AI Drives Change

80% of AI data goes unprotected

70% of cyberattacks involve critical infrastructure

456% rise in GenAI enabled scams in 1 year

Fortra Cybersecurity Drives Confidence

Secure adoption of **150+** GenAI tools

5M+ threats detected every day

Mitigate phishing sites within **2 Hours**

Fortra Protects the Names You Know

mastercard · salesforce · UNITEDHEALTH GROUP · Cargill · AMERICAN EXPRESS · TikTok · Goldman Sachs · FedEx · Coca-Cola · Uber · DELTA

AI-Powered Solutions You Trust

Eliminate blind spots and reduce risk with complete data visibility and control across endpoints, cloud, AI, and collaboration tools. It's time to secure AI with confidence.

Data Security

Discover, classify, and protect sensitive data—guarding what matters most wherever it goes.

Brand Protection

Disrupt phishing and impersonation campaigns before they reach customers or damage trust.

Offensive Security

Identify and exploit real-world attack paths and uncover security gaps before adversaries do.

Your Problems, Solved

Stopping the attacks that target your data and people every day.

DATA SECURITY

USE CASE	FORTRA SOLUTION
An engineer tries pasting proprietary code into an unapproved GenAI tool for help troubleshooting. **Fortra automatically blocks the sensitive parts** before submission, preventing accidental data leakage.	Endpoint Data Loss Prevention (eDLP)
Automated scanning reveals LP agreements, K-1s, and valuation models stored in open file shares—**everything is auto-flagged and access is tightened.**	Network Data Loss Prevention (nDLP)
The security team discovers that hundreds of employees have started using an unapproved AI writing tool. Instead of shutting it down immediately, they **assess the risk and set policies to allow safe usage.**	Cloud Access Security Broker (CASB)
An employee tries emailing customer SSNs externally. Because the file is labeled as "PII," **Fortra blocks the email with a message explaining why.**	Data Classification (DCS)
Fortra tracks exactly who opened, edited, or attempted to print a protected document, helping quickly resolve investigations.	Enterprise Digital Rights Management (EDRM)
An employee tries visiting a website from a phishing email. **Fortra flags it as malicious, blocks it instantly, and creates a log**—preventing a malware infection.	Secure Web Gateway (SWG)
A fraudulent capital call email slips into one inbox—**Fortra finds every copy across the firm and deletes them within minutes.**	Cloud Email Protection (CEP)
An attacker spoofs the CEO and emails finance requesting an urgent wire transfer related to a portfolio transaction. **Fortra blocks the message instantly, stopping fraud** before anyone can act on it.	Secure Email Gateway (SEG)
Your employee receives an unexpected docusign email and is unsure if they should open it. The employee reports the suspicious email, **Fortra triages the submission, identifies it as malicious, and extracts indicators to stop the wider campaign across the environment.**	Suspicious Email Analysis (SEA)
A remote developer accesses an internal app without using a VPN. **Fortra validates their identity and device in real time before access is granted.**	Zero Trust Network Access (ZTNA)

BRAND PROTECTION

USE CASE	FORTRA SOLUTION
Attackers create fake profiles of portfolio CEOs. **Fortra alerts fire immediately, and impersonation attempts get shut down**—preventing account takeover and reputational damage.	Executive Protection
A phishing attack is distributed to team members via SMS. **Fortra is able to quickly detect, block access, and completely mitigate the site** to prevent a team member from falling prey to account takeover.	Account Takeover Prevention
A website surfaces that is impersonating your company domain. **Fortra quickly identifies the look-alike domain, takes it offline, and prevents attackers from tricking customers into entering credentials.**	Online Impersonation
Fortra automated monitoring flags counterfeit listings and has them removed before they spread widely—protecting customers and brand trust.	Counterfeit Protection

OFFENSIVE SECURITY

USE CASE	FORTRA SOLUTION
Pen testers use Core Impact to uncover exploitable weaknesses in new portfolio company networks and applications. Actionable reports help leaders prioritize remediation, meet regulatory needs, and establish a pre-integration security baseline.	Core Impact Pen Testing Software
Red teams use Cobalt Strike and Outflank to simulate advanced, evasive attackers moving laterally across networks and accessing critical systems. These exercises validate an organization's ability to detect, contain, and respond, offering a realistic measure of security maturity.	Cobalt Strike and Outflank Red Team Tools
Fortra delivers risk-based vulnerability management, **prioritizing the vulnerabilities most likely to impact critical systems and data**—so teams remediate faster and more strategically.	Vulnerability Management