SPANNING
A Kaseya COMPANY

DATASHEET

SPANNING DARK WEB MONITORING

FRONT-LINE PROTECTION AGAINST CYBERTHEFT AND FRAUD | PURPOSE-BUILT FOR GOOGLE WORKSPACE

BENEFITS

- Reduces the risk of a significant data loss incident requiring a costly, resource-intensive recovery and restoration effort
- Reduced risk of IP theft
- Reduced risk of financial fraud
- Reduced risk of a Business Email Compromise attack

KEY CAPABILITIES

- Continuous and intelligent search, analysis and monitoring of the dark web for potentially compromised or stolen Google Workspace credentials
- Reports on all accounts in the domain – even if they are not licensed for backup
- Administrator email alerts
- Administrator dashboard integrated into Spanning Backup for Google Workspace
- Configurable report views
- Tailored notification settings

PREVENT DATA LOSS BEFORE IT OCCURS

Spanning Dark Web Monitoring for Google Workspace alerts administrators of compromised or stolen employee credentials, enabling them to take proactive steps to secure those accounts before malicious activity occurs. They can then leverage Spanning's audit reporting and search capabilities to determine if data loss has taken place and restore corrupted data in just a few clicks. The service is pre-configured and provides intuitive administrator controls integrated with Spanning Backup, activated within Google Workspace, and designed to provide an administrator experience identical to Google Workspace.

PROTECTING GOOGLE WORKSPACE CREDENTIALS

Email is the primary target for hacking and fraud, and weak or stolen credentials are the number one hacking technique. Google Workspace credentials enable access to more than just that individual's email account. They secure access to all the user's Google Workspace applications and services, such as Drive, Team Drives, Hangouts, and Sites, as well as other Google services containing sensitive information, including Analytics, Ads, and Google Cloud. Additionally, they protect thousands of data-rich, third-party business applications, such as Human Resource Management, Payroll, Customer Relationship Management, Project Management, Professional Services Automation, and Marketing Automation systems.

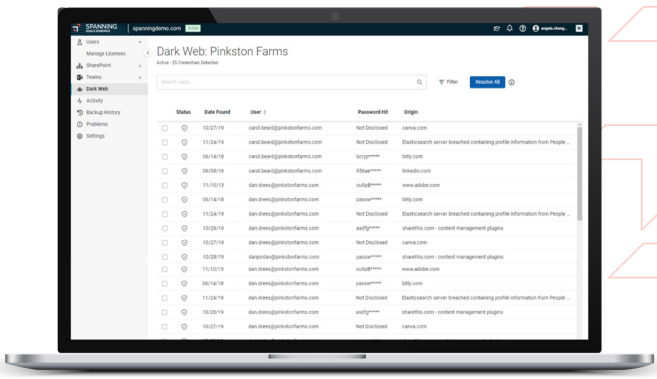
PROACTIVE DEFENSE AGAINST ACCOUNT TAKEOVER ATTACKS

Account Takeover (ATO) attacks have become a very common and lucrative business for cybercriminals, who steal or buy credentials from third-party breaches and then reuse them to gain easy access to corporate systems. This enables them to steal IPs, perpetrate business email compromise, access financial accounts, and commit other types of cyber fraud. Spanning Dark Web Monitoring reduces the risk of an ATO, protecting the business from potential financial and competitive impacts and minimizing the chance of a significant data loss incident requiring a costly, resource-intensive recovery and restoration effort.

FAST AND EASY TO INSTALL AND USE

Our service is pre-configured and provides intuitive administrator controls integrated with Spanning Backup, activated in Google Workspace, and designed to provide an administrator experience identical to Google Workspace.

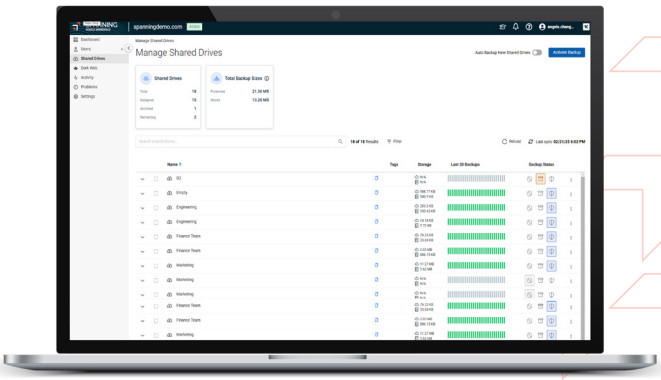
- Functionality is installed and configured in minutes
- Instant, automatic connectivity to your domain
- Report with current status plus alerts of newly identified compromised accounts
- Customizable Dashboard enabling filtered views based on Date, Active Status, Type, and Source



INDUSTRY-LEADING MONITORING PLATFORM

Spanning Dark Web Monitoring is based on the latest in dark web surveillance technologies. We combine human expertise and sophisticated Dark Web intelligence with comprehensive search capabilities to identify, analyze and proactively monitor for your organization's compromised or stolen credentials.

- Powerful, comprehensive search of botnets, criminal chat rooms, blogs, websites and bulletin boards, peer-to-peer networks, forums, private networks, and other black-market sites
- Leverages a combination of human and artificial intelligence for enhanced analysis
- Monitors over 500 distinct Internet Relay Chatroom (IRC) channels, 600,000 private websites, 600 Twitter feeds, and executes 10,000 refined queries daily



LEARN MORE ABOUT SPANNING AND START *A FREE TRIAL HERE.*

LEARN MORE

SPANNING
A Kaseya COMPANY

Spanning Cloud Apps, a Kaseya company, is the leader in SaaS Cloud-to-Cloud Backup, proven and trusted by more than 10,000 organizations across the globe to provide enterprise-class data protection. Spanning's cloud-native, purpose-built solutions for Microsoft 365, Google Workspace, and Salesforce provide easy-to-use yet powerful capabilities for end users and administrators and meet the rigorous requirements for listing on Microsoft AppSource, Salesforce AppExchange and Google Workspace Marketplace.

10032025