DATA SHEET

CloudWave | BlueOrange Compliance Penetration Testing Services

See Your Environment Through an Attacker's Eyes

INTRODUCTION

Hospitals and healthcare organizations face constant threats from cybercriminals seeking to disrupt operations, steal sensitive data, or hold systems for ransom. Firewalls, antivirus, and MFA are important first steps, but they don't answer the most critical question: *Could an attacker still break in?*

CloudWave | BlueOrange Compliance penetration testing provides that answer. Our experts — certified Offensive Security Certified Professionals (OSCP) with deep healthcare experience — simulate real-world attacks to reveal how an adversary could exploit your systems, applications, and people. The result is actionable insight you can use to close security gaps, strengthen compliance, and protect patient care.

Our certified Offensive Security Certified Professionals (OSCP) simulate real-world attacks to reveal how an adversary could exploit your systems, applications, and people.

TYPES OF PENETRATION TESTS

We tailor our testing to your unique environment, with tiered options that scale to your security maturity:

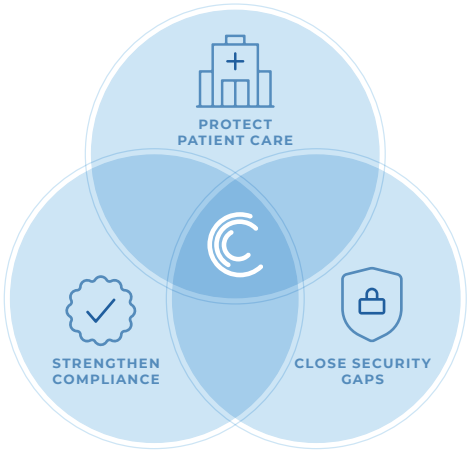
Internal Network Penetration Testing
Identifies exploitable weaknesses within your internal environment — simulating insider threats or compromised devices.

External Network Penetration Testing
Targets internet-facing assets to uncover misconfigurations, unpatched systems, or open services that attackers could use to gain access.

Web Application Testing
Evaluates custom and third-party applications for vulnerabilities that could expose data or compromise functionality.

Human Risk Testing (Phishing & Social Engineering)
Measures employee readiness with phishing simulations and other techniques to identify gaps in awareness and training.

Tiered Testing Options
From foundational assessments to advanced, customized scenarios, we deliver the right level of rigor for your organization's needs.



METHODOLOGY

Our penetration testing follows a structured, standards-based approach aligned with NIST frameworks:

1. **Planning** – Define objectives, scope, and rules of engagement collaboratively with your team.
2. **Scanning** – Perform reconnaissance and identify vulnerabilities using automated and manual techniques.
3. **Accessing** – Attempt entry via phishing, credential misuse, or direct network exploitation, depending on scope.
4. **Exploiting** – Simulate attacker behavior to determine how far an intrusion could spread and what data could be exposed.
5. **Analyzing & Reporting** – Deliver both executive-level insights and detailed technical findings, including compliance scoring and a prioritized remediation roadmap.

REPORTING & DELIVERABLES

At the end of every penetration test, you'll receive more than just a technical report — you'll get the clarity and guidance needed to strengthen your security posture and prove your due diligence. CloudWave | BlueOrange Compliance provides deliverables for both executives and technical teams, ensuring findings are understood and actionable across your organization.

Your deliverables include:

- **Executive Summary** – High-level overview of test results, risks identified, and business impact for leadership.
- **Detailed Technical Report** – Comprehensive findings with exploit details, screenshots, and references mapped to industry standards.
- **Prioritized Remediation Roadmap** – Step-by-step guidance on how to address vulnerabilities, ranked by severity and business risk.
- **Compliance Scoring** – Alignment of findings to HIPAA, PCI-DSS, and NIST Cybersecurity Framework requirements.
- **Optional Retesting** – Validation that fixes have been successfully implemented and risks eliminated.
- **Debriefing Session** – Live review with our experts to answer questions, clarify next steps, and help your teams act with confidence.

CloudWave | BlueOrange Compliance provides deliverables for both executives and technical teams, ensuring findings are understood and actionable across your organization.

BENEFITS

With CloudWave | BlueOrange Compliance penetration testing, you gain more than a report — you gain a clear path to resilience:

- **Actionable Outcomes** – Detailed remediation guidance, optional engineer-assisted support, and retesting to validate fixes.
- **Compliance Alignment** – Supports HIPAA, PCI-DSS, and NIST Cybersecurity Framework requirements.
- **Cyber Insurance Readiness** – Demonstrates proactive risk management, often required for coverage.
- **Operational Protection** – Reduce the risk of downtime, financial loss, and reputational damage.
- **Executive & Technical Value** – Results include leadership-focused summaries as well as technical findings for IT and security teams.

YOU'LL ACHIEVE THESE OUTCOMES

Every penetration test engagement is designed to leave you with not just a list of vulnerabilities, but a clear path to improvement. With CloudWave | BlueOrange Compliance, you'll walk away with confidence in where your defenses stand, what needs attention, and how to prioritize next steps.

You'll gain:

- A clear view of how attackers could exploit your systems, applications, or users.
- Practical, prioritized remediation guidance with optional retesting to confirm fixes.
- Stronger alignment with compliance frameworks including HIPAA, PCI-DSS, and NIST.
- Validation of your current security investments through real-world testing.
- Insight into staff awareness and readiness through phishing and social engineering campaigns.
- Documentation to support regulators, partners, and cyber insurance requirements.
- Reduced risk of downtime, data loss, and reputational harm through proactive defense.

ABOUT CLOUDWAVE

CloudWave is a full-service cybersecurity and cloud services provider built exclusively for healthcare. Protecting over 350 hospitals and health system environments, CloudWave delivers end-to-end solutions that combine secure hosting, IT operations, and 24/7 threat detection and response. Services include managed security, risk and compliance, disaster recovery, systems management, and cloud optimization—all delivered with a healthcare-first mindset. Powered by AI-driven security operations and supported by U.S.-based Network and Cybersecurity Tactical Operations Centers, CloudWave provides a cyber-ready foundation for safe, uninterrupted patient care.

ABOUT BLUEORANGE COMPLIANCE

BlueOrange Compliance, a CloudWave company, is a leader in information privacy and security, regulatory compliance, and risk management services. Together with CloudWave, BlueOrange Compliance delivers end-to-end cybersecurity solutions for healthcare organizations facing increasingly complex compliance landscapes, including HIPAA, HITECH, OCR, and other industry-specific regulations.

The combination of our proven track record in compliance audits, risk assessments, cybersecurity testing and training, and cybersecurity consulting and risk management services along with CloudWave's advanced threat detection, incident response, and cloud infrastructure capabilities results in a comprehensive set of offerings that empower healthcare organizations to secure sensitive data, streamline compliance efforts, and mitigate evolving cyber threats.