Source Defense Case Study
Nextiva

Streamlining PCI DSS 4.0.1 Compliance While Strengthening eSkimming Security

How a global customer experience leader achieved automated compliance and enhanced digital supply chain visibility with Source Defense

EXECUTIVE SUMMARY

Nextiva, a leading Unified Customer Experience Management SaaS provider serving over 100,000 businesses globally, partnered with Source Defense to meet PCI DSS 4.0.1 requirements 6.4.3 and 11.6.1 while strengthening their overall eSkimming security posture. Facing the challenge of managing third and fourth-party scripts across their payment infrastructure without proper visibility, Nextiva needed a solution that could deliver both compliance automation and enhanced threat monitoring capabilities.

FULL COMPLIANCE

Achieved full PCI DSS 4.0.1 compliance within one week of implementation

AUTOMATED PROCESS

Transformed complex resource-intensive compliance project into streamlined automation

ENHANCED VISIBILITY

Unprecedented visibility into digital supply chain across entire web ecosystem

Source Defense's platform enabled Nextiva to achieve **full PCI DSS 4.0.1 compliance within one week of implementation**, transforming what could have been a complex, resource-intensive compliance project into a streamlined, automated process. Beyond meeting regulatory requirements, the partnership provided Nextiva with unprecedented visibility into their digital supply chain, positioning them to expand their security monitoring capabilities across their entire web ecosystem.

CLIENT PROFILE

COMPANY DETAILS

- **Company:** Nextiva
- **Industry:** Customer Experience Technology / SaaS
- **Headquarters:** Scottsdale, Arizona
- **Founded:** 2008
- **Global Reach:** 100,000+ businesses served worldwide with operations across seven countries

Nextiva has established itself as a global innovator in unified customer experience technology, operating a comprehensive SaaS platform that enables businesses to deliver superior customer interactions. With international operations spanning **India, the United Kingdom, Spain, Ukraine, Mexico, Poland, and Canada,** Nextiva's digital infrastructure supports complex, multi-jurisdictional payment processing requirements.

As a SaaS provider where trust forms the foundation of customer relationships, Nextiva operates under the principle that their platform must deliver secure, reliable, and scalable experiences. This commitment to security excellence drives their proactive approach to compliance and risk mitigation, making them an ideal candidate for advanced eSkimming security solutions.

THE CHALLENGE

Limited Visibility into Digital Supply Chain Risk

Prior to implementing Source Defense, Nextiva faced a critical gap in their security architecture: they lacked comprehensive insight into the third and fourth-party scripts operating on their payment pages. This blind spot introduced significant uncertainty and risk into their payment processing infrastructure.

INCOMPLETE SCRIPT VISIBILITY
No comprehensive inventory of third and fourth-party scripts executing on payment pages

REGULATORY COMPLIANCE PRESSURE
Urgent need to meet PCI DSS 4.0.1 requirements 6.4.3 and 11.6.1 by the March 2025 deadline

RISK AMPLIFICATION
Operating without visibility into the behavior and security posture of digital supply chain partners

COMPLIANCE COMPLEXITY
Need for a solution that could streamline compliance demonstration to assessors

THE GROWING ESKIMMING THREAT LANDSCAPE

While Nextiva had not experienced direct security incidents, the company recognized that operating without proper eSkimming visibility represented an unacceptable risk level. As highlighted in Source Defense's research with Verizon, **the average website now contains over 18 third-party scripts**, with financial and payment-processing platforms often hosting significantly more. Each script represents a potential attack vector that traditional server-side security measures cannot protect against.

THE SOLUTION

Comprehensive Evaluation Process

Nextiva conducted a thorough evaluation of multiple solutions designed to address PCI DSS 4.0.1's new eSkimming security requirements. During this assessment, Source Defense distinguished itself through several key factors:

DIRECT PCI DSS 4.0.1 SUPPORT

Source Defense provided explicit support for both requirement 6.4.3 (Payment Page Script Management) and 11.6.1 (Tamper Detection for Web Pages), ensuring comprehensive compliance coverage.

USER-FRIENDLY IMPLEMENTATION

The solution's straightforward, intuitive design minimized complexity while delivering enterprise-grade security capabilities.

COMPREHENSIVE MONITORING CAPABILITIES

Beyond basic compliance requirements, Source Defense offered the ability to monitor third and fourth-party scripts across Nextiva's entire web ecosystem, not just payment pages.

IMMEDIATE VALUE DEMONSTRATION

During the proof of concept phase, Source Defense partnered with Nextiva to scan their existing environment, providing immediate, actionable insights that demonstrated the platform's value proposition.

RAPID DEPLOYMENT AND INTEGRATION

The implementation process exemplified Source Defense's commitment to minimal operational disruption and includes exceptional customer support with precise instructions and proactive assistance:

1
WEEK
Full deployment completed within one week

2
LINES OF CODE
Simple two-line code implementation

1
INTEGRATION
Minimal, with only Okta integration required

"Implementing Source Defense was a smooth process. The customer support team at Source Defense demonstrated exceptional professionalism and efficiency. They provided precise instructions, which streamlined the implementation."

- Bruce Walton, Senior Information Security Manager

WHY SOURCE DEFENSE

Industry-Leading eSkimming Security Expertise

Nextiva's selection of Source Defense was driven by several compelling factors that align with Source Defense's position as the pioneer in eSkimming security:

PROVEN PCI DSS 4.0.1 EXPERTISE

As a Principal Participating Organization with the PCI Security Standards Council, Source Defense played an active role in developing the very requirements Nextiva needed to meet. This deep regulatory involvement translated into a solution purpose-built for compliance success.

COMPREHENSIVE THIRD-PARTY VALIDATION

Source Defense's effectiveness has been independently validated by leading security assessors including CoalFire and VikingCloud, providing Nextiva with confidence in their solution selection.

TECHNOLOGY INNOVATION

Source Defense's patented real-time JavaScript sandboxing technology delivers capabilities unavailable from other vendors, providing both prevention and detection capabilities that address the full spectrum of eSkimming threats.

PARTNERSHIP APPROACH

Rather than simply delivering a technology solution, Source Defense demonstrated a genuine partnership approach, working collaboratively with Nextiva to understand their specific environment and requirements.

source DEFENSE

RESULTS
Automated PCI DSS 4.0.1 Compliance

Source Defense delivered immediate, measurable results that transformed Nextiva's compliance posture:

COMPLIANCE AUTOMATION

- Requirements 6.4.3 and 11.6.1 compliance fully automated

- Streamlined compliance demonstration to assessors

- Clear compliance status visibility through the PCI Dashboard

OPERATIONAL EFFICIENCY

- Eliminated manual script inventory and monitoring processes

- Reduced compliance-related workload on security and IT teams

- Automated reporting and documentation generation

ENHANCED VISIBILITY

- Complete inventory of all third and fourth-party scripts

- Real-time monitoring of script behavior and changes

- Comprehensive understanding of digital supply chain risk

"Complying with Requirements 6.4.3 and 11.6.1 is completely automated thanks to Source Defense. The latest PCI Dashboard provides a clear overview of the compliance status across all of our payment pages."

\- Bruce Walton, Senior Information Security Manager

PARTNERSHIP EXCELLENCE

Beyond technical capabilities, Source Defense demonstrated exceptional partnership value:

RESPONSIVE SUPPORT
Prompt, comprehensive responses to all inquiries

ONGOING COLLABORATION
Regular communication focused on expanding and improving application usage

CONTINUOUS IMPROVEMENT
Platform enhancements that make monitoring even more efficient

BUSINESS IMPACT
Strategic Value Delivery

The partnership with Source Defense has delivered significant strategic value to Nextiva across multiple dimensions:

RISK MITIGATION

While Nextiva had not previously experienced eSkimming security incidents, the implementation of Source Defense has effectively eliminated the uncertainty and risk associated with unmonitored third-party scripts.

COMPLIANCE CONFIDENCE

The automated compliance capabilities provide Nextiva with complete confidence in their ability to demonstrate PCI DSS 4.0.1 adherence to assessors, eliminating compliance-related operational stress.

CUSTOMER TRUST ENHANCEMENT

By implementing comprehensive eSkimming security measures, Nextiva can provide additional assurance to their users regarding continued PCI compliance and security, reinforcing the trust that forms the foundation of their customer relationships.

OPERATIONAL SCALABILITY

The minimal management requirements (typical Source Defense clients spend **around an hour per month** managing the platform) allow Nextiva to maintain comprehensive security without straining their security operations team.

FUTURE GROWTH ENABLEMENT

Perhaps most significantly, the partnership has positioned Nextiva for expanded security capabilities:

Planned Expansion:

- Leverage Source Defense for broader code supply chain understanding
- Extend monitoring beyond payment pages to encompass the entire web ecosystem
- Develop more sophisticated threat detection and response capabilities

Strategic Partnership:

- Regular communication with Source Defense to identify optimization opportunities
- Collaborative approach to expanding application usage
- Access to platform enhancements and new capabilities

CONCLUSION

Nextiva's partnership with Source Defense exemplifies how organizations can transform complex compliance challenges into strategic security advantages. By selecting a proven industry leader with deep regulatory expertise and innovative technology, Nextiva achieved automated PCI DSS 4.0.1 compliance while establishing a foundation for comprehensive eSkimming security.

The success of this implementation demonstrates several key principles:

THE VALUE OF EXPERTISE
Partnering with the pioneer in eSkimming security, a company that helped develop the very standards requiring compliance and delivered both immediate results and long-term strategic value.

THE IMPORTANCE OF PARTNERSHIP
Source Defense's collaborative approach, exceptional support, and commitment to ongoing improvement transformed a vendor relationship into a true strategic partnership.

THE POWER OF AUTOMATION
By automating compliance requirements that could have consumed significant security team resources, Source Defense freed Nextiva to focus on broader security and business objectives.

THE FOUNDATION FOR GROWTH
Rather than simply solving an immediate compliance need, the partnership established a platform for expanded security capabilities and enhanced digital supply chain visibility.

For organizations seeking to address PCI DSS 4.0.1 requirements while building comprehensive eSkimming security capabilities, Nextiva's experience demonstrates the strategic value of partnering with Source Defense. The combination of proven technology, regulatory expertise, and exceptional partnership approach delivers both immediate compliance success and long-term security enhancement.

"We recommend Source Defense as a robust and user-friendly application that provides comprehensive insights into the website code supply chain and identifies potential risks within that chain. Source Defense effectively assists in meeting PCI requirements 6.4.3 and 11.6.1 seamlessly. Source Defense has proven to be an excellent partner."

- Bruce Walton, Senior Information Security Manager

Ready to transform your eSkimming security posture like Nextiva?

Achieving PCI DSS 4.0.1 compliance and maintaining protection against eSkimming threats doesn't have to be complex, resource-intensive, or disruptive to your business. Contact Source Defense today to discover how our proven platform can deliver automated compliance and comprehensive digital supply chain protection for your organization. It's the smarter, easier way to meet the mandate and secure against eSkimming - without the headaches.

As a member of the PCI Board of Advisors, a PCI Participating Organization and the pioneer in eSkimming security, Source Defense plays a leadership role related to the requirements for web security found in PCI DSS 4.0.1.

We've helped more than a thousand of the world's leading brands address these issues. We've also been educating merchants, PSPs, eCommerce platform providers and QSAs on the vulnerabilities in modern website designs that make eSkimming attacks possible; providing guidance around ambiguity in the standard; advising on the pros and cons of guidance provided by the council, and have made available a free assessment, monitoring and management solution for both merchants and QSAs.

Schedule a Demo with a Security Expert Today!
https://sourcedefense.com/request-demo/