FORTRA™

DATASHEET *(Cybersecurity)*

Infrastructure Protection for Proactive Security

The modern threat landscape demands that organizations do more than just defend against cyber attacks. They must anticipate attacks before they happen and proactively adapt their cybersecurity strategy.

Our Infrastructure Protection suite allows your organization to identify and prioritize the risks that truly pose the biggest threat to your infrastructure. You'll gain actionable insight into what steps are needed to fix security gaps and where reinforcement is required. The result is a more efficient and more effective cybersecurity program that can protect your organization and eliminate weaknesses before they are exploited.

Vulnerability Management & Assessment

Vulnerability management tools help to identify, evaluate, and report on security weaknesses that may be putting your organization at risk. Easy to deploy, low maintenance, and scalable, these solutions should help simplify your security.

Fortra VM

Encapsulating the best of our Frontline VM and beSECURE VM solutions, this risk-based vulnerability management solution utilizes proprietary scanning technology to perform comprehensive security assessments that also prioritize and track results. It also enables continuous scanning for network and application vulnerabilities, using specialized methodologies and daily updates to catch 99.9% of detectable vulnerabilities

- **Web Application Scanning (WAS)**
  This web application scanning tool provides insight into the security state of your organization's web applications, a list of prioritized vulnerabilities, and technical recommendations.
- **Active Threat Sweep (ATS)**
  Quickly and reliably analyzes assets for active threat activity and indications of compromise. This tool reduces dwell time and provides coverage for devices without traditional endpoint protection.
- **Black Box Fuzzing**
  beSTORM uses dynamic application security testing and fuzz testing to assess applications, protocols, or hardware for code weaknesses, all without needing access to source code.

Penetration Testing Tools and Services

Penetration testing tools allow cybersecurity professionals to safely validate the exploitability of security weaknesses before a malicious attacker does. Automated solutions can guide testers on techniques and methods, centralize testing, and generate reports that can aid in remediation efforts.

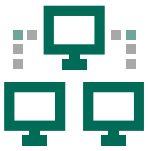
Pen Testing Software

The Core Impact penetration testing software allows you to safely test your environment using the same tactics as today's threat actors. Operators can use a certified exploit library to gain a foothold or pivot throughout a target environment, determining the likeliest attack path across network infrastructure, endpoints, web, and applications.

Pen Testing Services

For organizations that need to outsource penetration testing, we offer pen testing services that include network and infrastructure penetration testing, web application penetration testing, wireless penetration testing and more.

Adversary Simulation



Adversary simulation tools help test the security posture of an organization to see how it will fare against real-world attacks. Typically, red teams use a portfolio of tools to help them run advanced engagements that can bypass defensive measures and detection tools, move laterally, escalate privileges, achieve persistence, exfiltrate data, and more.

Cobalt Strike

With this advanced threat emulation tool, companies can model the tactics and techniques of a quiet long-term embedded threat actor in an IT network. Ideal for performing post-exploitation tasks, Cobalt Strike can be easily modified with custom scripts, adjustable attack kits, and user-created extensions.

Outflank Security Tooling (OST)

This red team tooling suite was assembled and developed by experts exclusively for experienced red teams. It provides coverage for every aspect of an engagement, with tools for initial breach, lateral movements, privilege escalation, achieving persistence, and final exfiltration.

Professional Security Services

Our cybersecurity experts offer a consultative approach, ensuring you get services tailored to your particular needs. With several different teams available, organizations can get fresh perspectives without having to change vendors.

Professional Security Services

This trusted team of certified experts works closely with vulnerability management to perform assessments that help organizations safeguard their IT infrastructure from cyber-attacks through exercises that highlight security gaps. Their offerings include web application and network pen testing, physical security testing, social engineering, and wireless security testing.

Security Consulting Services

This advanced security team can provide new ways to improve your security, including increasing user awareness, finding new vulnerabilities, circumventing access controls, and finding paths to compromise high-value assets that were not explored before. Their offerings include pen testing, software and application security testing, and red team exercises.

Red Teaming Services

These experienced red teamers with diverse specializations focus on collaborative engagements to leave organizations better prepared. Their offerings include red teaming and attack simulation, advanced penetration tests, incident response, SOC support, advisory, and blue team training.

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.