FORTRA

DATASHEET

Fortra CASB

Protect your cloud data with complete visibility and control

Security challenges introduced by your growing cloud footprint

In the modern work environment, we rely on cloud services to collaborate with colleagues, contractors and partners. It no longer matters where we work or what device we use — we now have easy access to the data we need to be productive.

Amid the skyrocketing collaboration, your data is going where it's needed. Employees work from everywhere, collaborating over networks and devices that you may not have control over. They're also juggling between personal and work cloud apps to keep up with life responsibilities. Collaboration may have skyrocketed, but so have the risks your data is exposed to.

Maintaining visibility and control as you move to the cloud

As your organization collaborates in the cloud, you need to protect your data while also making sure you stay compliant with regulations. You need an intricate knowledge of your data and how your users behave to ensure that only the right people have access.

You need to be able to spot suspicious activity such as excessive login attempts or mass downloads, regardless of devices or cloud. The same goes for being able to locate your data across multiple clouds and classify it to prevent leaks. In this collaborative environment with no boundaries, you need to regain the visibility and controls you had in your perimeter.

Control access to your data wherever it goes

Security needs to follow your data wherever it goes — regardless of who is using it, how it's being used and which cloud services it flows through. In one place, Fortra CASB helps discover, classify, and protect your data, with complete visibility into your cloud and SaaS apps so you can secure and control data sharing across users, apps, and devices.

We enable you to dynamically dial-in precise access with deep understanding of how your users behave and the types of data they access and share. With an optimal combination of forward and reverse proxies, we give you control over all endpoints and app instances regardless of whether they are managed by your organization or not.

BENEFITS

- Simplifies security governance on all cloud and SaaS apps
- Integrates with productivity suites such as Google Workspace and Microsoft 365
- Delivers extensive data discovery capabilities across multi-cloud deployments
- Protects data with advanced classification and data loss prevention (DLP)
- Secures and controls data shared externally with encryption and rights management
- Detects insider threats with user and entity behavior analytics (UEBA)
- Manages security posture of cloud infrastructure and applications
- Detects and prevents advanced zero day threats with Cloud Sandbox

In addition, Fortra CASB integrates with enterprise mobility management (EMM) solutions to enforce access policies at the endpoint. We also ensure that you stay in control across multi-cloud environments. This helps you meet compliance requirements and protect your sensitive intellectual property by restricting how your data is handled.

Selection of context-aware attributes

- User
- User group
- IP address
- Location
- Device type
- Operating system
- User behavior
- Device compliance
- IP risk

Discover, classify, and protect your data

Controlling access to your cloud services and data is the first step, but you also need to know what data you have, where it is located and how to protect it. CASB gives you the capability to locate all your data across cloud services, users and devices. We also classify the data in real time to protect it with the highest level of encryption.

Fortra enables you to scan historical data in the cloud to discover any unprotected information and open file shares, preventing potential data exposure. With centralized data loss prevention (DLP) policies, you can detect, classify and protect sensitive data across any cloud deployment, email and applications in a consistent manner. This enables you to preserve the integrity of your regulatory data such as Personally identifiable information (PII), Protected health information (PHI), and information classified as Payment Card Industry (PCI), while enabling seamless collaboration.

Your organization can enforce enterprise digital rights management (EDRM) to secure offline information exchange and file sharing. Based on the level of sensitivity, EDRM automatically encrypts sensitive files while they are downloaded, and permits only authorized users with valid decryption keys access to those files.

Detect and remediate cyber threats

Clouds are highly targeted by cyberattackers because they have valuable data. In addition, their APIs enable lateral movement to adjacent cloud services that by-passes conventional network anti-virus systems. CASB scans all inbound and outbound content to detect and stop viruses, malware and ransomware.

CASB automatically quarantines infected content on the fly without adding any noticeable latency.

With the addition of Cloud Sandbox, CASB can identify malicious content that isn't identified as a known threat, to reduce the risk of exposure across your ecosystem. Files, hashes, and URLs are scanned to identify and quarantine advanced threat vectors like zero day malware. Each file submission is compared to threat actors' latest known tactics and signatures using static analysis, AI, and machine learning. You not only receive a verdict, but supporting contextual details like MITRE ATT&CK mapping and file, registry, process, and network changes.

CASB User and Entity Behavior Analytics (UEBA) continuously assesses users, devices and activities to detect anomalous behavior and remediate potential threats. Examples include excessive file downloads, login attempts from a user, or persistent login attempts by an unauthorized account.

Know the security posture of your clouds

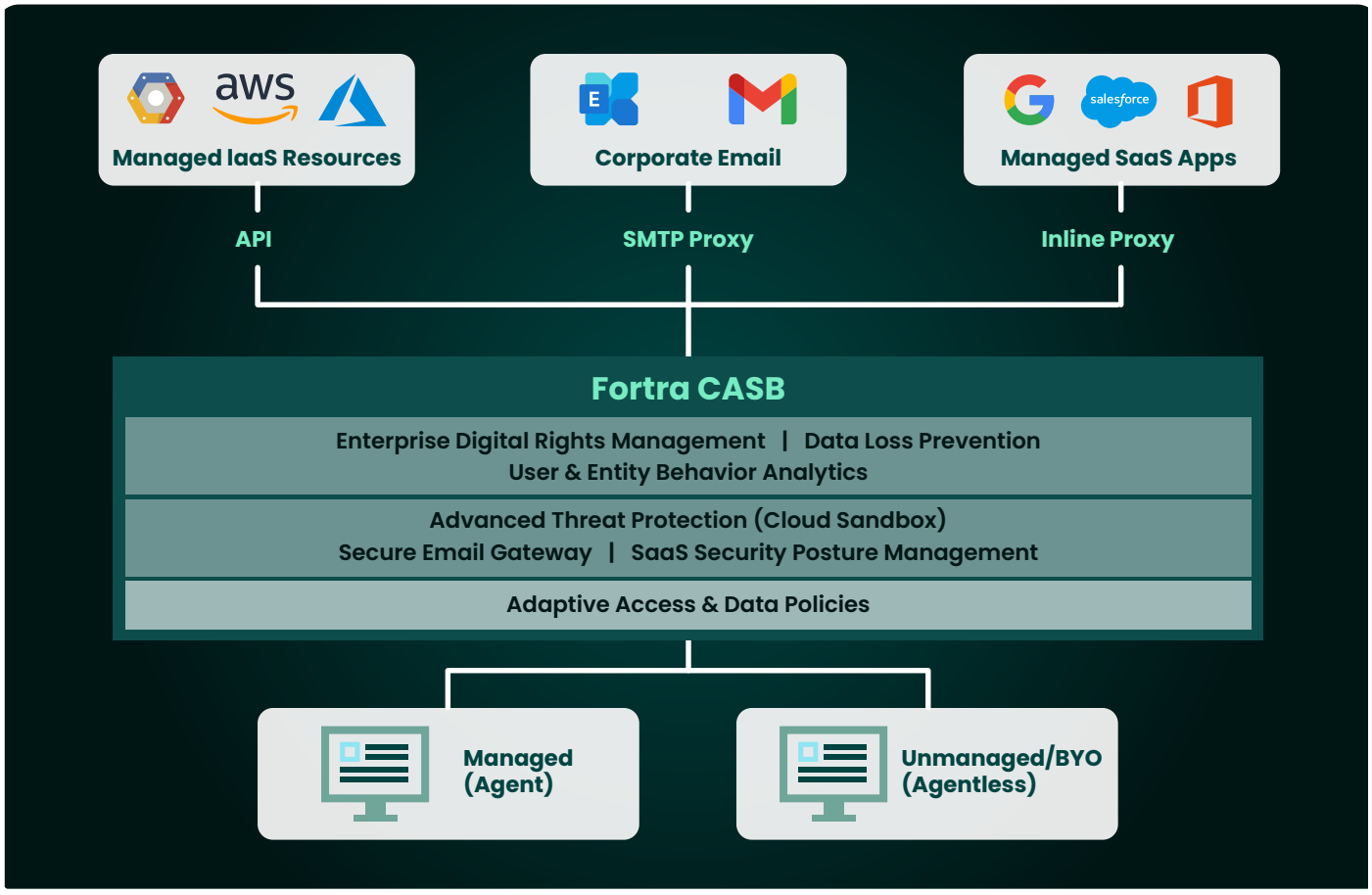
With visibility into the security posture of cloud infrastructure and applications, you can enforce data protection policy controls. Cloud and Software-as-a-Service Security Posture Management (CSPM/SSPM) perform automated assessments and remediation of SaaS and Infrastructure-as-a-Service environments to detect misconfigurations and enforce security guardrails to prevent account compromise.

Secure against shadow IT

Fortra CASB also helps your organization limit the risk exposure of shadow IT. By integrating with existing network devices, firewalls, and proxy services, CASB assesses cloud service usage and provides you with complete visibility into cloud services used by your organization. This information is delivered to you through intuitive in-depth dashboards, real-time alerts, and audit reporting.

The Fortra CASB Advantage

- Frictionless deployment for cloud apps
- Agentless design for rapid deployment
- Zero Trust adaptive access control
- Cloud and SaaS Security Posture Management
- Cloud email security and governance
- Advanced policy engine and compliance management
- Advanced data protection including:
  - Data discovery
  - Data Loss Prevention
  - Enterprise Digital Rights Management
  - Encryption
- Enterprise integrations with
  - Identity Access Management
  - Data Loss Prevention
  - Data classification
  - Security Information and Event Management
  - Security Orchestration Automation and Response
  - Mobile Device Management



FORTRA

Fortra.com

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.