FORTRA

DATASHEET *(Cybersecurity)*

Offensive Security-Essentials Bundle

Frontline VM and Core Impact

Frontline Vulnerability Manager (Frontline VM™) and Core Impact are two robust security tools designed to evaluate business critical networks and infrastructure for security vulnerabilities.

Though both tools work to identify and prioritize security weaknesses, each offers unique strengths and distinct features. Frontline VM is a SaaS vulnerability management solution, mostly used for performing intelligent network scanning. Core Impact is a penetration testing tool, typically used for exploitation and lateral movements in various environments.

This document provides an overview of the key functionalities of each of these tools and how they can be used together to amplify your security testing efforts.

Frontline Vulnerability Manager

Risk Scoring

Frontline VM's determines the severity of the vulnerabilities discovered in an environment, evaluates how those affect assets, and uses that information to calculate an overall security rating score called Security GPA. Vulnerability severity has a five-level scale from trivial to critical and is determined based on an estimate of how much damage an attack would have on the confidentiality, integrity, and availability of the asset on which the vulnerability exists. Asset ratings are based on the highest-level vulnerabilities discovered on a given asset.

Active View

While individual scans target specific assets, the Active View dashboard provides an aggregate view of a network and discovered vulnerabilities based on data consolidated from all previous scans to provide a more comprehensive overview of the security state of an environment. Additionally, trending graphs enable users to keep track of existing vulnerabilities, providing information like vulnerability age and remediation time trends.

Vulnerability Details

Frontline VM provides thorough information on the vulnerabilities that are identified including instance data that provides proof of the vulnerability's existence on a network. Each discovered vulnerability also comes with vulnerability details, including class, severity level, and, when available, steps for remediation.

Core Impact

Vulnerability Exploitation

Core Impact exploits security weaknesses associated with networks, people, web applications, endpoints, Wi-Fi, and SCADA environments. Using an up-to-date library of commercial-grade exploits, Core Impact reveals how chains of exploitable vulnerabilities open paths to your organization's mission-critical systems and assets.

Multi-Vector Testing

Core Impact can test across the environment. Network pen tests 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. Web application pen tests find weaknesses through web crawling, pivoting attacks to web servers, associated databases, and backend networks to confirm exploitability. Client-side social engineering tests deploy phishing campaigns to discover which users are susceptible and what credentials can be harvested.

Remediation Validation

Core Impact stores previous testing sessions, which can be quickly and easily rerun in order to validate that remediation efforts, such as new compensating controls, are effective.

Seamless Integrations

By combining vulnerability management and pen testing, businesses get the security essentials needed to proactively protect their networks. Core Impact users can import scanner data from Frontline VM and automatically validate vulnerabilities to determine if any of these vulnerabilities can be exploited and identify what business-critical assets and data can be accessed through that exploit. By integrating these tools, security teams are provided with real-world risk context that can intelligently guide plans for remediation.

Core Impact and Frontline VM integrate seamlessly, providing centralization that can reduce console fatigue and increase efficiency. Having multiple tools from Fortra's large portfolio of cybersecurity solutions simplifies your security, allowing you to save time with one point of contact and access to the same best-in-class support.

Features and Functionality

While these tools have clear differences, they are both used for assessing cybersecurity risk, so there are understandably a few features that overlap. However, even these overlapping features have their own distinctions within each tool.

Automation

Frontline VM can be scheduled to run scans automatically. Users can set preferred scanning times when determining the type of scan they would like to run. Scans are easily configurable, though several types of scans are built-in, including application discovery, host discovery, and port scanning. The ability to automate these scans removes the risks associated with manually generated scans.

Core Impact also provides automation capabilities using Rapid Penetration Tests (RPTs), which are intuitive wizards that provide step-by-step guidance throughout the pen testing process. There are multiple types of RPTs to help simplify testing, including information gathering, initial attacks, privilege escalation, and vulnerability validation.

Prioritization

Frontline VM uses multiple sources of threat intelligence and proprietary technology to determine the risk level of vulnerabilities identified in the scanning process. It also provides the context needed for businesses to understand their own risk appetite and be able to prioritize the vulnerabilities that pose the greatest risk to their unique environments.

Core Impact uses imported data from vulnerability scanners and its own information gathering capabilities to exploit vulnerabilities using the same methods as attackers in order to determine how much risk a security vulnerability may pose to that specific environment.

Comprehensive Reporting

Frontline VM provides detailed vulnerability and patch management reports. These asset-specific documents are highly customizable, with multiple filtering options to allow users to tailor their report for different security needs, including compliance audits.

Core Impact tracks and logs all actions taken during a testing session, including actions taken on remote hosts. Users can then leverage the simple and intuitive reporting templates to auto-populate pertinent data from the logs.

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.