



C1 Cyber Visibility WAVES Assessment

Proactive Security for Modern Enterprises

Comprehensive Security Simplified

In today's complex digital environments, organizations face significant challenges in gaining full visibility into their IT infrastructure. Blind spots in asset inventory, unmonitored devices, and misconfigured systems create vulnerabilities that cybercriminals can exploit. Without continuous visibility into internal and external assets, organizations are exposed to security breaches, compliance violations, and operational inefficiencies.

The C1 Cyber Visibility WAVES Assessment provides organizations with comprehensive insights into their entire IT environment, enabling proactive identification of security risks and vulnerabilities. This solution delivers an in-depth understanding of an organization's attack surface through advanced asset discovery, vulnerability detection, and actionable risk prioritization.

Leveraging C1's Advisory WAVES methodology, this assessment goes beyond traditional audits by uncovering hidden assets, misconfigurations, and compliance gaps. The result is a tailored security roadmap that empowers organizations to mitigate risks, strengthen compliance, and optimize security operations—all without disrupting business workflows.

The C1 Advantage: Proactive Cyber Visibility and Risk Mitigation

Comprehensive Asset Discovery

Complete Inventory: Identify all IT, cloud, and endpoint assets across hybrid and multi-cloud environments.

Agentless Discovery: API integrations with over 900+ IT and security tools for seamless, real-time asset visibility.

Shadow IT Detection: Discover unmanaged or unauthorized devices and applications.

Actionable Security Insights

Risk Prioritization: Vulnerabilities are evaluated based on real-world risk, enabling focused remediation efforts.

Policy Validation: Validate security policies and configurations against industry best practices.

Automated Recommendations: Receive tailored, prioritized action plans to address critical security gaps.



Proactive Risk Management

Continuous Monitoring: Ongoing visibility into asset changes, misconfigurations, and emerging vulnerabilities.

Attack Surface Management: Consolidate internal and external asset data for complete risk assessment.

Incident Response Readiness: Accelerate forensic investigations with detailed asset and vulnerability data.

Enhanced Compliance and Reporting

Compliance Alignment: Supports regulatory standards such as HIPAA, PCI-DSS, and GDPR.

Audit-Ready Reports: Detailed executive and technical reports for compliance and security oversight.

Risk-Based Dashboards: Visualize security posture with real-time risk metrics and vulnerability trends.

Operational Efficiency and Cost Optimization

Reduced IT Burden: Simplifies asset management and vulnerability tracking to free up IT resources.

Optimized SaaS Usage: Identify and eliminate redundant or underutilized SaaS licenses to reduce costs.

Streamlined Operations: Integrates with existing security tools to minimize complexity.

Core Solution Components

Comprehensive Inventory: Accurate, real-time asset tracking across cloud, on-prem, and hybrid environments.

Lifecycle Management: Monitor software and hardware End-of-Life (EOL) to avoid unpatched systems.

Device Discovery: Identify unknown or unmanaged devices with automated scanning.

Vulnerability and Threat Detection

Security Gap Analysis: Detect misconfigurations and missing security controls.

Vulnerability Prioritization: Focus on the most critical risks with contextualized insights.

Attack Surface Management: Consolidated internal and external asset views for risk reduction.



Compliance and Risk Reporting

Audit-Ready Reports: Executive-level summaries and technical documentation for compliance reviews.

Continuous Compliance Monitoring: Real-time tracking of compliance requirements and security controls.

Risk-Based Dashboards: Visual insights into vulnerabilities and remediation progress.

Policy Validation and Automation

Automated Policy Checks: Validate security policies and automate compliance checks.

Custom Remediation Plans: Tailored action items for quick and effective risk mitigation.

Integration with IT and Security Tools: Enhances existing security investments through seamless integration.

Why Choose C1?

Proven Expertise: C1's Advisory WAVES methodology ensures comprehensive and actionable assessments.

Operational Simplicity: Seamlessly integrates with over 900+ IT and security tools.

Proactive Risk Mitigation: Prioritized risk insights and automated recommendations.

Compliance Confidence: Supports industry compliance standards with audit-ready reporting.

Cost Efficiency: Reduces unnecessary SaaS spend and optimizes IT resources.

C1 Cyber Visibility WAVES Assessment: Seamless Execution in 5 Steps

Discover: Complete asset inventory across hybrid and multi-cloud environments.

Analyze: Identify vulnerabilities, misconfigurations, and security gaps.

Prioritize: Contextual risk analysis with actionable, prioritized remediation steps.

Validate: Automate policy checks and validate security controls.

Optimize: Implement recommendations for ongoing risk reduction and compliance.

Get Started Today with C1 24/7 Threat Monitoring and Incident Response

C1's 24/7 Threat Monitoring and Incident Response provides continuous protection, enabling your organization to detect and mitigate threats in real-time.

Contact a C1 Security Expert for a free consultation or request a demo:

onec1.com/what-we-do/security/cybersecurity/risk-mitigation/waves