FORTRA

Minimize Risk To Your Corporate Data With End-to-End Visibility and Intelligent Security Controls

Free Your Hybrid Workforce
with Fortra Cloud Data Protection

Equipped with personal tablets and smartphones, workers can now connect directly to your corporate resources from their home and unsecured networks. While this has streamlined business operations and boosted productivity, it has also exposed your valuable data to new risks.

Currently, many organizations rely on traditional security tools that focus on static, point-in-time authentication that is ideal for data access within a defined perimeter. The philosophy is that if a user's identity is proven with a password and a second factor of authentication, then they are safe to access data.

The problem is that users are not always using corporate devices, may have malicious intent or accidentally share sensitive information with an unauthorized user. If you are using a virtual private network (VPN) or single sign-on (SSO), you can authenticate and authorize users at the time of access, but these tools will not protect from any malicious or accidental exfiltration of corporate data.

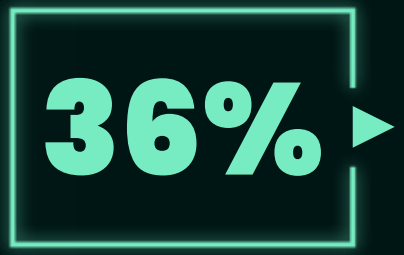
HIGHLIGHTS

- **With hybrid work, your data is now flowing freely between cloud apps, private apps, and endpoint devices, which means it's exposed to countless new risks.**
- **To minimize risk to your data as it's being accessed from anywhere, you need visibility from endpoint to cloud, including continuous assessment of device and user risk levels as well as an understanding of data sensitivity levels.**
- **Alongside end-to-end insights, you also need the ability to enforce consistent policies regardless of where your organization's data resides or how it's accessed.**

With the countless apps, users, and endpoints to keep tabs on, the traditional, appliance-based approach to security is no longer enough. Point products create silos, which in turn create management burdens on your already stretched IT and security teams. They also give you limited insights and control over what's happening to your data.

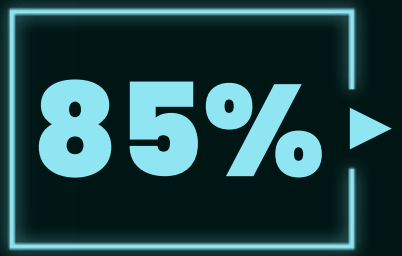
To ensure that your data is protected in this complex environment, you need to pivot into a platform approach. This requires finding a solution that combines continuous end-to-end monitoring alongside a unified policy framework.

In this eBook, we will discuss how to minimize the risk to your data and how Fortra's cloud data protection product line can effectively minimize risk regardless of where your data resides.



of IT and security professionals cite remote users as the top contributor to public-cloud related data loss.

- Enterprise Strategy Group



of data breaches involve a human element, including errors and misuse of credentials.

- Verizon Data Breach Investigations Report (DBIR)

Mitigating risk starts with getting complete visibility of the land

The cloud has made it simpler to streamline and scale operations. It also gives your users easy access to apps and data so they can stay productive from anywhere and any device. But this way of working also introduces a host of new threats like phishing attacks, cloud misconfigurations, and corporate data exfiltration from these apps.

It's no longer reasonable to assume that your on-premises tools have insights into the activities within your infrastructure and the entities seeking to access your resources. Instead, you need continuous insights into the various environments where your data is flowing.

Fortra's cloud data protection product line provides end-to-end insights into these three major areas:

Cloud apps

Thanks to cloud apps, you no longer have to worry about running your own data centers, but there are still a lot of responsibilities that fall onto your IT and security teams. Ultimately, it's up to you to secure your environment, configure them, and understand what data resides within the apps and how it can be shared across users, devices and networks. Fortra grants robust insights into what's happening in your cloud apps.

Private apps

As organizations go through digital transformation, resources in private clouds or on premises are sometimes forgotten. This could make them targets for malicious users that want to move laterally around your infrastructure. Fortra continuously monitors and protects data residing in your private apps. It provides users' access to these apps based on the risk posture of their devices and only gives users access to the apps they are authorized to access.

The web and shadow IT

With hybrid work, the internet has become your default corporate network. Therefore, it's critical that you have visibility into internet usage, not just to intercept malware but also to prevent data leakage and enforce acceptable use policy. And the unmanaged cloud apps your employees are using are part of this picture. Fortra inspects both inbound and outbound internet traffic for any sensitive or malicious content that may affect integrity of your corporate data or compromise your underlying infrastructure.

Contextual insights to precisely protect data

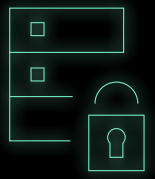
It's not just about the breadth of insights. You also need to understand the context and fluctuating risk levels affecting the integrity of your data.

It's this continuous insight into users, device posture, and consistent policy enforcement that separates some cloud security solutions from others. With a focus on protecting data, Fortra's cloud data protection product line ensures that policies are enforced even when data is being suspiciously modified or it flows to unmanaged devices, including mobile devices.

"29% of IT and security professionals cite persona devices as the top contributor to public-cloud related data loss"

- Enterprise Strategy Group

Fortra equips your team with:



Endpoint security

Personal devices including mobile devices are used to access corporate resources. And due to the different apps they can have installed and the networks they can connect to, these endpoints' risk levels are constantly fluctuating. With continuous monitoring of endpoint device health, you can protect your data from insecure networks and outdated operating systems as well as app vulnerabilities, malware, and phishing attacks.

User and entity behavior analytics (UEBA)

With people working from anywhere, you no longer have the control you used to have within corporate perimeters. Therefore, it's critical that you constantly monitor the behavior of your users. Whether it's the apps that they connect to or how they access and modify data, identifying anomalous behavior is critical to prevent a malicious insider or a compromised account from stealing your data.

Data loss prevention (DLP)and digital rights management (DRM)

To protect data effectively, access security is not enough. You need controls to protect and reduce risk to your corporate data. With native data protection capabilities as part of a cloud security platform, you can identify data sensitivity and enforce the right policy to limit access like masking and redacting sensitive information, or encrypting and sharing sensitive documents, instead of denying access to information outright.

Unified insights and dynamic policy enforcement

With thousands of activities and entities and hundreds of apps to keep tabs of, figuring out how to protect your data can be overwhelming. By combining endpoint-to-cloud visibility with advanced data protection capabilities, Fortra automates the process of minimizing data risk.

By leveraging deep insights alongside a unified policy engine, Fortra protects our customers and their data, and keeps them compliant. Data loss can be either accidental or malicious - Fortra protects against both possibilities:

Accidental data exfiltration

Cloud apps have made collaboration and data access very simple. But that also means it's easy to accidentally share content to the wrong person. By monitoring network traffic, Fortra can detect whether sensitive data is being leaked out. With native data protection, the platform can enforce various data protection measures including watermarking and keyword redaction.

Malicious insider threats or account takeover

Whether it's a legitimate user gone rogue or an employee's account that's been taken over, it's difficult to detect whether a user is putting your data at risk. Using user behavior analysis in our analytical engine, Fortra benchmarks what's normal so that when anomalies are detected, such as excessive downloading or data modification, the platform can block or caution the users, based on the policies set by an administrator.

Minimizing data risk requires a holistic approach

The digital landscape has become much more complex because of cloud adoption and hybrid work. With data no longer residing in one place, organizations need security that can handle that complexity.

This requires a fundamental shift in how you approach, plan, and deploy your security strategy. Rather than rely on appliance-based tools that forces teams to be divided into silos, you need to look at a platform approach.

Fortra's cloud data protection product line provides insights into users, endpoints, apps, and data, ensuring that data is protected regardless of whether it’s in cloud apps, private apps, endpoint devices, or flowing through the internet.

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.

| fta-cdp-ebook-0625-r1-an