FORTRA

DATASHEET (Cybersecurity)

Core Impact

Penetration testing software to safely uncover and exploit security weaknesses

Core Impact uses the same techniques as today's threat actors to efficiently test the security of an IT infrastructure to help minimize risk and protect valuable assets. With the help of guided automations, organizations can discover, test, and report in just a few simple steps.

Simple Enough for Your First Test, Powerful Enough for the Rest

Core Impact's Rapid Penetration Tests (RPTs) are intuitive wizards that enable testers to swiftly conduct penetration tests. Users can efficiently execute common tasks, saving time while providing a consistent, repeatable process for their testing infrastructure. Additionally, Core Impact allows you to quickly re-test exploited systems to verify that remediation measures or compensating controls are effective and working.

Leverage a Robust Library of Core Certified Exploits

Using an up-to-date library of commercial-grade exploits, developed and tested by Core Security's own cybersecurity experts, Core Impact reveals how chains of exploitable vulnerabilities open paths to your organization's mission-critical systems and assets. In addition to internally written exploits, Core Security partners with ExCraft Labs to provide add-on packs for supplementary SCADA, medical, and IoT exploits, on top of the standard exploits included with Core Impact.

Centralize Your Pen Testing Toolkit and Maximize Testing Visibility

Gather information, exploit systems, and generate reports, all in one place. Every phase of the penetration test process can be executed and managed from a single console with an intuitive dashboard. Instead of switching back and forth between tools, additional solutions can also be integrated or incorporated to further expand your testing program, such as Cobalt Strike, OST, Metasploit, PowerShell Empire, and Plextrac. This centralization not only simplifies the testing process, not having to manually compile documentation, but it also makes reporting more consistent and efficient.

PRODUCT SUMMARY

KEY FEATURES

- Intuitive automation for deploying advanced level tests
- Extensive and reliable library of certified exploits
- Multi-vector testing capabilities
- Teaming capabilities in a collaborative workspace
- 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 including 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

For those that prefer a more visual experience, users can enjoy Core Impact's interactive attack map as their central workspace. This network graph view displays a real-time overview of attack chains, pivoting and any other activities completed during testing, providing visual insight that allows security teams to better determine the best path forward in the testing engagement.

Common Core Impact Use Cases

Core Impact offers diverse testing functionality in order to provide thorough coverage and security insight so organizations know who, how, and what is vulnerable in their IT environments.

Proving Compliance with Industry Regulations

Multiple regulations require organizations have regular assessments of their security infrastructure to ensure sensitive data is properly protected. Core Impact provides an easy to follow and established automated framework that can support industry requirements and standards, including PCI-DSS, CMMC, GDPR, and NIST. For example, the NIST reports map alignment with both the MITRE ATT&CK framework and NIST's catalog of security and privacy controls. Additionally, Core Impact's reporting capabilities can help prove adherence to regulations during internal or external audits.

Conduct Network and Web Application Tests

Accurately identify and target internal information systems for network penetration testing. Core Impact can help exploit vulnerabilities in critical networks, systems, hosts, and devices by imitating an attacker's methods of access and manipulating data, as well as testing defensive technologies' ability to stop attacks.

Run web application penetration tests to find weaknesses through detailed web crawling, pivoting attacks to web servers, associated databases, and backend networks to confirm exploitability.

Conducting Ransomware and Phishing Simulations for Increased Security Awareness

Easily deploy phishing campaigns for client-side social engineering tests to discover which users are susceptible and what credentials can be harvested. Use the step-by-step process to 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.

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.

Validating Vulnerabilities Surfaced Through Scanners

Core Impact's one-step test can quickly validate the results of over 20 different third-party scanners, including beSECURE, Frontline VM, Nessus and 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.

Vulnerability Scan Validation*

- Acunetix Web Vulnerability Scanner
- beSECURE
- Burp Suite Professional
- Cenzic
- Frontline VM
- GFI LANguard
- HP WebInspect
- IBM Enterprise Scanner
- IBM Internet Scanner
- IBM Rational AppScan
- McAfee Vulnerability Manager (formerly McAfee Foundstone)
- Microsoft Baseline
- nCircle
- Nessus
- Nexpose
- Nmap
- NTOSpider
- Patchilnk VMS
- Qualys Guard
- Qualys Web Application Scanner
- Retine
- SAINT
- STAT Guardian
- Tenable Security Center
- 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.