FORTRA™

How Multiple Industries Found Success with Digital Guardian Secure Collaboration

Table of contents

What Is Digital Guardian's Secure Collaboration?

In the digital age, where data reigns supreme and security is paramount, organizations across various industries are continually challenged to safeguard their sensitive information. While organizations' specific data protection needs may vary across different industries, one common thread unites them all: the pursuit of robust and user-friendly solutions that can seamlessly integrate into existing workflows. Digital Guardian's Secure Collaboration has emerged as a pivotal tool in this endeavor. With its ability to protect data at a granular level and enhance existing data protection tools like data loss prevention (DLP) and data classification, our solution has enabled a wide variety of organizations to navigate complex security challenges successfully.

The following collection of 19 case studies serves as a testament to the diverse capabilities and tangible benefits that organizations across the manufacturing, media & entertainment, financial services, healthcare, and technology industries have experienced with Digital Guardian's Secure Collaboration solution. These success stories are not just accounts of data protection; they are narratives of transformation, where organizations, despite differing needs and industry-specific demands, leveraged Secure Collaboration to bolster their data protection capabilities.

Throughout these case studies, one message is clear: Digital Guardian's Secure Collaboration solution is more than just a powerful tool. It is a transformative force that empowers organizations to protect their most valuable asset—data—without being forced to make unwanted compromises for the sake of security. The stories herein demonstrate that whether an organization seeks enhanced control over sensitive documents, improved integration with existing tools, automation of security processes, or robust encryption, Secure Collaboration is the versatile and effective solution that can deliver tangible results. Join us as we unravel 19 success stories of organizations that have harnessed the power of our robust solution to achieve data protection excellence.

Media & Entertainment Organizations
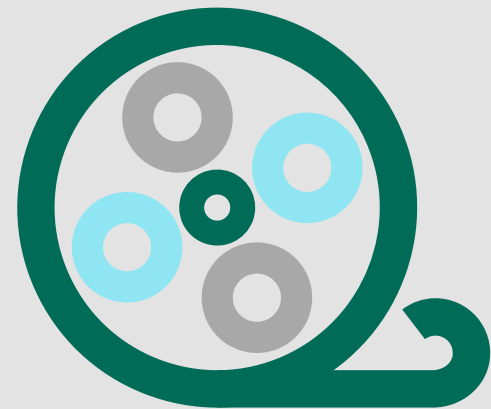
Why Media & Entertainment Organizations Choose Secure Collaboration

Within the media and entertainment industry, organizations undoubtedly must uphold content quality to succeed, but just as importantly, they must maintain audience trust, address intellectual property concerns, and comply with increasingly stringent data privacy regulations. For those reasons, it's of critical importance for these organizations to protect the viewership metrics, user-generated content, streaming behavior, demographic insights, content consumption patterns, and other forms of data that they collect and use. And to enable the continuous production of original, high-quality content, organizations' intellectual property, including their copyrighted content and proprietary media assets, are just as important to protect.

The Pokémon Company International
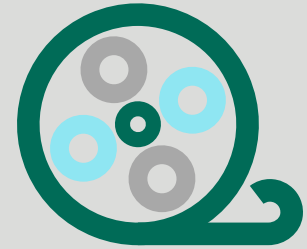
The Pokémon Company International faced the challenge of securing valuable, rich media files like game designs across collaborative external parties, but they needed a solution compatible with existing tools that wouldn't slow down collaboration and productivity. Finding a solution that enabled continuous visibility over data shared with third parties and the mitigation of associated risks was another top priority.

Digital Guardian's Secure Collaboration offered a content-agnostic solution that dynamically and persistently protected content, regardless of file type. Seamless integration with key tools already in use by the organization, like Office 365, SSO, AD, and Dropbox, ensured smooth operations. Lastly, a full audit trail with granular tracking provided detailed insights into how content was accessed, enhancing security.

2:23

**The Pokémon Company**
INTERNATIONAL

A Renowned American Movie Studio, a Large American TV Network, & a Large American Sports Association
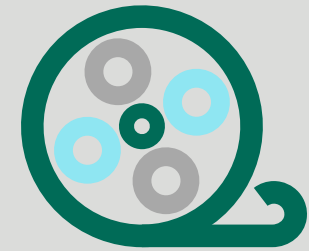
An American movie studio, TV network, and sports association all faced the similar, common challenge of maintaining control over sensitive documents stored in Dropbox and shared externally. The three organizations were all similarly juggling multiple security solutions – making their objective of protecting files and email messages needlessly tedious — so implementing a comprehensive, enterprise-ready security solution at scale was at the top of their list of priorities.

Our Secure Collaboration solution stepped in with dynamic access controls that persistently protected secured content, even after being shared. By offering a unified solution for files and email, all three organizations successfully streamlined their security practices. Our solution's file and storage-agnostic approach seamlessly integrated with existing workflows and tools, promoting user adoption and workflow efficiency.

Large American Movie Studio
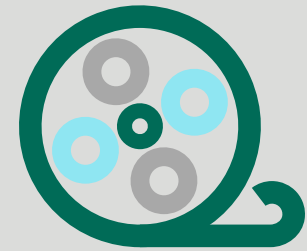
Two other large American movie studios found value in Secure Collaboration but, in comparison to the aforementioned studio, faced more specific challenges. The first of the two studios ran into security obstacles related to its custom .Net application for generating payment statements. These statements required secure and efficient distribution, but the existing, fully manual process was time-consuming, costly, and lacked the security the organization required.

Our Secure Collaboration solution's Software Development Kit (SDK) was integrated with the custom application to automate document protection upon generation. The studio also automated statement delivery through our solution's email connector, further eliminating unnecessary manual steps. Our solution provided the studio's talent with secure access to statements anytime, anywhere, and without the need for passwords or installations.

Large American Movie Studio
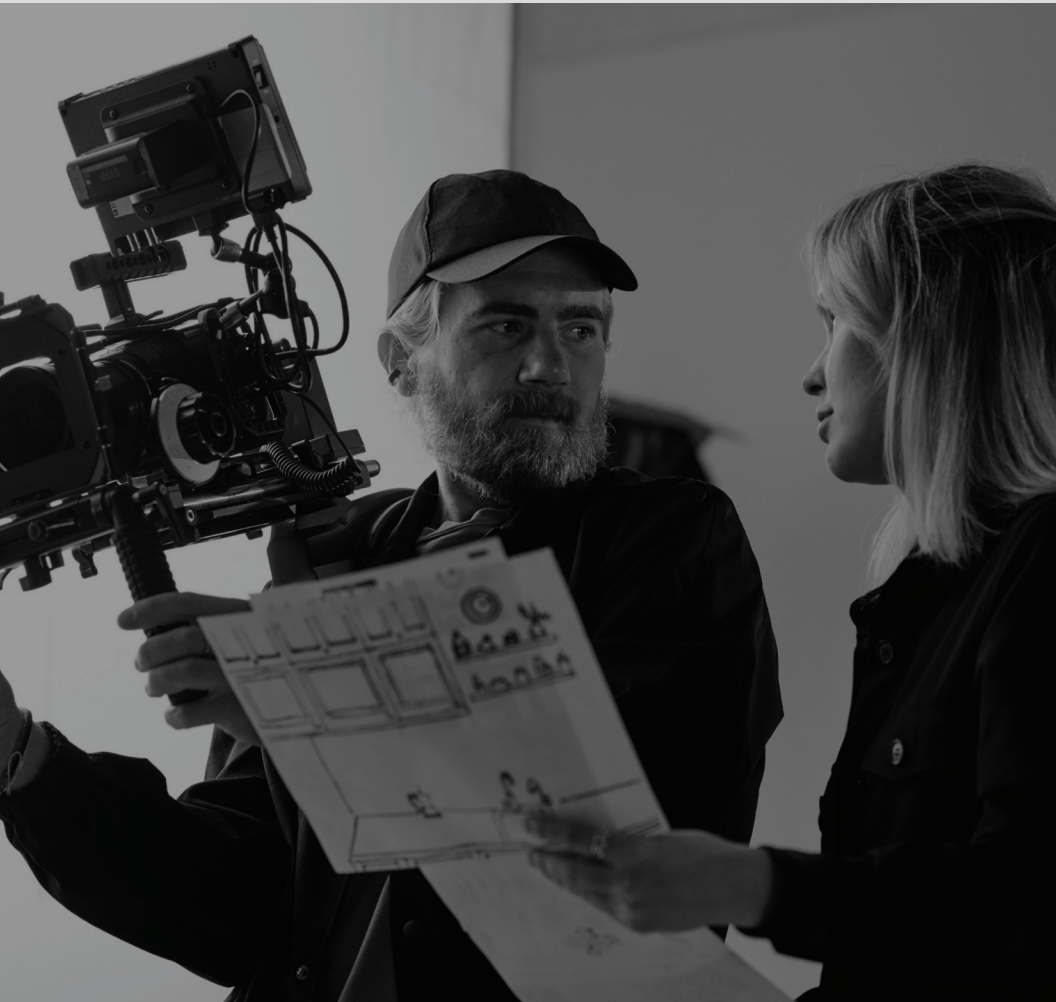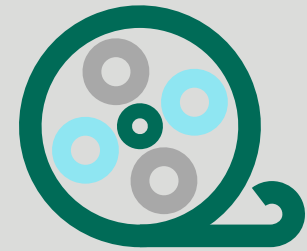
The second of the two studios faced challenges in providing and managing access to its script distribution system, which was custom-made and not user-friendly. They needed a cleaner, scalable solution for delivering scripts to external talent and integrating it with their custom application.

In this instance, Secure Collaboration's SDK was seamlessly integrated with KeySafe to protect scripts delivered to external talent, successfully reducing manual workflows by a significant margin. Furthermore, the inclusion of our solution's View in Browser capabilities ensured a frictionless experience for "blue-chip" end users, meaning the organization no longer had to worry about those end users managing passwords or software installations.

Large American Theme Park & Movie Studio
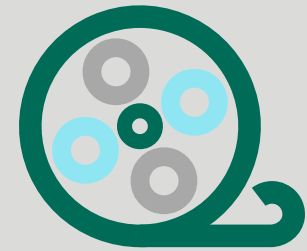
This organization provided a service to expatriate employees that handled their taxes. However, securely sharing tax-related data was cumbersome. Their existing solutions — SharePoint and Cryptzone — required constant administration and had scalability issues.

Secure Collaboration's integration with SharePoint automated encryption and policy assignment, eliminating end-user intervention. The protection traveled with tax documents, regardless of whether they were being handled by the company, employees, or Deloitte at any given time. And similarly to the previous movie studio represented here, our solution's View in Browser capability simplified access for end users on any device, enhancing efficiency.

Manufacturing Organizations
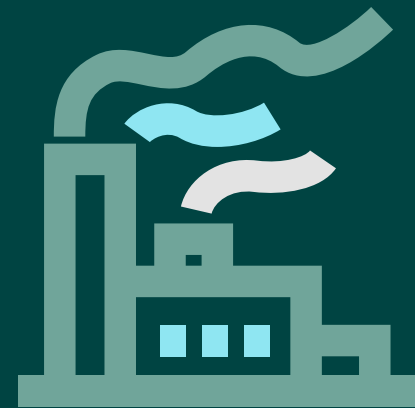
Why Manufacturing Organizations Choose Secure Collaboration

In contrast, organizations in the manufacturing industry harness various data types to optimize processes, drive innovation, and ensure quality control, often including production metrics, supply chain data, product specifications, and quality assurance records. Moreover, IoT devices, and the real-time data on machine performance and production lines that they generate, promise enhanced productivity and cost savings and are of critical importance to modern manufacturing organizations. The stakes are high for manufacturing organizations, as breaches or disruptions in their data can result in costly downtime, product defects, supply chain disruptions, and even compromises in intellectual property. Implementing comprehensive data protection solutions can prevent organizations from encountering any such issues.

Leading Global Resources Company
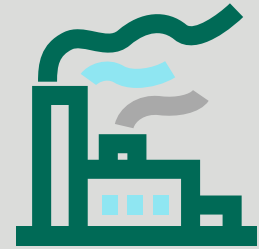
A leading global resources company faced challenges in controlling and securing various types of sensitive information, including intellectual property, financial data, PII, and contractual information. They also needed to secure files across multiple platforms, including SharePoint, OneDrive, Documentum, and internal file shares (SMB). Finally, the organization sought a solution that would integrate with their existing data loss prevention (DLP) and data classification solutions, and apply information rights management based on context.

Digital Guardian's Secure Collaboration offered always-on protection for sensitive information, regardless of its location, yet also automated security processes based on file location, preventing data leaks. This solution allowed for automation of security without requiring end-user involvement, ensuring comprehensive protection.

Global Building Materials Company
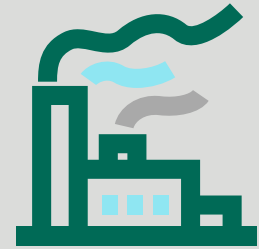
This global building materials company faced significant challenges in protecting its intellectual property (IP). With over 100 patents, their IP was the core of their business. The organization's 10-K and 20-F filings with the SEC identified the protection of their IP as three of their top five priorities in both 2017 and 2018. More specifically, they needed a solution to protect CAD designs and other sensitive files stored in SharePoint and shared externally via ShareFile.

After an exhaustive evaluation, the organization chose our Secure Collaboration solution as their path forward. Integration with SharePoint automated the protection of sensitive files upon upload and sharing with partners, and by eliminating the use of point solutions like ShareFile and FTP, the company maintained control and visibility over its most sensitive IP.

Large US Food Company
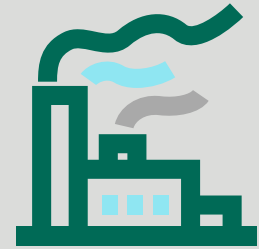
A large US food company faced the challenge of maintaining visibility and controlling access to confidential formulas and sensitive data. They needed a security solution that seamlessly integrated with Microsoft Office tools like SharePoint and could internally secure financial reports and legal agreements.

Secure Collaboration provided dynamic access controls that prevented data from being shared beyond approved recipients, while simultaneously offering visibility and control over sensitive information without hindering collaboration. Furthermore, its file and storage-agnostic nature ensured smooth integration with the company's existing ecosystem of tools.

American Food Processing Machinery and Airport Equipment Company
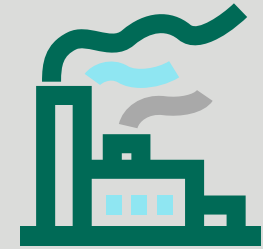
An American food processing machinery/airport equipment manufacturing organization faced multiple security-related challenges. They found that they were losing control over proprietary drawings shared through Windchill and Creo, lacked monitoring access to PDFs distributed through platforms like Box and Citrix ShareFile, were vulnerable to data leaks via email attachments and/or insider threats, and weren't achieving adequate employee buy-in to guarantee secure workflows.

Our Secure Collaboration solution gave the organization the ability to see and block access to PLM files in real-time. It allowed them to expire vendors' and customers' access to marketing assets and alter permissions for content shared with previously approved recipients. And finally, employees across global offices could now work in a streamlined and secure manner.

American Multinational Conglomerate
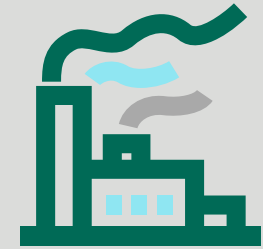
The American multinational conglomerate had to protect data shared through cloud services, secure critical IP in CAD and PLM systems, enforce access controls and security policies consistently, and secure sensitive data generated by legacy business apps during their global digital transformation.

Secure Collaboration enabled the organization to store and collaborate on highly classified data in modern tools like Box, driving cost savings and efficiency. The solution's audit logs provided centralized reporting and alerting, even for content outside the company. Lastly, the solution automated security protocols, like the application of encryption, without impacting employees, ensuring a consistent data security approach.

FORTRA

Large American Shoe Manufacturer
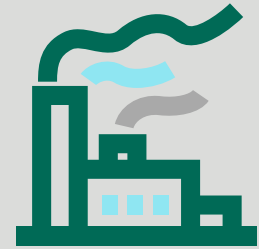
Initially deploying WatchDox, another secure collaboration tool, proved unsuccessful for this large American shoe manufacturer after experiencing low adoption, poor end user feedback, and high maintenance costs. They needed a solution that could protect complex design documents (CAD, Adobe Creative Suite, etc.) while being intuitive for end users. They also had a wide array of use cases and custom apps to support.

Secure Collaboration was deployed globally in under three months and received positive feedback from end users for its user experience. Integration with Box ensured the protection of IP across multiple devices and countries while reducing user count and overall costs. Since the original deployment, the organization also deployed our solution's SDK to protect 3D design documents throughout their lifecycle.

Learn more about Secure Collaboration on our website

Large American Clothing Manufacturer
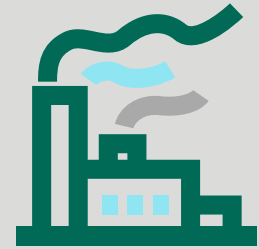
At the time of deployment, a large clothing manufacturer had a proprietary, 100% green method for cutting and conditioning jeans/denim that they needed to protect as they distributed it to international manufacturing partners. They required secure sharing while maintaining control and integrity of their manual.

Secure Collaboration enabled the company to protect documents before sharing them with over 25 manufacturing partners globally, and it was deployed quickly to meet the launch date for the announcement. Our solution's agentless delivery option ensured partners could access the content without needing to install clients.

Financial Services Industry

Why Financial Service Organizations Choose Secure Collaboration

In the dynamic landscape of the financial services industry, data reigns supreme as the lifeblood of modern organizations. From banking institutions to investment firms and insurance companies to fintech startups, these entities rely on a diverse array of data types to fuel their operations and gain a competitive edge. Commonly utilized data in this sector includes sensitive customer information such as personal identifiers, financial transactions, and credit scores. Additionally, organizations frequently leverage market data, economic indicators, and historical trends to inform decision-making processes and optimize investment strategies. While the acquisition and utilization of data offer immense opportunities for growth and innovation, it also exposes organizations to a heightened level of risk. Protecting these data assets is of paramount importance, not only to ensure compliance with stringent regulatory requirements but also to safeguard customer trust and maintain the integrity of financial markets.

Global Venture Capital Firm

A global venture capital firm faced significant challenges in securing sensitive IR communications, and their business operations were restrained because these communications lacked protection beyond the organization. Additionally, they experienced a loss of visibility and control over files shared externally with limited partners (LPs). Controlling access to internal and financial files uploaded and shared via Box proved to be another challenge.

Digital Guardian's Secure Collaboration came to the rescue by offering persistent protection that seamlessly integrated with existing workflows. With Secure Collaboration, the customer regained control over their data, thanks to dynamic data protection and access controls. Now, all sensitive data is automatically secured when uploaded to Box, providing a comprehensive audit trail for added security and visibility.

Global Bank

A global bank was grappling with the need for rigid access control policies and general security for highly sensitive documents. The COVID-19 pandemic further emphasized the necessity of providing on-demand secure document access for thousands of users, but the organization found that their virtual desktop infrastructure (VDI) was costly and caused customer support issues.

Secure Collaboration's "magic folder" provided bank executives with secure and exclusive access to highly sensitive documents, and the organization had access to detailed audit logs for exceptional visibility and tracking of sensitive, unstructured data. This innovative solution eliminated the need for VDI, resulting in cost savings and optimized call center agent productivity while still ensuring the protection of customer information.

Healthcare Organizations

Why Healthcare Organizations Choose Secure Collaboration

In the healthcare sector, data plays a pivotal role in patient care, medical research, and operational efficiency. Healthcare organizations, encompassing hospitals, clinics, pharmaceutical companies, and research institutions, rely on various data types to enhance healthcare outcomes and propel medical advancements. These include electronic health records (EHRs), patient demographics, treatment histories, medical imaging files, and genomic data. These datasets are invaluable for diagnosing and treating patients, conducting clinical trials, and personalizing medical interventions. However, within this data-rich healthcare ecosystem, the significance of data protection cannot be overstated. Unlike other industries, healthcare data breaches can have dire consequences beyond financial loss. Unauthorized access to patient data can jeopardize patient privacy, lead to medical identity theft, and even endanger lives. Furthermore, healthcare entities must adhere to strict regulatory standards, such as HIPAA in the United States, that necessitate robust data security measures for patient information.

Community Health System

A non-profit community health system serving patients across a Southern U.S. state, faced the loss of visibility and control over internal data, including PHI and PII, after sharing. They needed to secure data stored and shared across various record management systems. Accurate auditing of data subject to HIPAA was crucial, and they sought to streamline security solutions.

Our Secure Collaboration solution provided persistent and dynamic protection, tracking, controlling, and blocking access even after data was shared. Its content and storage-agnostic nature complemented their existing tools, and granular analytics offered a full chain of custody. The solution's seamless integration with productivity tools like Dropbox preserved employees' existing workflows.

Regional Health Center

This non-profit regional health center in Southern California provides lifelong services and support for people with developmental disabilities. They sought to modernize their collaborative efforts by using cloud storage like Box while maintaining control over the PHI being shared. But in doing so, they had to demonstrate sufficient security and audit capabilities to comply with strict HIPAA regulations and prevent unauthorized distribution of information.

Secure Collaboration provided strong security that's automatically integrated with tools like Box, ensuring the protection of sensitive data while maintaining productivity. Its data-centric technology offered a full audit trail for tracking access to and use of PHI, along with the ability to alter or revoke access in real-time, meeting HIPAA compliance requirements.

Technology Organizations
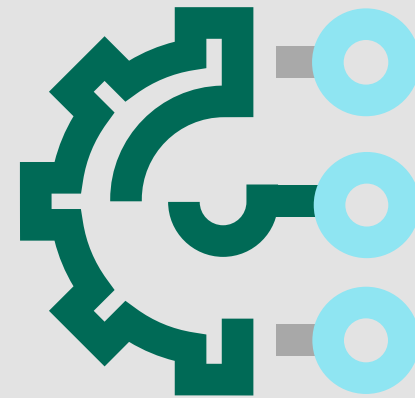
Why Technology Organizations Choose Secure Collaboration

The technology industry encompasses a broad range of organizations from software giants to hardware innovators and digital service providers. Within this landscape, user-generated insights, vast software repositories, performance analytics, proprietary intellectual assets, invaluable customer feedback, and more are all used to drive organizations' core operations, fuel product development, enhance user experiences, foster innovation, and maintain a competitive edge over competitors. Given the sensitivity of such data, breaches in the tech sector have ramifications extending beyond financial losses, encompassing damage to brand reputation, loss of customer trust, and potential legal consequences, meaning data protection and regulatory compliance often take center stage for most technology organizations.

Global Network Equipment and Software Company
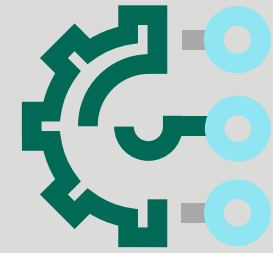
A global network equipment/software company's prior attempts to deploy enterprise-wide encryption and access control saw low adoption rates, thus stalling. Tech support had no way to protect sensitive customer data and logs or enforce ethical walls. GDPR compliance, including the discovery and classification of content across 90,000 employees and six continents, along with the security of that data across hundreds of cloud apps and custom business processes were also significant challenges.

The organization began by implementing our Secure Collaboration solution to address two key use cases: brand asset protection and high-value document management. Integration with Confluence, Box, and Alfresco extended protection to customer logs shared with tech support. The creation of a 'Trusted Security Zone' ensured encryption, tracking, and audit capabilities, even outside the company.

Why Digital Guardian's Secure Collaboration?

Digital Guardian's Secure Collaboration solution on its own is a standout choice for organizations seeking robust data protection. Unlike some competing solutions, Secure Collaboration prioritizes user-centric security experience, ensuring seamless integration into daily operations without hindering productivity. Furthermore, our solution's granular control over data access sets it apart. Rather than simply providing blanket protections, organizations can assign specific permissions at the individual file level, offering unparalleled data protection precision even after Send. That precision extends to encrypted data, regardless of whether it's at rest or in motion, inside or outside of your corporate environment.

Secure Collaboration's unique strength, however, lies in its ability to enhance other data protection tools like data loss prevention (DLP) and data classification. It interlocks intuitively with DLP systems, reinforcing DLP policies with file-level protection and ensuring data remains secure -- even in scenarios where DLP may fall short on its own. Moreover, our solution streamlines data classification efforts by identifying sensitive data and automatically applying protection policies to sensitive files, reducing the risk of human error and ensuring compliance.

In conclusion, Digital Guardian's Secure Collaboration is a powerful and versatile data protection solution. Its user-friendly, data-centric approach, granular control, robust encryption, and synergy with your organization's existing data protection infrastructure make it a compelling choice. With Secure Collaboration, organizations can secure their data effectively, streamline data protection processes, enhance productivity, and gain peace of mind.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.