FORTRA

Offensive & Defensive Security Tools

WE BREAK THE ATTACK CHAIN

Recon

Weaponize

Deliver

Application Security Testing

Cobalt Strike & Outflank Red Team Tools

Pen Testing Services

Security Configuration Management

Vulnerability Management

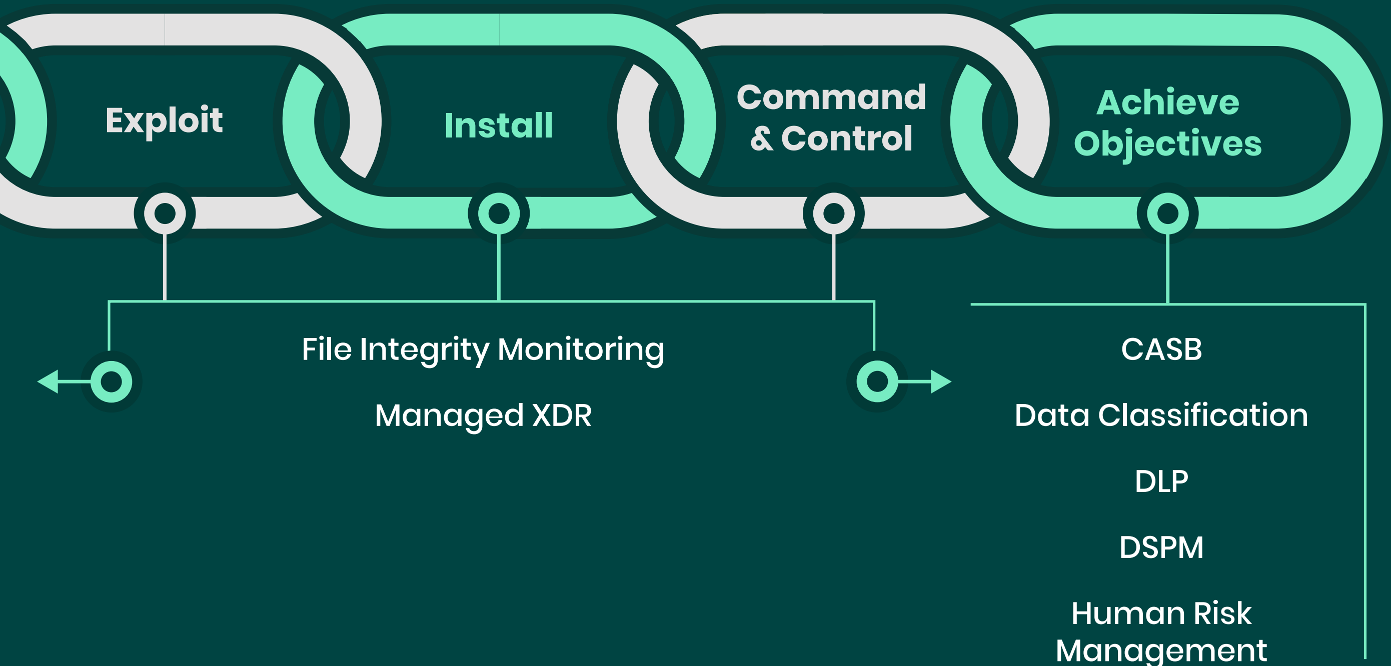
Brand Protection

Email Security

Managed WAF

Secure Web Gateway

Zero Trust Network Access



Exploit

Install

Command & Control

Achieve Objectives

File Integrity Monitoring

Managed XDR

CASB

Data Classification

DLP

DSPM

Human Risk Management

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.

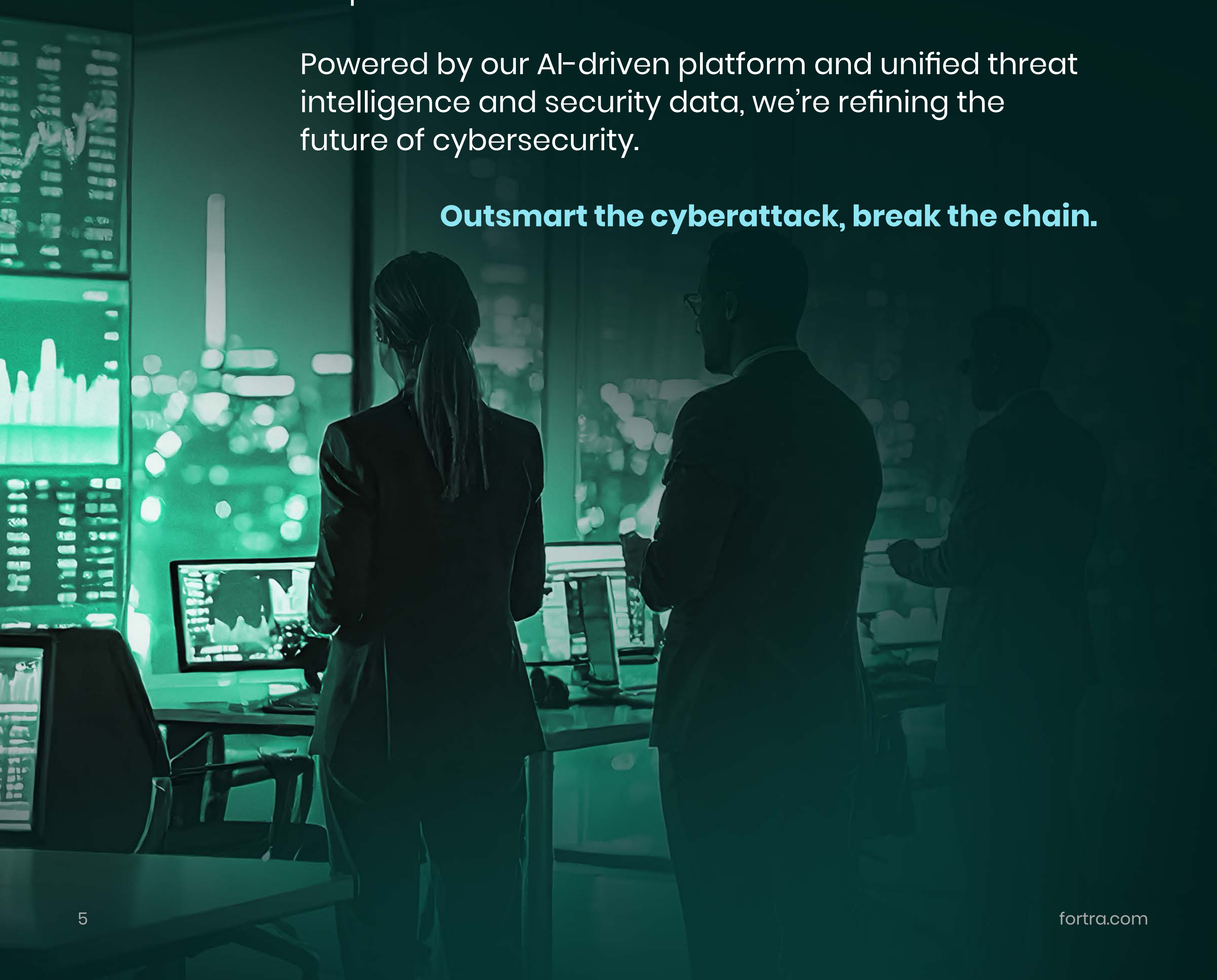
Defensive cybersecurity emphasizes preventing, detecting, and responding to attacks targeting an organization's systems, networks, and data.

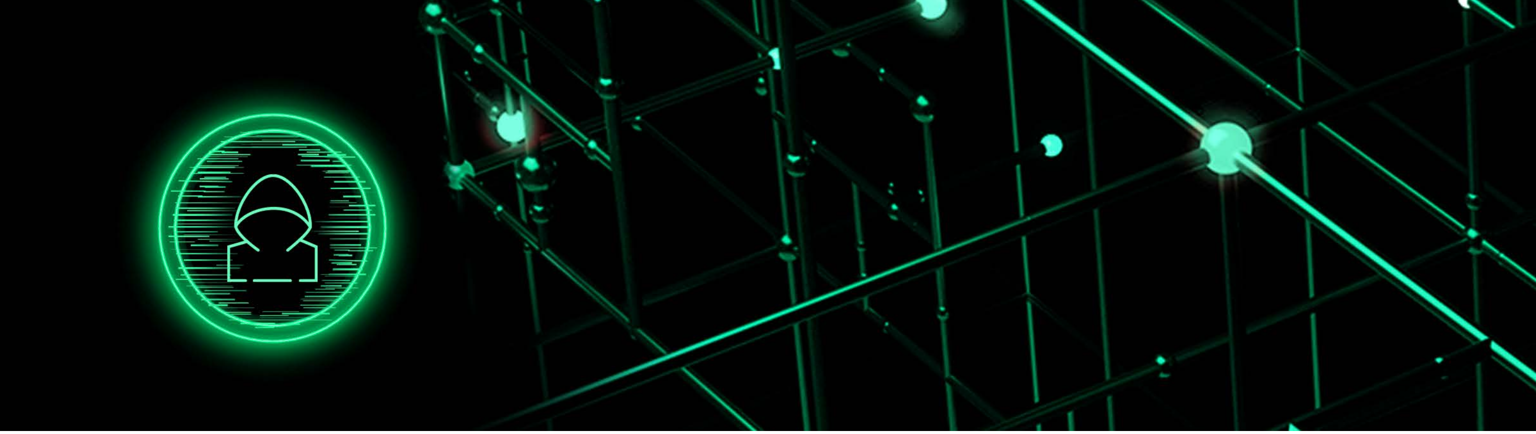
When integrated, these disciplines create a comprehensive security framework that enhances resilience and serves as a powerful deterrent to adversaries.

At Fortra, we break the attack chain. Our comprehensive suite of offensive and defensive cybersecurity solutions empowers practitioners to outpace threats.

Powered by our AI-driven platform and unified threat intelligence and security data, we're refining the future of cybersecurity.

Outsmart the cyberattack, break the chain.



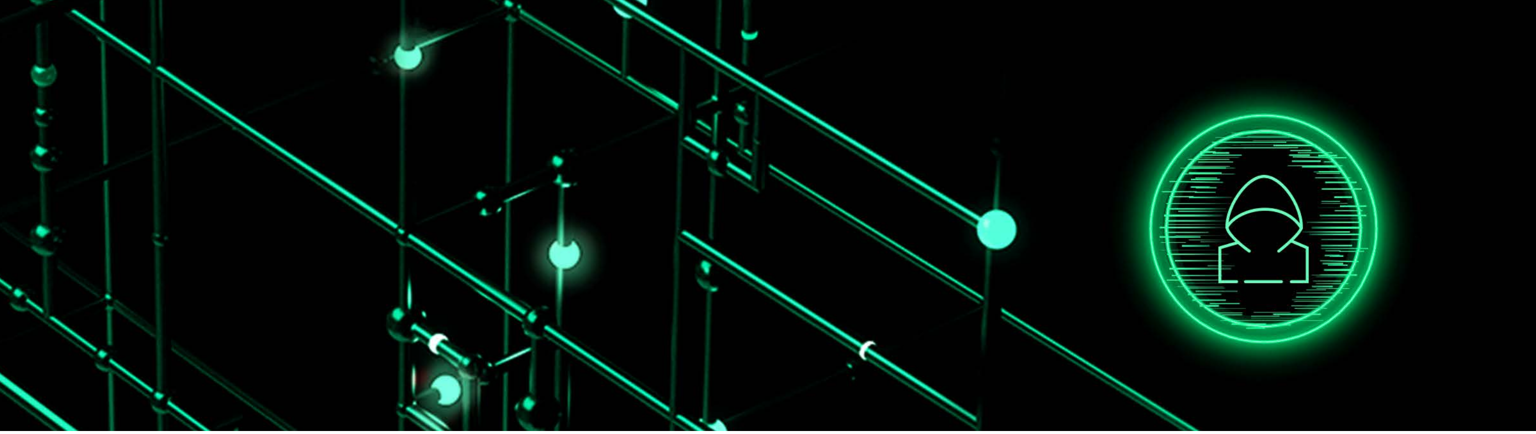


Cobalt Strike & Outflank Red Team Tools

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



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.

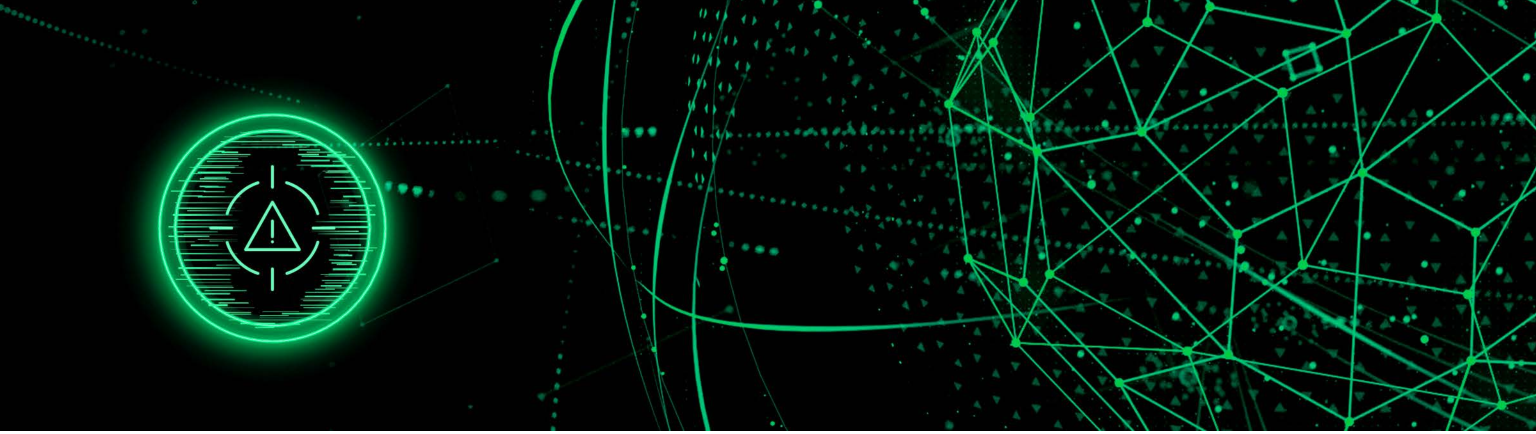
Core Certified Exploits

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



Pen Testing Services

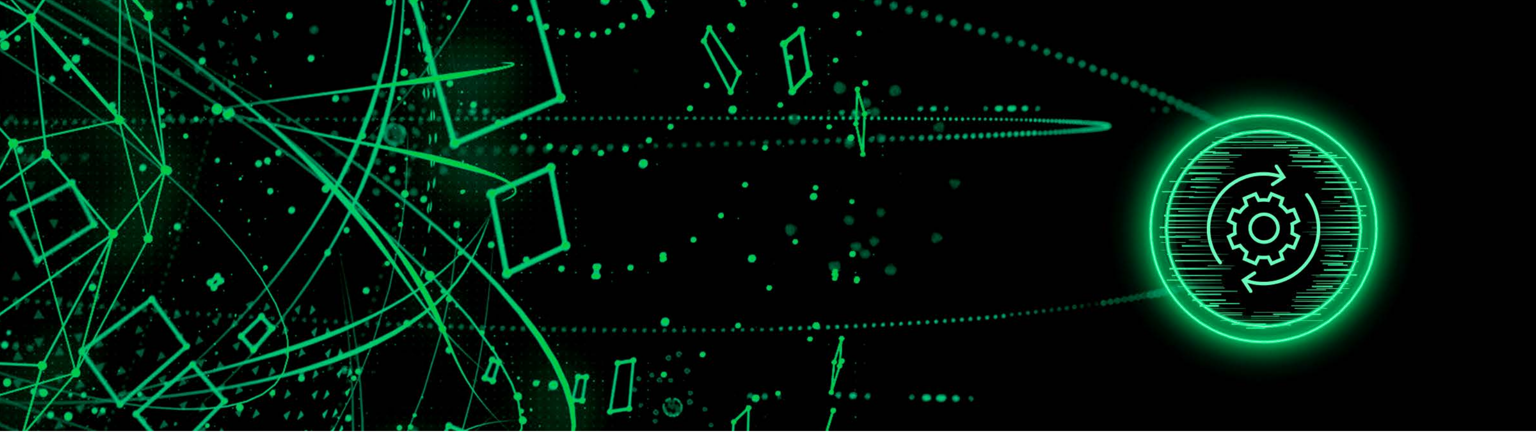
Certified penetration testers use real-world tactics to uncover hidden weaknesses and deliver actionable insights

Fortra’s Penetration Testing experts provide reliable security tests, from basic pen tests to complex engagements with sophisticated attack emulation. Our team will uncover security weaknesses and provide detailed suggestions on remediation.

Pen Testing types:

- Network Security
- Application Securityv
- Web Applications
- Mobile Applications
- Application Programming Interface (API)
- Social Engineering (Remote or On-site)

LEARN MORE



Security Configuration Management

Automate compliance and detect misconfigurations across cloud, on-prem, IT/OT

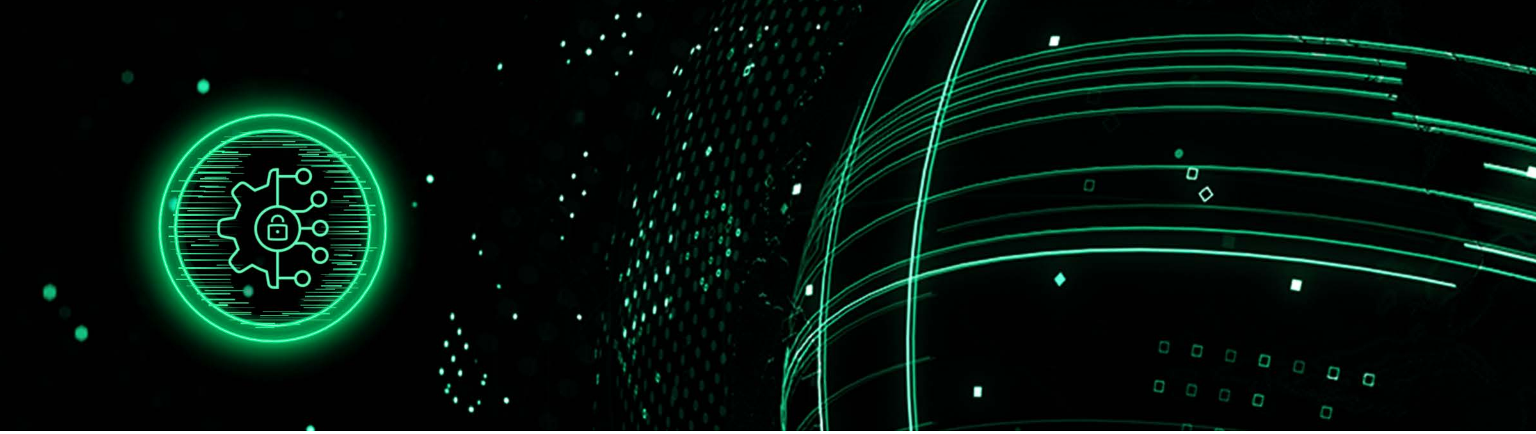
Security configuration management (SCM) software helps identify misconfigurations that make your systems vulnerable before an attack occurs and also monitor for unusual changes to critical files or systems.

SCM helps secure on-prem, cloud and IT/OT environments.

Benefits:

- Continuous compliance with standards such as PCI DSS
- Clear misconfiguration remediation guidance
- Complete device and asset discovery gives a clear picture of your network
- Create and enforce your customized compliance policies

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

Brand Protection

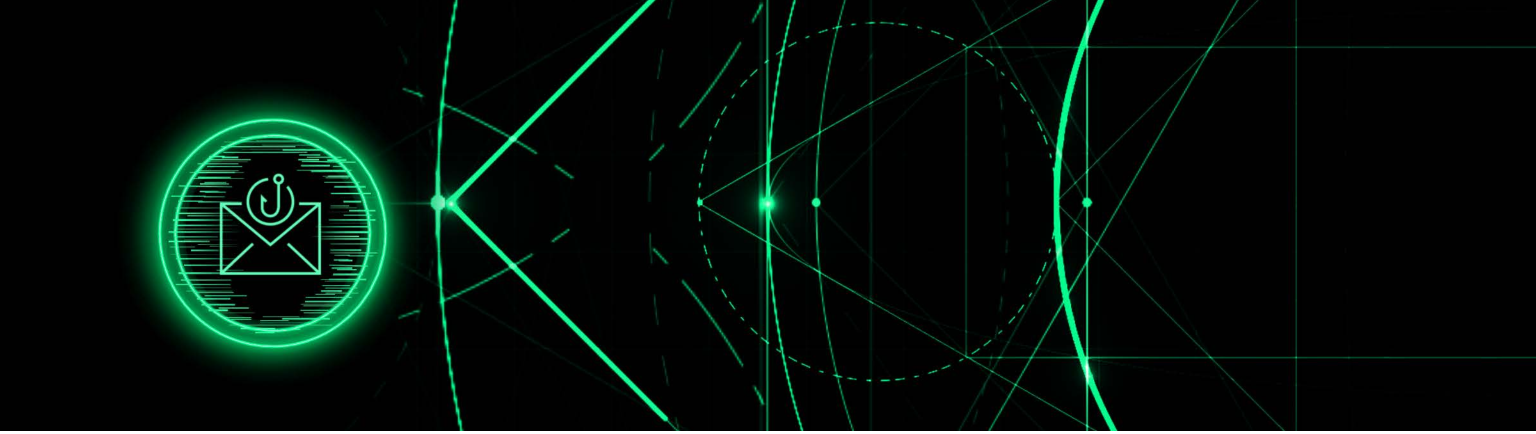
Break the attack chain of fraud and brand impersonation

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



Email Security

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

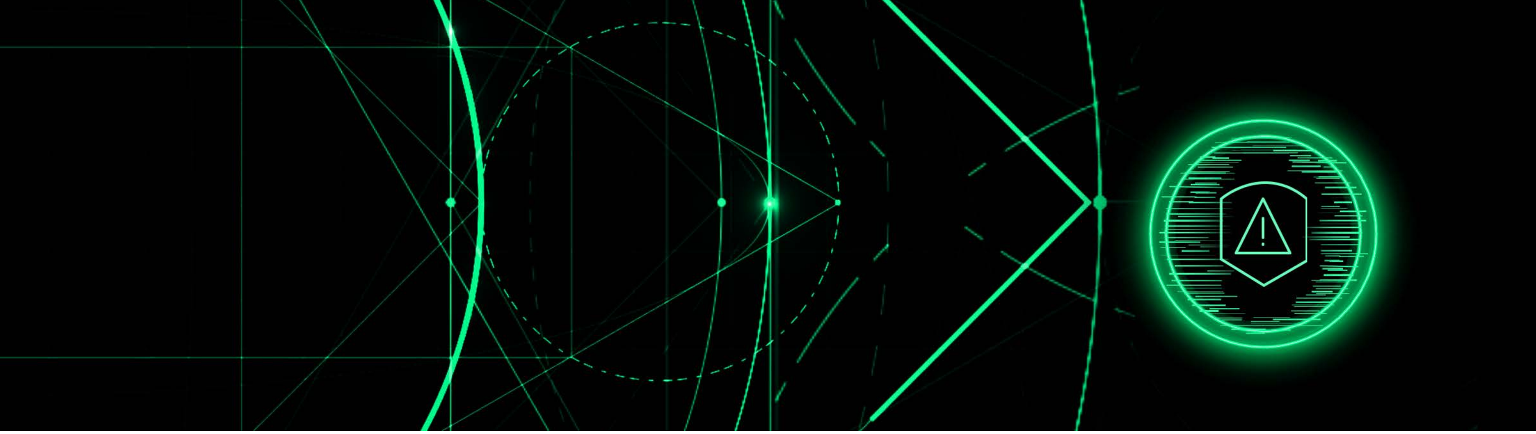
Too many threats get past traditional email security controls. Impersonation threats, like Business Email Compromise (BEC) and credential phishing, continue to plague inboxes, accounting for more than 95% of reported email threats.

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



Managed WAF

Fully optimized, enterprise-grade protection for optimal value from your WAF

While many web application firewalls (WAFs) offer features to secure web apps and APIs, most fall short of delivering ideal protection. This is largely due to organizations struggling to keep pace with dynamic applications, shifting business priorities, and the evolving threat landscape.

Fortra Managed WAF works alongside your team to ensure optimized, application-aware policies that keep apps online and protect users, data, and networks. We harness the power of machine learning to craft tailored traffic profiles for each customer. Security experts refine these profiles to ensure precise, site-specific protection for websites and APIs. This approach delivers effective protection by blocking malicious traffic while ensuring seamless access for legitimate users and bots.

Get the most out of your WAF, with always optimized, enterprise-grade protections. Keep your apps online and your users, data, and network protected from compromise.

LEARN MORE

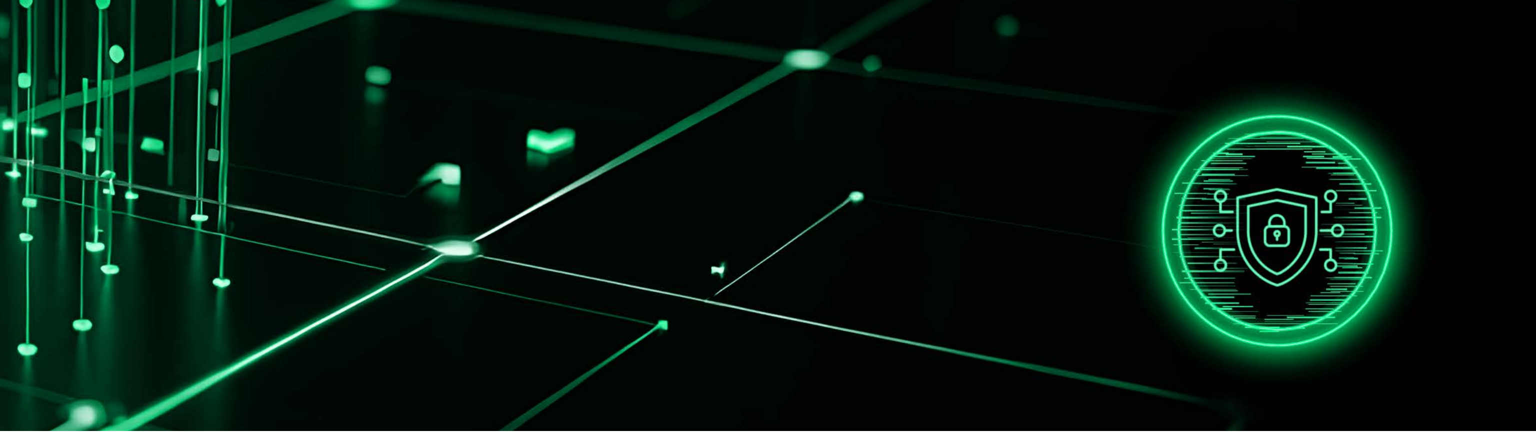
Secure Web Gateway (SWG)

Protect against internet threats and data leakage

Fortra SWG protects users, networks, and corporate data from internet-based threats including malware, zero-day, and browser-based attacks by inspecting all incoming and outgoing web traffic for malicious content and sensitive information.

Organizations that restrict social media access or limit certain downloads on employee devices can rely on SWG to enforce these policies effectively.

LEARN MORE



Zero Trust Network Access (ZTNA)

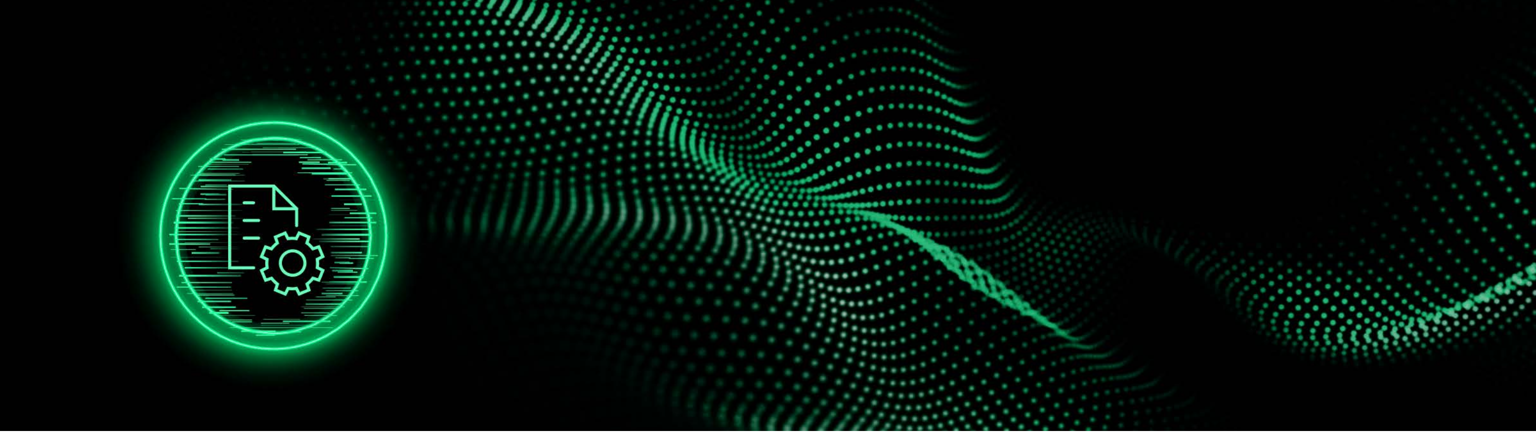
Securely connect users to all private resources

Fortra helps you take the next step on your zero-trust journey, from identifying needed controls to implementation.

Fortra ZTNA is a cloud-delivered zero trust network access solution that provides seamless access to private applications and protects the data stored within these applications, no matter where the user or app is located. Unlike a virtual private network (VPN), ZTNA is a cloud-native service that reduces management overhead, protects the data stored in private applications, and avoids backhauling traffic to deliver a better end user experience.

We work with customers across every industry on their zero-trust journey to "never trust, always verify." Together, we identify the problems they need to solve, identify what controls will fit the problem set, and help simplify implementation of a zero trust approach.

LEARN MORE



File Integrity Monitoring

Audit-ready integrity monitoring that secures and simplifies

Integrity and Compliance Monitoring 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:

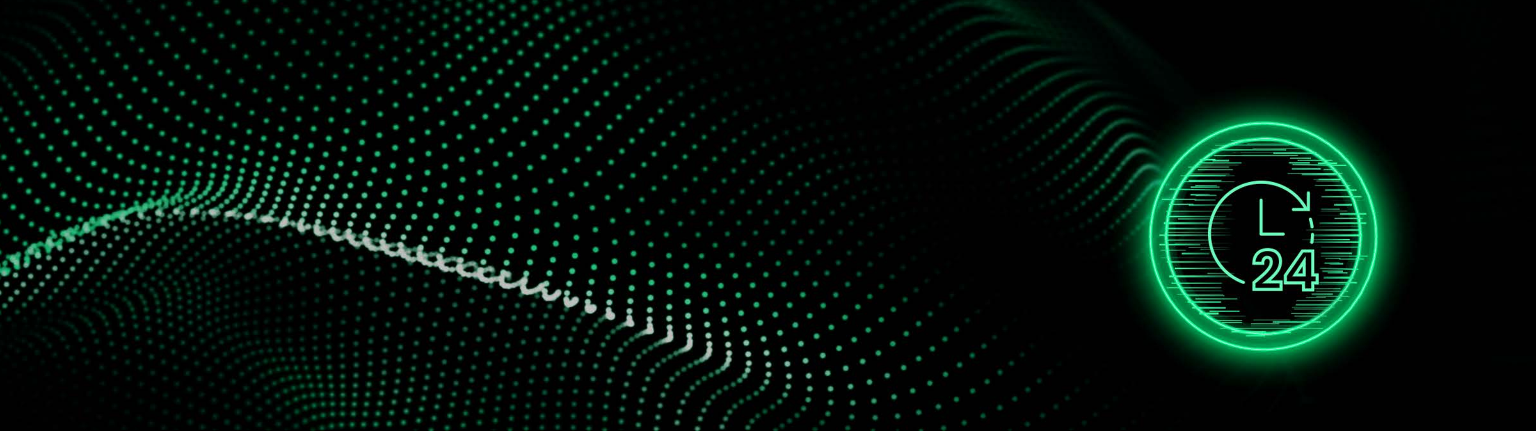
Continuously compares your systems against trusted security baselines and industry standards, reducing risks from misconfigurations and ensuring a hardened environment.

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, Fortra Integrity and Compliance Monitoring helps you maintain security, resilience, and regulatory confidence.

LEARN MORE



Managed XDR

24/7 telemetry and threat monitoring across identity, networks, cloud, and endpoints

Fortra XDR provides 24/7 threat monitoring to help organizations reduce risks and resolve incidents faster. Fueled by robust threat intelligence, advanced machine learning, and automation, our Security Operations Center (SOC) notifies you of high and critical incidents within 15 minutes of detection and our cyber risk experts work with you until those threats are resolved.

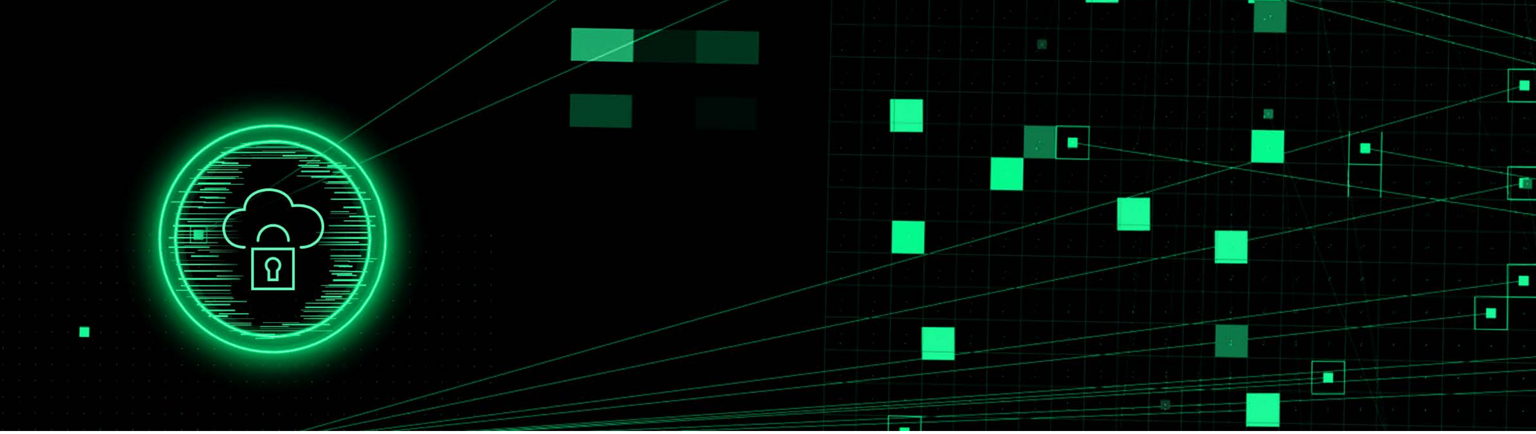
Three key elements that set Fortra XDR apart include:

- Comprehensive Coverage and Visibility
- Broad Detection and Response
- 24/7 Managed Expertise and SOC Services

Our extended detection and response solution seamlessly integrates with existing third-party tools, technologies, and APIs, ensuring that organizations can enhance their current security infrastructure without disruption. And with our quick deployment, you'll be up and running so you can immediately begin detecting threats.

Fortra XDR isn't just another tool for your IT stack; it's a proactive, managed solution providing predictable pricing, maximum visibility, and optimized coverage.

LEARN MORE



Cloud Access Security Broker (CASB)

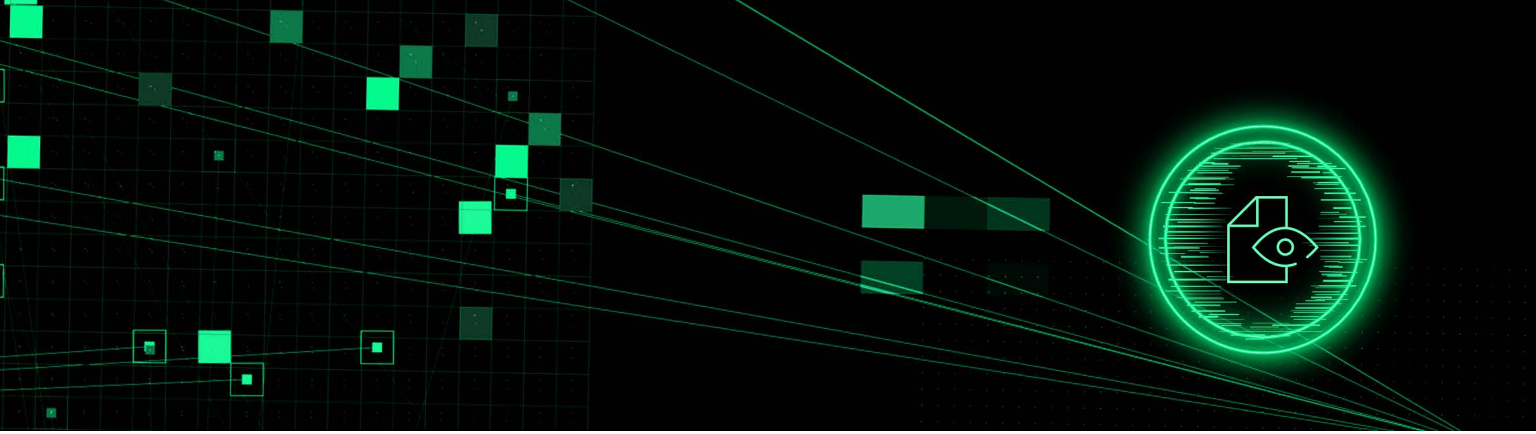
Get visibility and control over your data in the cloud

With your employees already using cloud applications like Google Drive, Microsoft 365, or Dropbox, extra measures are needed to keep your corporate data safe. With today's common cloud apps, your employees might upload sensitive files to the wrong place, download apps or files they shouldn't, or use unauthorized shadow apps.

Fortra CASB monitors cloud activity and keeps data safe by:

- Making sure only the right people access the right things
- Stopping risky logins from untrusted places or devices
- Keeping an eye on unsanctioned shadow cloud apps employees may try to use

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)

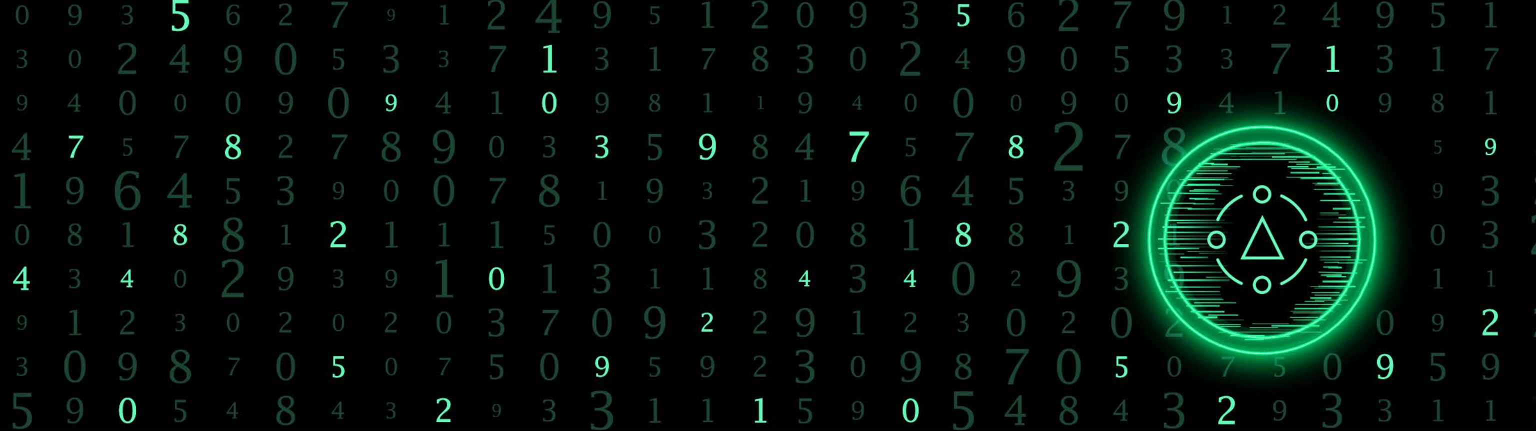
Available in AWS Marketplace

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



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?

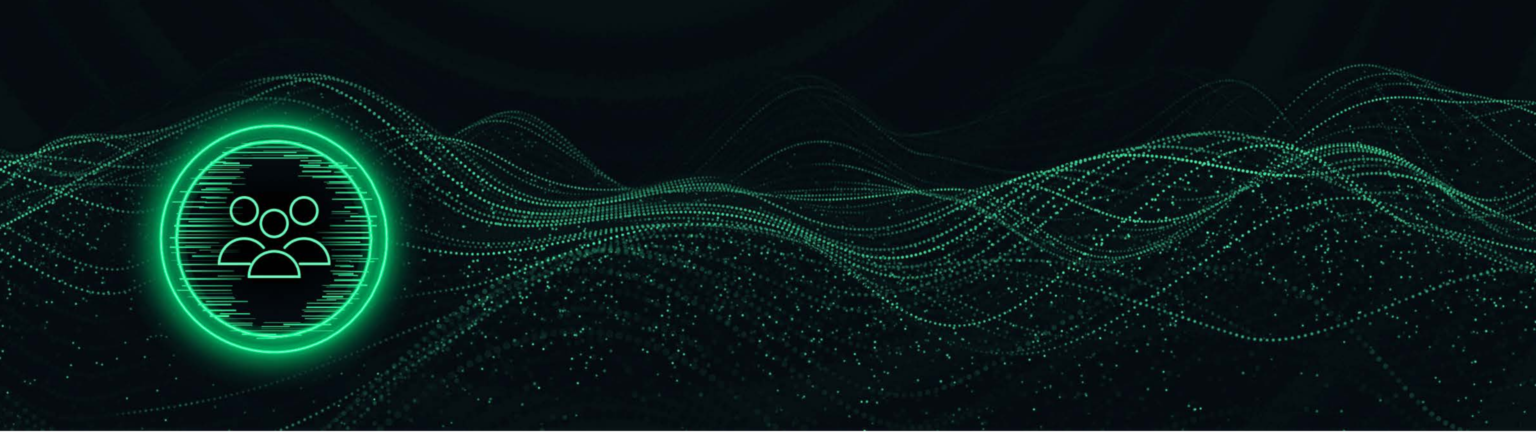
Classify

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

Protect

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

LEARN MORE



Human Risk Management

Build a security-first organizational culture

Fortra Human Risk Management (HRM) 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 HRM professionals (Managed HRM)
- Customized program plans and expert guidance (HRM Advisory Services)

LEARN MORE

FORTRA®

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.