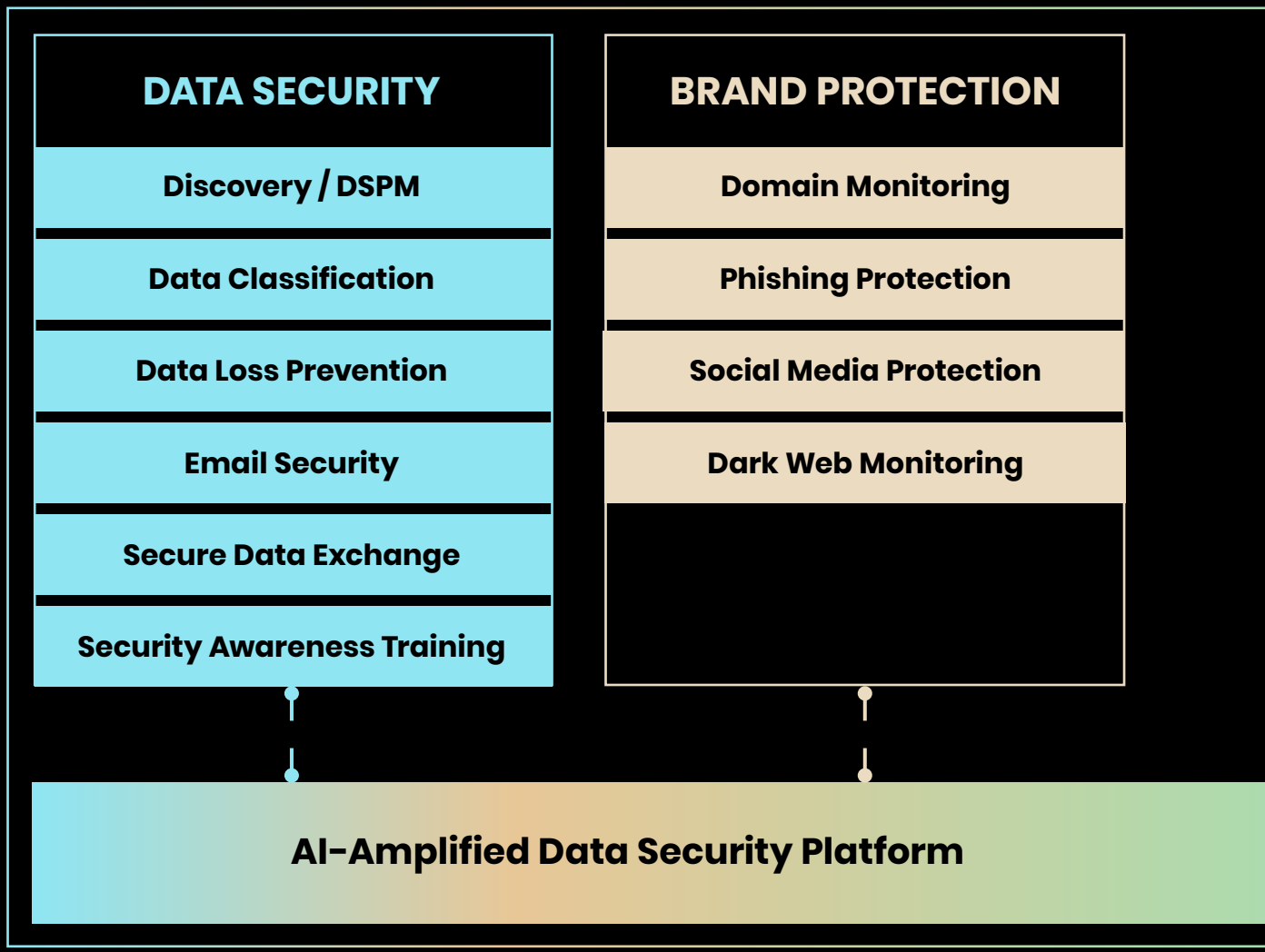
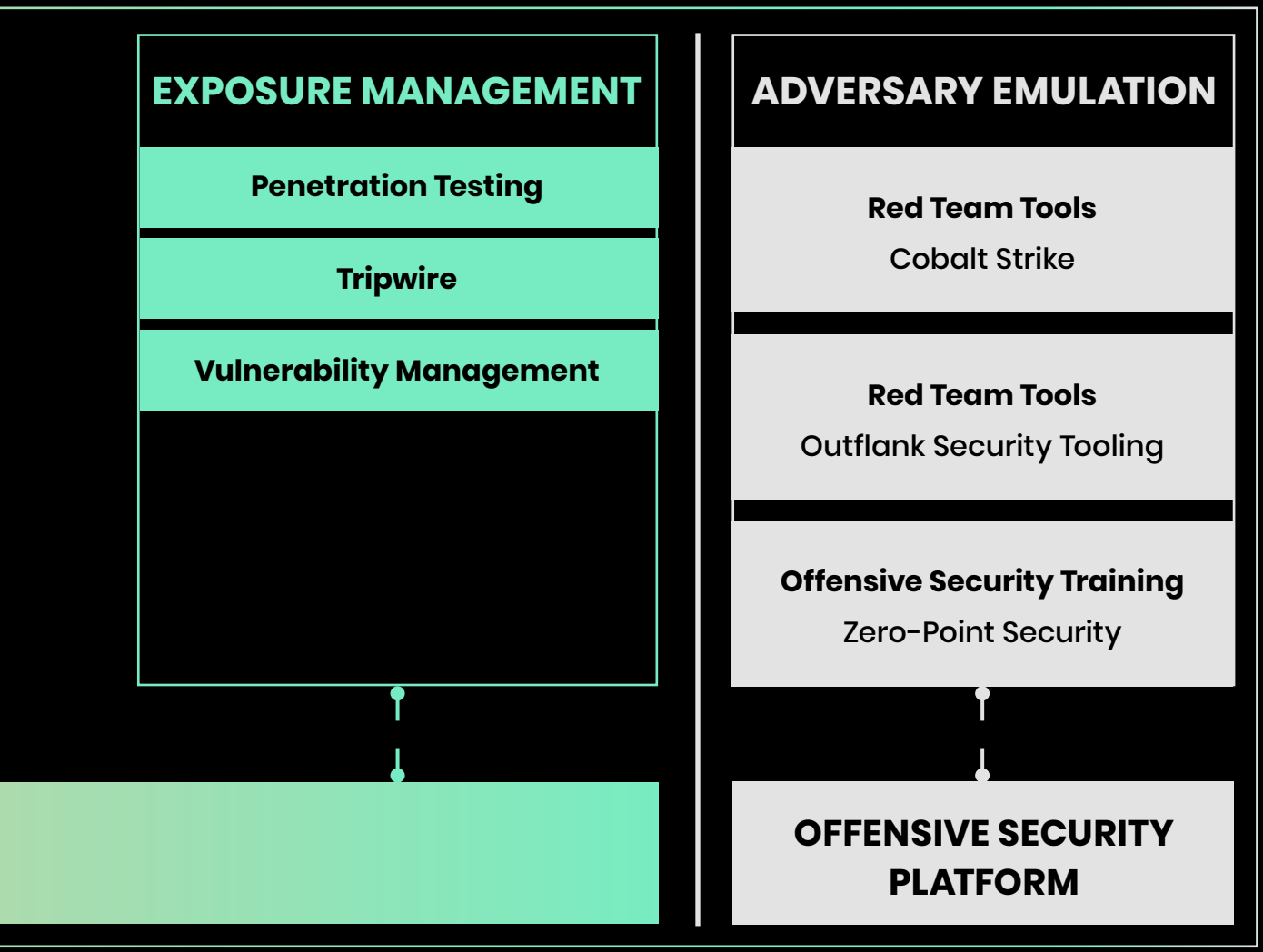
FORTRA®

Offensive & Defensive Security Tools

PROTECT YOUR DATA. ADOPT AI.



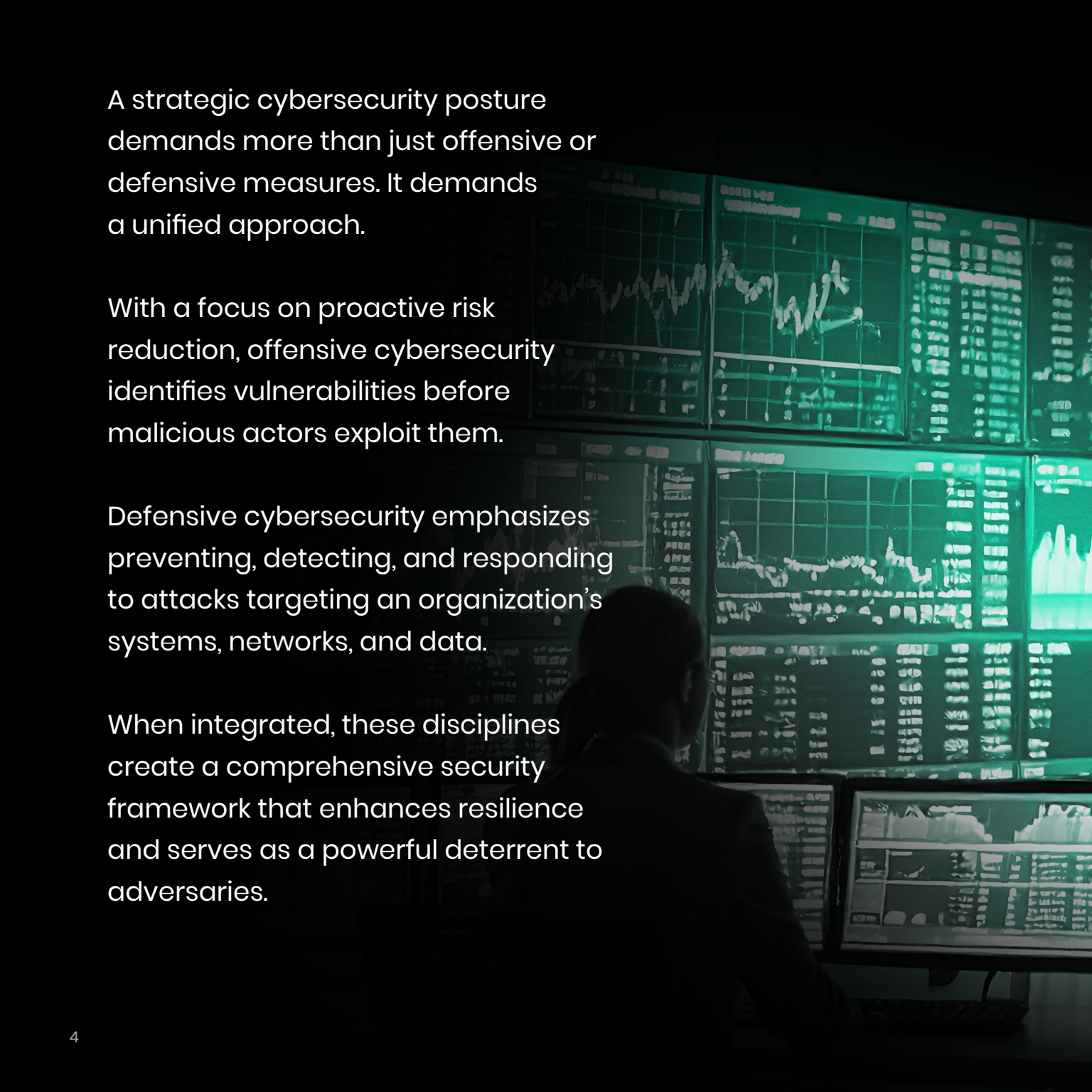

EXPOSURE MANAGEMENT
Penetration Testing
Tripwire
Vulnerability Management
ADVERSARY EMULATION
Red Team Tools
Cobalt Strike
Red Team Tools
Outflank Security Tooling
Offensive Security Training
Zero-Point Security
OFFENSIVE SECURITY PLATFORM

A strategic cybersecurity posture demands more than just offensive or defensive measures. It demands a unified approach.

With a focus on proactive risk reduction, offensive cybersecurity identifies vulnerabilities before malicious actors exploit them.

Defensive cybersecurity emphasizes preventing, detecting, and responding to attacks targeting an organization's systems, networks, and data.

When integrated, these disciplines create a comprehensive security framework that enhances resilience and serves as a powerful deterrent to adversaries.



Fortra's AI-amplified data security platform brings intelligence, monitoring, response, and testing together in one platform to protect your organization's reputation and brand, data, and users. It gives security teams the visibility they need to understand what risks they're facing and clarity about what actions to take next.

Data Security Posture Management (DSPM)

Know where your data lives, who can access it, and how to protect it

DSPM helps organizations discover, classify, and protect sensitive data across cloud environments. It gives security teams visibility into where data is stored, how it's being accessed, and where it may be at risk so they can proactively reduce exposure and maintain control.

Fortra DSPM brings that visibility and control to the cloud apps and platforms your team relies on every day, like Google Drive, AWS, and Microsoft Azure.

Discover

There's a sensitive payroll file open to the internet. Want to fix that?

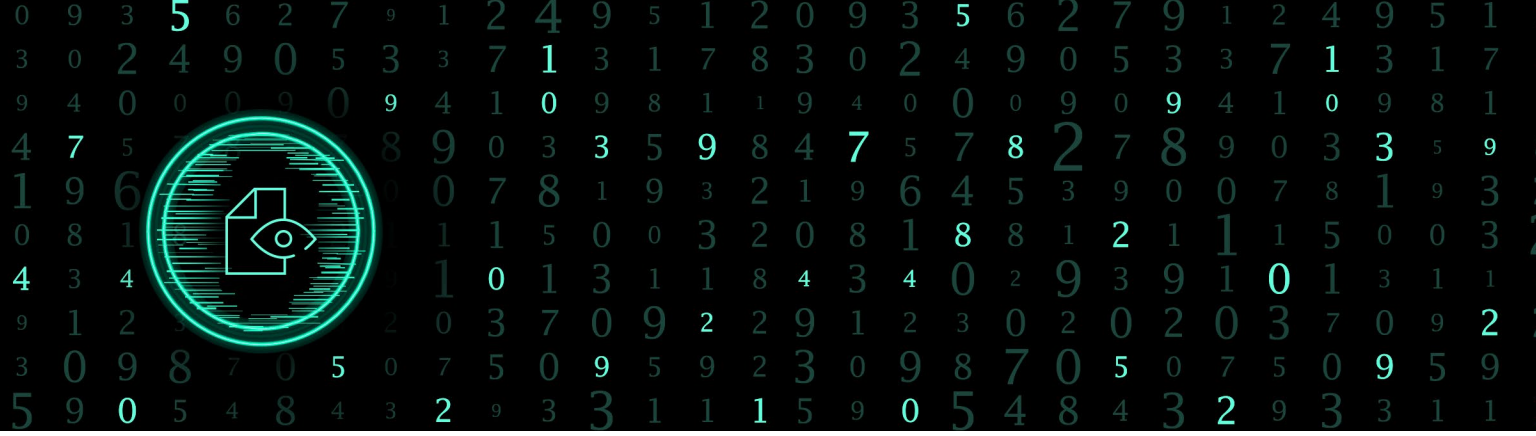
Classify

This file has sensitive information. Shouldn't it be protected?

Protect

This employee can still access this data. Want to remove them?

LEARN MORE



Data Classification

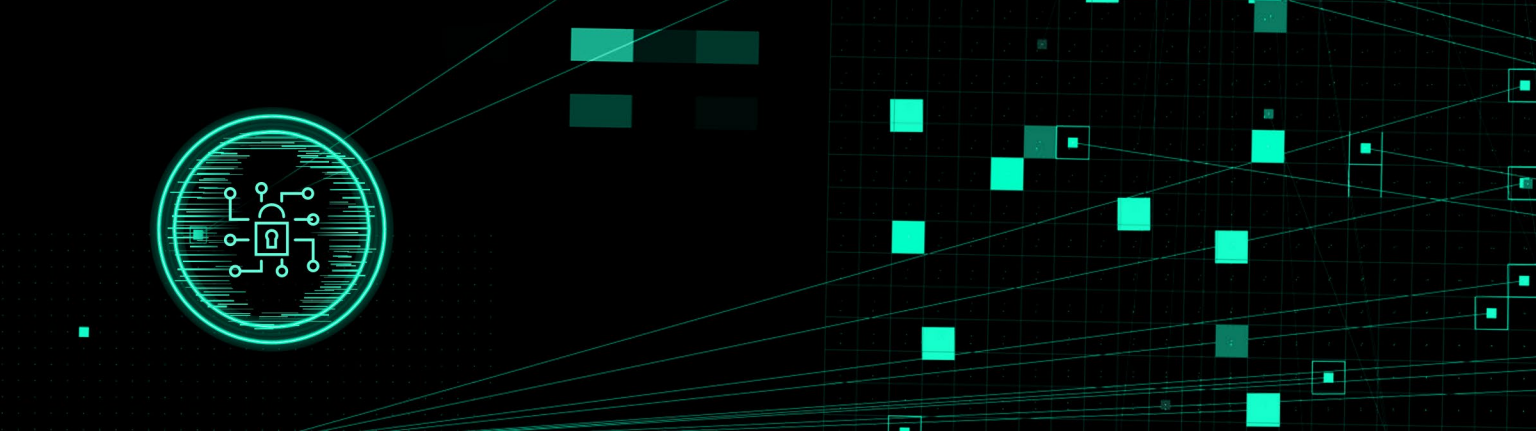
Straightforward data classification for sophisticated compliance

Fortra Data Classification provides a straightforward experience experience for your users on what should be secured and how to handle it. By adding context to your data, you empower both people and systems to make informed decisions about its use.

Our tool embeds metadata attributes into emails, documents, and files at every stage of the content lifecycle and can automatically add visual markings to help organizations meet compliance and legal requirements

Unlike other solutions that offer simplistic “sensitivity labels,” Fortra Data Classification enables users to define and utilize a wide range of identifiers, including department, customer, and country, for precise data categorization.

LEARN MORE



Data Loss Prevention (DLP)

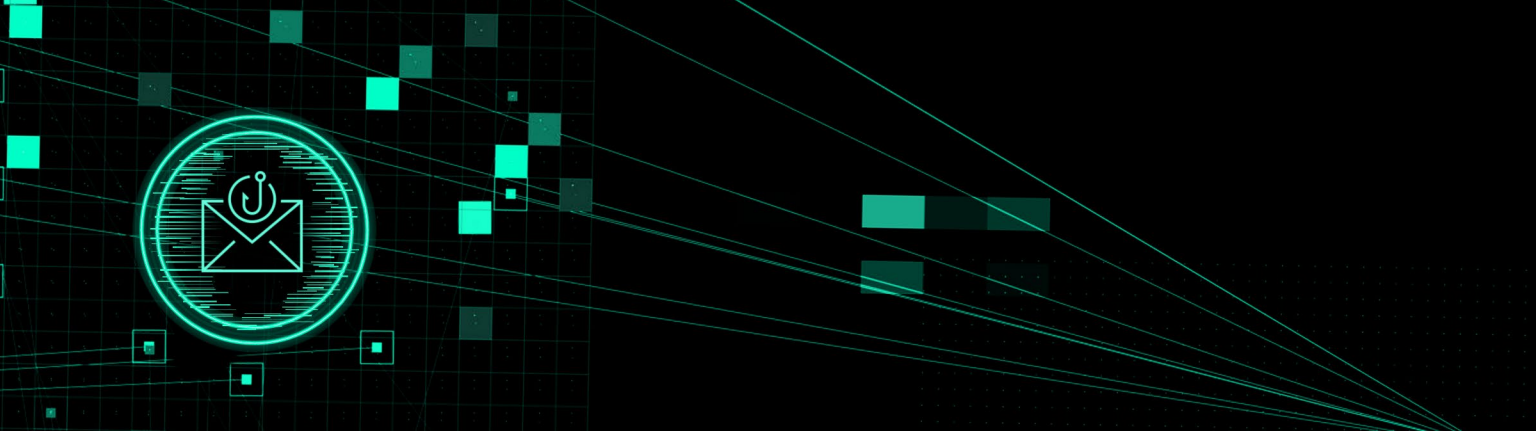
Available in AWS Marketplace

High-powered DLP, supported by experts who have your back

We know DLP can be complex, but it doesn't have to be.

- Endpoint DLP delivers the deepest visibility available on the market. Our agent captures and records all system, user, and data events – on or off the network.
- Network DLP supports compliance and reduces risks of data loss by monitoring and controlling the flow of sensitive data via the network, email, or web.
- Analytics & Reporting Cloud (ARC) runs on AWS to correlate and analyze system, user, and data events from endpoint agents and our network appliance to provide the visibility and context you need to identify and remediate insider and outsider threats.

LEARN MORE



Email Security

Advanced threat protection for cloud, on-premises, and hybrid email environments

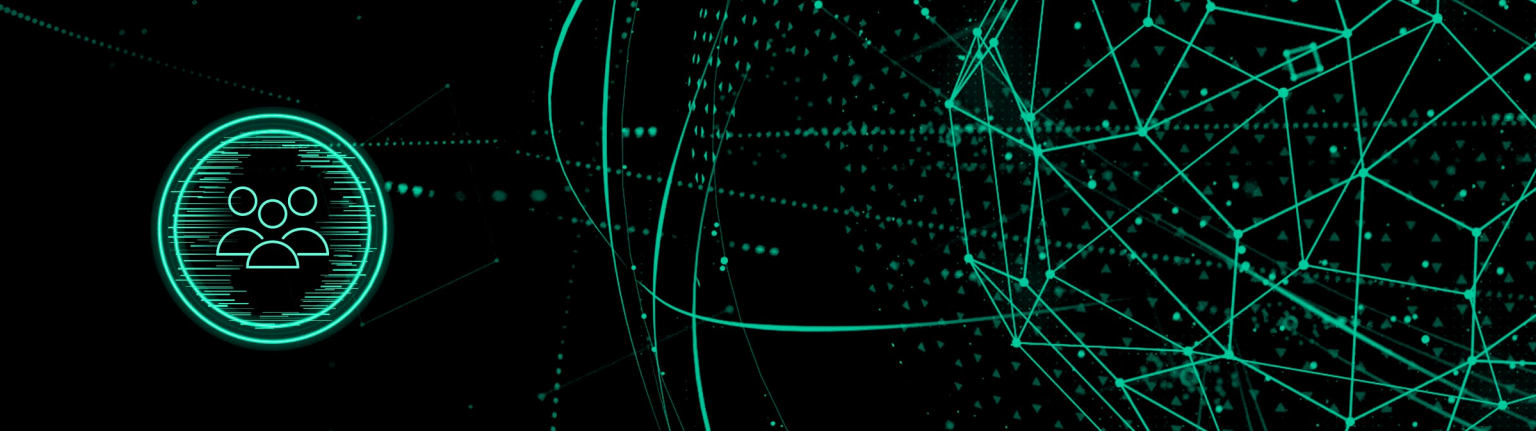
Too many threats get past traditional email security controls. Impersonation threats, like Business Email Compromise (BEC) and credential phishing, continue to plague inboxes, accounting for more than 95% of reported email threats.

Defenders need a better way. One that delivers everything it takes to stop modern email threats, including:

- AI that detects advanced impersonation, account takeover, and social engineering
- Threat intelligence that disrupts emerging threats
- Robust email authentication that prevents spoofing
- Engaging awareness training that drives users to recognize and report threats
- Expert triage that quickly resolves reported email threats
- Automated response that continuously purges threat across the environment

Fortra delivers comprehensive email security with interoperable solutions that protect against advanced email threats, minimize human risk, and reduce costs.

LEARN MORE



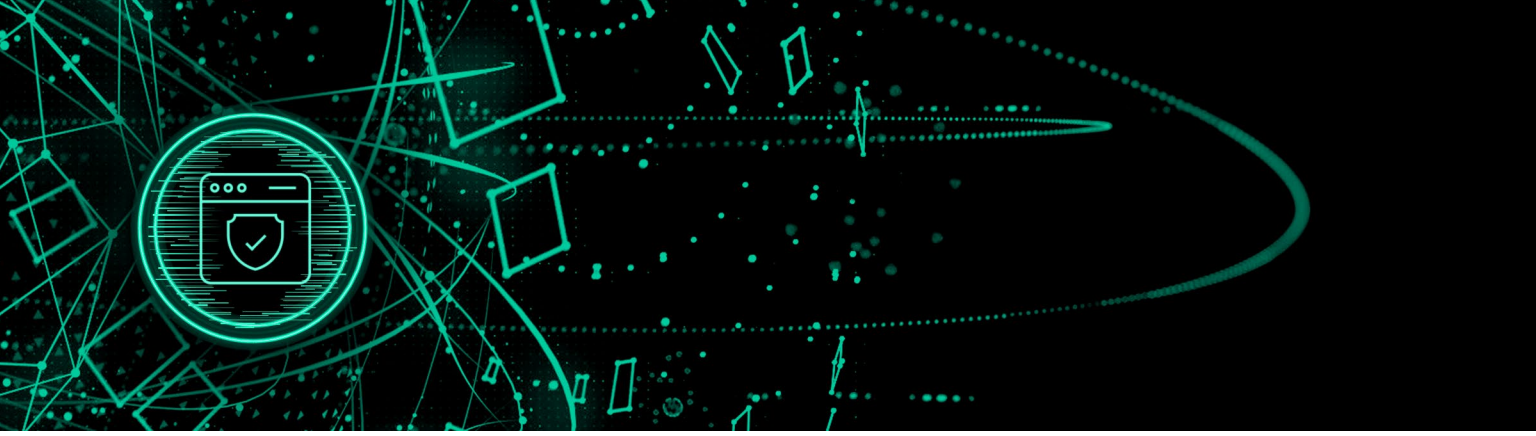
Security Awareness Training

Fortra Security Awareness Training (SAT) instills user behaviors that break the attack chain while helping organizations identify and manage human risk. With training from our offensive and defensive security experts, organizations can minimize risky employee behaviors and develop the positive habits needed to protect against modern social engineering threats.

Features include:

- Deep training curriculums on highest risk threats
- Training and simulations in response to emerging threats
- Engaging, high impact training in a variety of easy-to-consume formats
- Analytics all the way down to individual users
- Customization based on user roles and risk profiles
- Integrated phish reporting, triage, and response
- Optional program management by SAT professionals (Managed SAT)
- Customized program plans and expert guidance (SAT Advisory Services)

LEARN MORE



Brand Protection

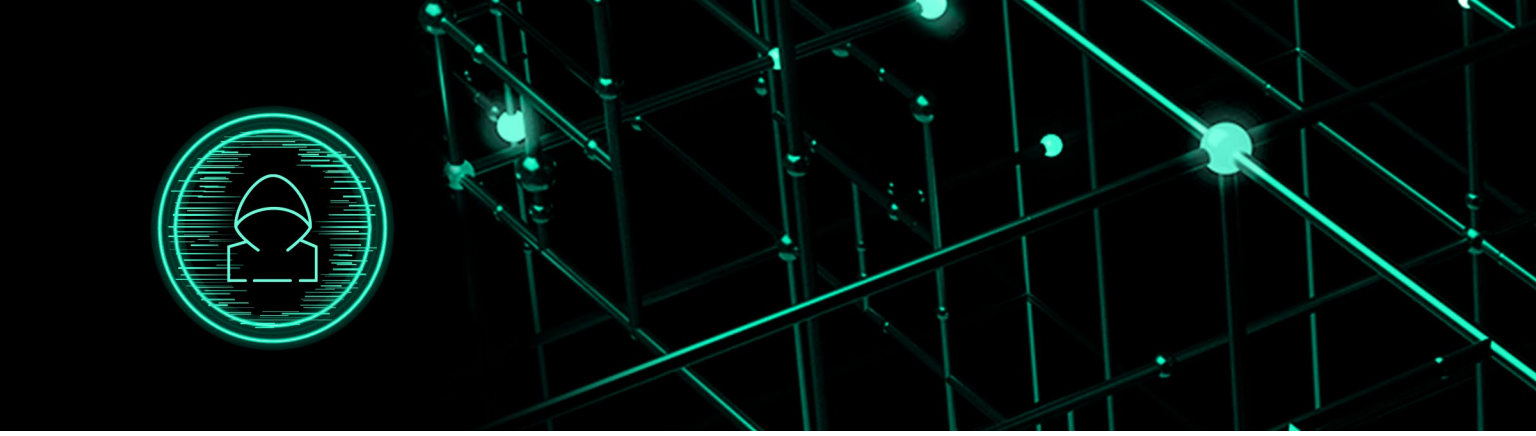
Break the attack chain of fraud and brand impersonation

Fortra Brand Protection detects and quickly mitigates lookalike domains, phishing sites, fake social profiles, and other external threats.

Features include:

- Coverage across open web, dark web, social media, email, and mobile
- Direct collection plus hundreds of public and private data feeds
- Advanced crawling and anti-evasion technologies
- Expert vetting and curation tailored to customer needs
- Global takedown network with killswitches and API integrations
- Automated browser blocking
- 15+ years of relationships and proven takedown success
- No customer intervention required for takedown
- Unlimited takedowns

LEARN MORE



Core Impact Pen Testing Software

Professional-grade penetration testing software that provides guided automation and certified exploits

Core Impact enables security teams to conduct advanced penetration tests with ease.

With guided automation and certified exploits, this powerful penetration testing software enables you to safely test your environment using the same techniques as today's attackers.

RAPID PENETRATION TESTING

Use automated Rapid Penetration Tests (RPTs) to discover, test, and report in just a few simple steps.

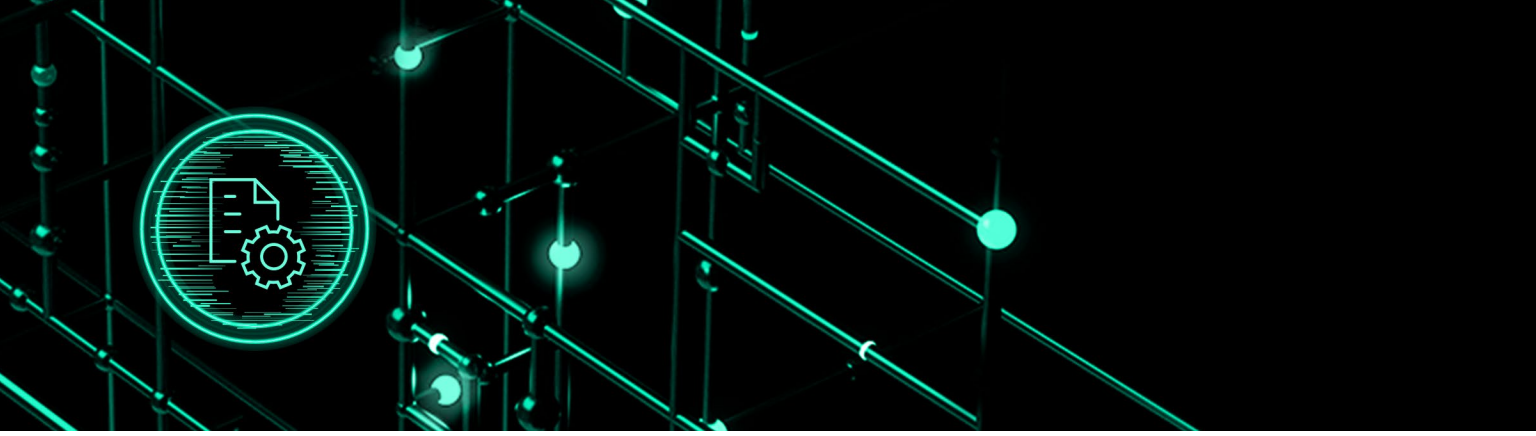
CORE CERTIFIED EXPLOITS

Leverage professionally written and validated exploit library for real-world testing capabilities.

CENTRALIZED TOOLSET

Gather information, exploit systems, and generate reports, all in one place.

LEARN MORE



Tripwire

Audit-ready integrity monitoring that secures and simplifies

Tripwire combines File Integrity Monitoring (FIM) and Secure Configuration Management (SCM) to ensure your environment stays secure, stable, and compliant:

File Integrity Monitoring

Detects unauthorized or suspicious changes to critical files, operating systems, servers, endpoints, network devices, and other critical assets, helping you identify threats like ransomware, malware, or insider activity before they spread.

Secure Configuration Management

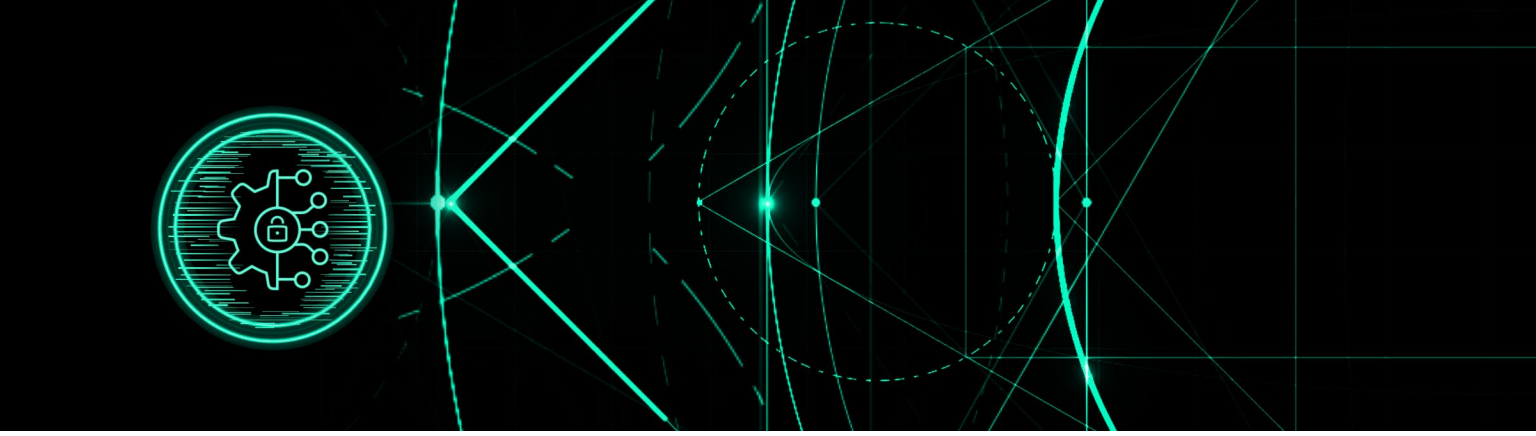
Continuously compares your systems against trusted security baselines and industry standards, reducing risks from misconfigurations and ensuring a hardened environment.

Compliance Reporting

Simplifies audits with clear, actionable reports mapped to regulatory frameworks such as PCI DSS, HIPAA, NERC CIP, and more.

With real-time visibility and continuous assurance, Tripwire helps you maintain security, resilience, and regulatory confidence.

LEARN MORE



Vulnerability Management

Risk-based vulnerability management to identify, assess, and prioritize security weaknesses fast

Fortra Vulnerability Management (VM) is a proactive, risk-based vulnerability management solution that is crucial to any cybersecurity portfolio.

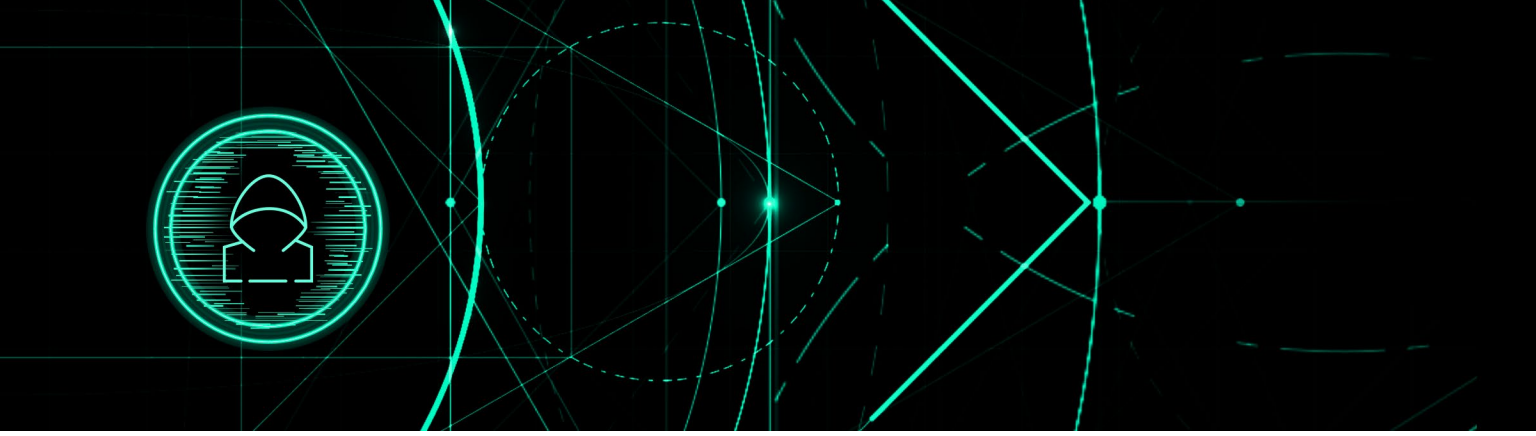
It streamlines the identification and prioritization of system weaknesses, so you can maximize existing IT resources and mitigate risks swiftly and effectively.

Features include:

- Security GPA® security posture rating
- Peer Insight
- Network Map asset visualization
- Threat Landscape exploitability context
- Connect API

Select the VM options that fit your organization via our scalable subscription model.

LEARN MORE



Cobalt Strike & Outflank Red Team Tools

Red teaming tools for advanced engagements

- Cobalt Strike and Outflank Security Tooling (OST) are top-tier red teaming solutions that enable operators to execute the diverse and varied tasks that each red team engagement requires.
  - Cobalt Strike provides post-exploitation capabilities through its Beacon payload and Malleable C2 framework.
  - OST is a broad arsenal of offensive security tools that covers the full attack chain with emphasis on evasion techniques.
- Using both Cobalt Strike and OST maximizes your red team's probability of attaining their objectives.

LEARN MORE

FORTRA®

 | fta-corp-br-0726-r8-as