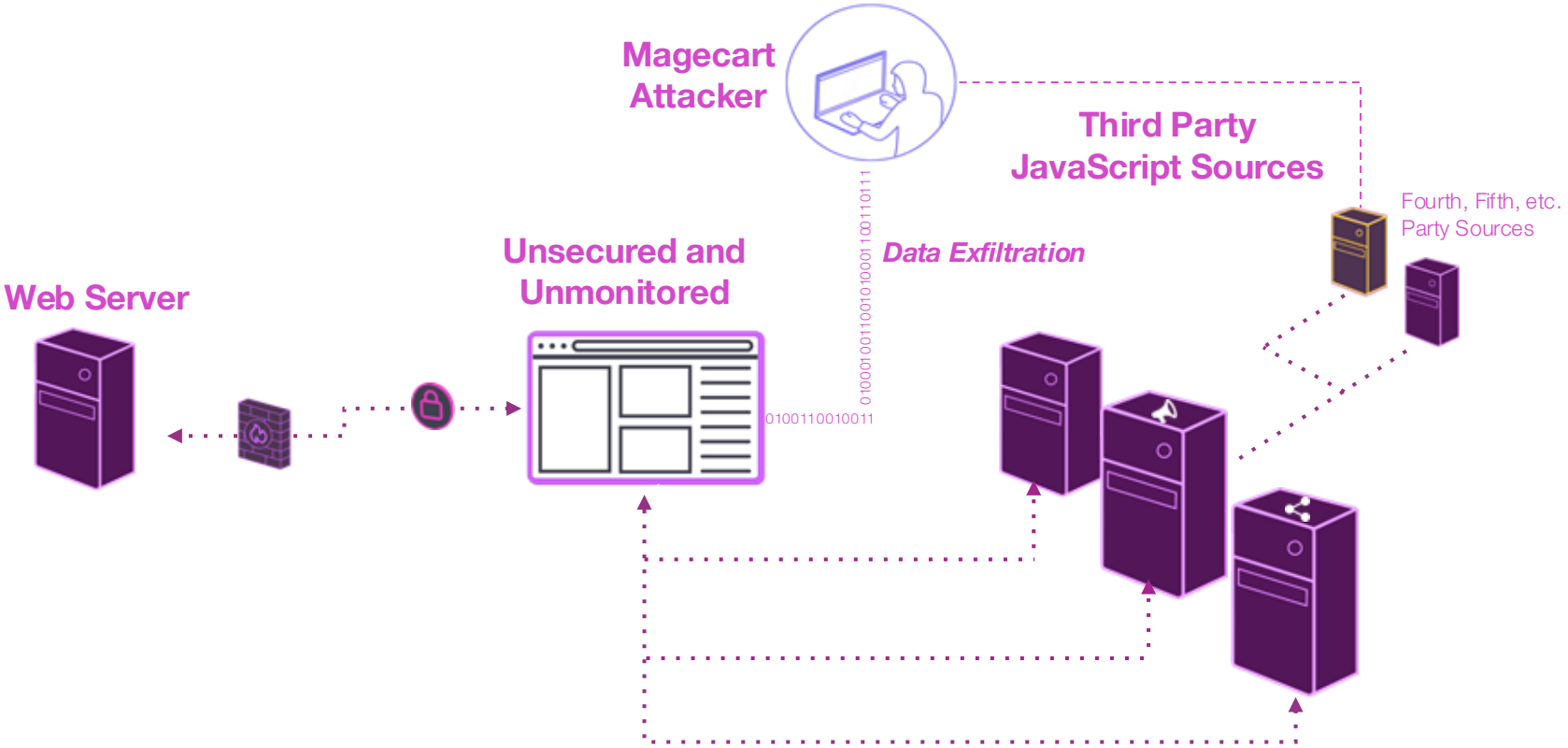
# What is a Client-Side Supply Chain Attack?

source DEFENSE



# Anatomy of a Client-Side Attack

source DEFENSE



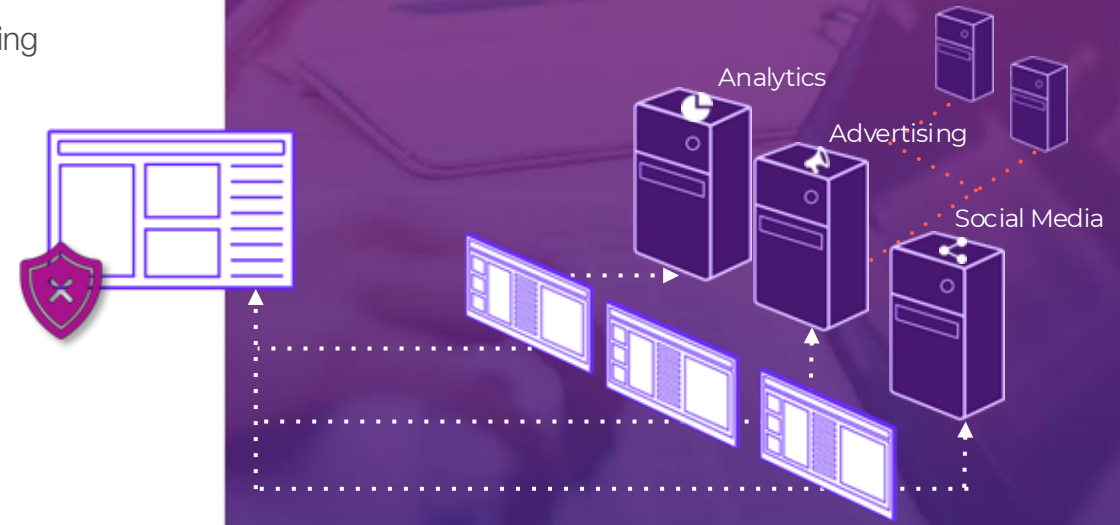
# CampusGuard ScriptSafe

Managing your client-side code, protecting your visitors and customers

- **Isolate** foreign scripts from the web page
- **Block** harmful activities such as eSkimming style attacks
- **Ensure** beneficial behavior
- **Thwart** attacks in real-time
- Securely **integrate** 3rd party code **with minimal effort**

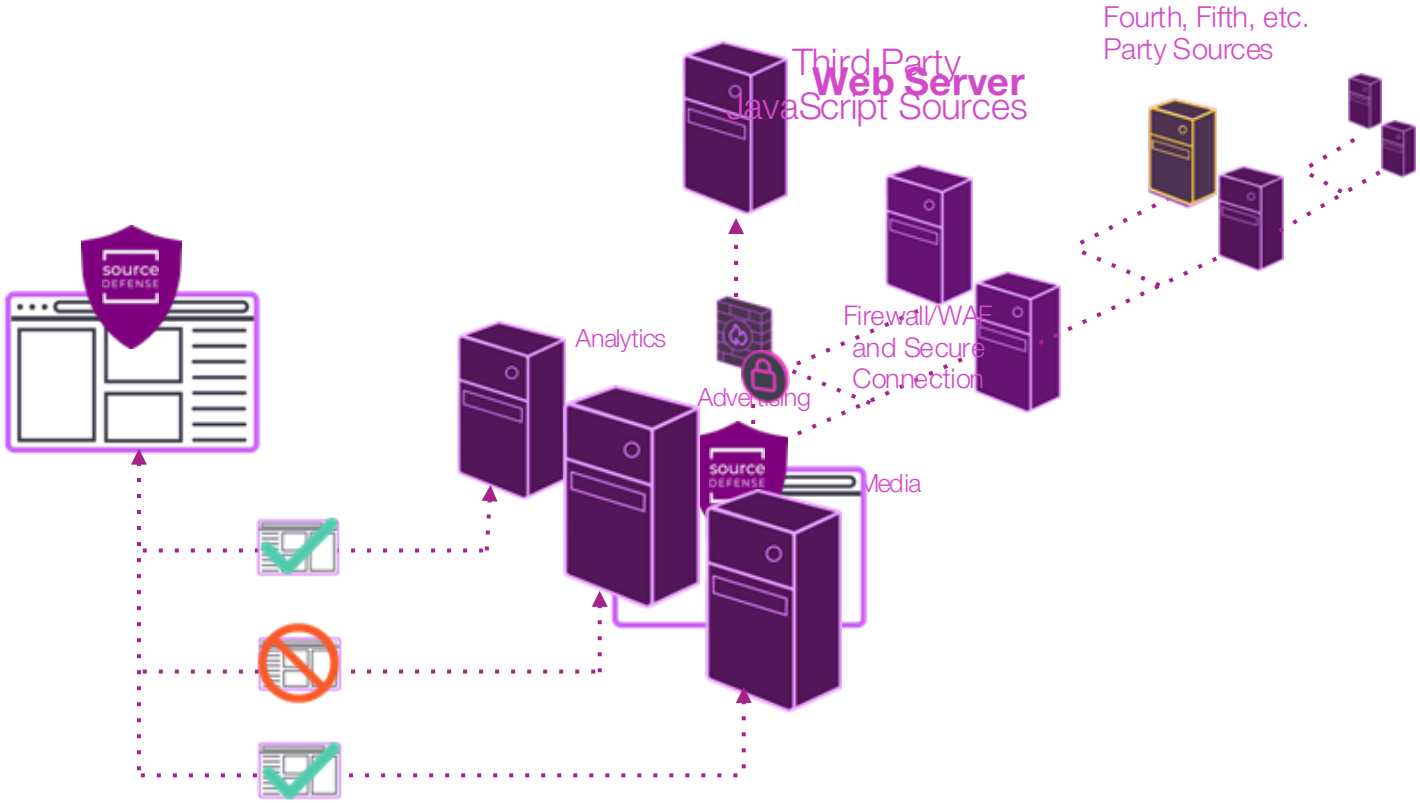
source DEFENSE

## REAL-TIME CODE CONTROL AND SUPPLY CHAIN VISIBILITY



# CampusGuard ScriptSafe

Real-time Client-Side Security



# Patented Prevention

In-line - Real-Time - Behavior-Based

## PROTECT | Proactive Data Protection

**Simple Deployment:**
Technology is actively deployed and running inside every browser session

**Real-Time Prevention:**
Allows legitimate script behaviors while blocking data leakage and malicious activity

**Fraud Disruption:**
Fraudulent data theft is prevented before the attack can execute


## DETECT | Immediate Fraud Detection

**No Integration Required**:
No client-side code deployment, allowing for rapid, wide-scale rollout

**Immediate Detection:**
Detects malicious activity & fraudulent data theft the instant it happens

**Actionable Intelligence:**
Data is returned via API, alerts, and UI for manual response or CTI

# Set-and-Forget Security…

source DEFENSE

Days to test

Hours to deploy

No new teams to hire / dedicate to management

Material risk reduction for a low-cost investment

# Questions?

Contact us for questions and more information:


Pete Campbell, CampusGuard

pcampbell@campusguard.com

www.campusguard.com


CAMPUSGUARD®

# The Payments Academy

Education, Collaboration, Leadership

If you have suggestions for a future webinar, please complete the Feedback Survey

Recordings of the 2025 and 2026 webinars are posted on the TPA website

| Date | Foundational Supporter | Topic/Title |
|---|---|---|
| November 12, 2025 | Bluefin | Securing the Future:<br>Protecting Higher Education from Data Breaches |
| January 14, 2026 | Arrow Payments | Fighting E-Commerce Fraud |
| February 11, 2026 | Nacha | ACH Rules for 2026 and Beyond |
| March 11, 2026 | J.P. Morgan | Instant Payments Unveiled:<br>Path to Success and Pitfalls to Avoid |
| April 8, 2026 | CampusGuard | Beyond the PCI Compliance Checklist:<br>Building Stronger Payment Security |

# The Payments Academy

Education, Collaboration, Leadership

## Save the Date for Next Year's TPA Conference

**St. Louis, Missouri, May 2 – 5, 2027**

Join The Payments Academy mailing list by clicking **JOIN OUR MAILING LIST** on our website - thepmtsacademy.org