



DATASHEET (CORE SECURITY)

Core Impact

Penetration testing software to safely uncover and exploit security weaknesses

Core Impact empowers organizations to proactively minimize risk and protect critical assets by using the same techniques as today's threat actors to assess their infrastructure's security posture. This powerful platform provides a unified environment for managing all phases of the penetration testing process, from reconnaissance to reporting.

Intuitive User Interface

Core Impact features a thoughtfully designed interface, providing a straightforward layout for even advanced testing:

- **Interactive Attack Map** – Follow tests in real time, with a visual overview of attack chains, pivot points, and other activities.
- **Dynamic Dashboards** – Tailor dashboards to display details on hosts, vulnerabilities, exploits, and other key metrics.
- **Structured Workspaces** – Stay organized with a centralized container for deploying, managing, and tracking engagements.
- **Report Generation** – Easily create clear, consistent reports to plan and prioritize remediation efforts.

Automated Workflows and Rapid Testing

Core Impact's Rapid Penetration Tests (RPTs) are pre-configured sequences that automate common penetration testing scenarios to simplify and accelerate testing:

- **Convenient Wizards** – Get step-by-step guidance throughout testing, with prompts for required input and configuration options.
- **Secure Agents** – Inject agents into a target host for remote execution of tasks including information gathering, web application crawling, privilege escalation, and more.
- **Multi-Vector Testing** – Test across the IT environment, including network, web application, and endpoints.
- **Effortless Retesting** – With consistently reproducible tests, quickly verify that remediation measures or compensating controls are effective and working.

Library of Core Certified Exploits

Core Impact boasts a diverse **library of commercial-grade exploits**, crafted and validated by Core Security's in-house security researchers. This up-to-date collection addresses a wide spectrum of vulnerabilities, spanning platforms including Windows, Linux, network appliances, and web applications. These exploits provide an OPSEC-safe method to demonstrate how chains of exploitable vulnerabilities open paths to an organization's mission-critical systems and assets.

PRODUCT SUMMARY

KEY FEATURES

- Intuitive automation for deploying advanced level tests
- Extensive library of expert-developed and certified exploits
- Multi-vector testing capabilities
- Ransomware simulation
- NTLM relay attack simulation
- Tailored reporting to build remediation plans
- Powerful integrations with other pen testing tools and more than 20 vulnerability scanners
- Robust safety features, including fully encrypted, self-destructing agents

PLATFORMS MONITORED

- Operating Systems like Windows, Linux, and Mac
- Cloud (Public, Private, Hybrid)
- Databases
- Web Services
- Network Appliances
- Software Applications
- Your Critical Data

SYSTEM REQUIREMENTS

- Windows 10 Enterprise 64 bit
- Windows 10 Pro 64 bit
- Windows Server 2016 Standard

Proving Compliance with Industry Regulations

Core Impact provides an easy-to-follow and established automated framework that can support industry requirements and standards. For example:

- **PCI-DSS** – Test systems handling cardholder data and generate PCI DSS-compliant reports
- **CMMC** – Helps provide proof of compliance for CMMC Level 4 or higher
- **GDPR** – Supports data protection impact assessments (DPIAs) required for systems processing personal data of EU residents
- **NIST** – Aligns tests with NIST's security controls catalog and generates report that maps to MITRE ATT&CK framework

Attack Technique Use Cases

Core Impact offers diverse testing functionality so organizations know who, how, and what is vulnerable in their IT environments.

NTLM Relay Attacks

Use the coercer module to trigger authentication attempts from target systems. From there, use the NTLMrelayx module to relay these connections to other systems and automatically run an attack module to install an agent, generate certificates, run LDAP queries, and more.

Phishing Campaigns

Deploy phishing campaigns to discover which users are susceptible and what credentials can be harvested. Easily create emails, select targets, and choose between browser redirects or web page clones. Challenge users with more sophisticated, tailored spear-phishing emails that are harder to identify as fake.

Ransomware Simulator

Pair phishing campaigns with the ransomware simulator and mimic the behavior of multiple ransomware families, encrypting user-specified files using a fully reversible symmetric key. Security teams can create and leave an explanatory README file once the exercise has been completed.

Layered Security with OffSec Interoperability

Core Impact offers interoperability with multiple other security assessment solutions to enable operational continuity for multi-stage engagements. Users can even create a structured testing methodology and consolidate vendors by bundling solutions.

Vulnerability Scanners

Core Impact's one-step test can quickly validate the results of over 20 different third-party scanners, including Fortra VM, Nessus, and or BurpSuite. After you complete a scan against your environment, Core Impact can evaluate the scan's output and provide a prioritized validation of your infrastructure's weaknesses.

Red Teaming Tools

With its Python-based framework, Core Impact is not only extendable, it can also serve as the central console. Instead of switching back and forth between tools, additional solutions can also be incorporated to further expand your testing program, such as Cobalt Strike, OST, Metasploit, PowerShell Empire, and Plextrac.

Vulnerability Scan Validation*

• Acunetix Web Vulnerability Scanner • Burp Suite Professional • CenZic	• Fortra VM • GFI LANguard • HP WebInspect • IBM Enterprise Scanner • IBM Internet Scanner	• IBM Rational AppScan • McAfee Vulnerability Manager (formerly McAfee Foundstone)	• Microsoft Baseline Security Analyzer • nCircle • Nessus	• Nexpose • Nmap • NTOSpider • OpenVAS • Patchlink VMS • Qualys Guard	• Qualys Web Application Scanner • Retine • SAINT • STAT Guardian	• Tenable Security Center • Tenable Vulnerability Management • Tripwire IP360
---	--	---	---	--	--	---

**A vulnerability scanner is not required to use Core Impact*

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.