



GTB Technologies[®]

Data Security that Works[®]

GTB Enterprise Data Security Suite

Unlimited Real Time Cloud Scans & On-Prem
DLP for Endpoint, Email, Cloud & Network

Protect the entire network with our Enterprise Data Security Suite



Phone Number
+1.800.626.0557

www.gttb.com



Major Drivers of Data Security Projects

Insider Threat Management

GTB Technologies Inc. Enterprise Data Security Suite delivers comprehensive solutions essential to achieve real use cases of Insider Threat Management and Data Security standards for enterprises across any industry.

GenAI Technology

GTB Enterprise Data Security Suite stands out as a leader in providing unparalleled protection of sensitive data including intellectual property and PHI/PII with a Generative AI (GenAI) technology that seamlessly integrates into existing security frameworks.

Data Privacy & Data Security Compliance

GTB Enterprise Data Security Suite will safeguard enterprise PHI/PII and intellectual property to meet compliance mandates such as HIPAA, GDPR, CCPA, LGPD, ITAR, NIST, PCI DSS, GLBA, CMMC etc. GTB Enterprise Data Security Suite is delivered in two phases with Data Discovery & Classification as well as Data Loss Prevention (DLP).

The GTB Enterprise Data Security Suite



Email DLP

Complete real time analysis on all outbound emails from Office 365 and G-mail. Commonly used actions include Block, Log, Quarantine and Encryption.



On-Prem & Cloud Discovery

Scan data at rest on fileshares, endpoints, databases, and cloud repositories to apply remediation actions in case confidential data is identified on unauthorized computers.



Endpoint DLP

Enterprise grade control on MacOS, Windows, and Linux computers. Light agents deployed as a Desktop-as-a-Service (DaaS).



Network DLP

GTB Endpoint Protection and Inspector monitors user activity where enterprises decide what confidential files can or cannot leave the company. These features are driven by AI to accurately identify the sensitive data with exact data matching.



Cloud DLP

GTB Endpoint Protection and Inspector oversee user activity with sensitive files in cloud apps, offering controls to monitor data sharing, destinations, and block actions for critical situations.



Auto Data Classification

Automatically apply persistent sensitivity labels for encryption, obfuscation, or DRM using multiple classification engines. Create granular labeling policies to meet data protection needs, allowing GTB to label files both on-premises and in cloud applications automatically.

Key Benefits

Simple Installation & Configuration

GTB Enterprise Data Security Suite has a user-friendly central management console that can be managed by any department.

Role Based Controls

Create unique exceptions or security rules from the company wide level all the way down to a unique user, computers, or groups.

Multi-Deployment Options

GTB Enterprise Data Security Suite can be deployed in multiple ways depending on the specific infrastructure environment of the enterprise.

Multi-Platform Installations

GTB Endpoint Protection offers security features and level of protection for MacOS, Windows, and Linux computers.

Out-of-the-Box Accuracy

Select predefined rules to be compliant with data privacy or data protection mandates that drive these projects. GTB Enterprise Data Security Suite leverages AI to accurately identify sensitive data in any industry.

Enterprise Ready Workflow

Get real time e-mail alerts for various events on company computers, users, groups, or unique assets.

GTB AI Lifeguard™

Protecting Against GenAI Unauthorized Usage of Sensitive Data

The proliferation of GenAI brings both innovation and challenges. While these AI technologies offer incredible potential, they also pose risks, particularly concerning the unauthorized usage of sensitive data. With decades of experience and a relentless commitment to innovation, GTB Technologies developed a suite of solutions tailored to safeguarding sensitive information across any industry.

Our journey in data security has been marked by unparalleled expertise. Through continuous research, development, and real-world application, we've honed our skills to address the evolving threats posed by GenAI and other emerging technologies.



Exact Data Matching

Exact Data Matching finds any Intellectual Property or records that are part of an indexed data source in either structured or unstructured targets.



Large Language Model

Advanced algorithms analyze email metadata and behavioral patterns to detect security threat terms by comparing them to normal communication patterns within each organization.



AI Pre-Defined Regular Expression

AI driven regular expression and terms needed to deliver data privacy and data protection mandates such as HIPAA, GDPR, CCPA, LGPD, ITAR, NIST, PCI DSS, GLBA, CMMC and more.

Data Discovery Server + Classification for Cloud Applications & On-Prem

SMBshares/Servers/Fileshares/Exchange/Exchange Online/Databases/SharePoint
OneDrive/AWS S3/Box/Dropbox/Google Drive/Google Workspace/Citrix Sharefile/Azure



File Shadowing

Enterpriseworkflow for high-severity items must include proof of violations. Create shadow copies of identified files for detailed reporting.



Smart Search

Increase speedand accuracy of each scan. Enterprises have the option to skip certain files with faulty data.



Optical Character Recognition

Extractand analyzetext and data from images and scanned documents to classify sensitive information, integrating with DLP and data classification for full data protection.



Real Time Monitoring

Abilityto detecta fileonce it is saved. The edits are then scanned for sensitive data.



Apply Classification Tags

Automatically apply customorpredefined tags to files in real time. Schedule scans to prepare for audits.



Enterprise Reports

Accurate C-suite reporting available after each scan to make educated decisions on files with sensitive data.



Fingerprint Detection

Identifyand track sensitive data using unique fingerprints. Accurately detect data patterns and signatures to prevent unauthorized access and exfiltration.



Quarantine Files

Automaticallymove files at scale. This remedial action for sensitive files is also useful for cloud migration projects.



Secure Remedial Actions

Implement data flow controls on selected files. Identify sensitive data and enable actions to meet data privacy and security requirements.



Incremental Scanning

Sequentially examine data in small, manageable portions to efficiently process information over time, avoiding the need to handle the entire dataset at once.



Emails vs Files

Scanand control specific user mailboxes and workstations for sensitive data, with optional remedial actions.



Discover FileShares

Scrapethewhole network for hidden or unknown fileshare within any subnet.



Multi-Threaded Technology

A file inspection method that can scan multiple files simultaneously.



File Copy

Seethe production files in a designated location for accurate results.

Inspector

For Email DLP and Network DLP

TCP Traffic / MicrosoftExchange /HTTPS Traffic/ SMTPTraffic/MTA/ICAP / Database /
File Inspection / Pattern Inspection



SIEM Integration

Ensure a seamless experience across security. Use any Security Information and Event Management products by externalizing logs.



Enterprise Email Workflow

Complete inspection of all outbound email traffic with multiple remedial actions, notifications, and reports to users, managers, and administrators.



Multi-Tenant Control

Access and control any Inspector via one centralized parent console or multiple child consoles.



Data Privacy & Security Compliance

Meet industry-specific compliance mandates by monitoring and controlling user activities exiting the enterprise, and set up workflows for different severity levels of events.



Content-Aware Reverse Firewall

DLP rules based on multiple objects to address use cases for insider threat management.



Email Alerts

Send email alerts to the sender, manager and/or security respondent concerning critical security incidents.



Rules on Destinations

Control where users can send data based on a domain or site destination.



Port and Protocol Agnostic

Inspector all outbound traffic flowing through the GTB Inspector.



Entra ID Sync

Effortlessly configure and deploy user or group-based rules while keeping user, machine, and group identities up to date.



File and Email Capture

Save a carbon copy of the file and/or email when a sender triggers a violation for further investigation.



Load Balancing

Evenly distribute incoming network traffic or workload across multiple servers, resources, or computing instances.



Logging & Audit

Ensure security, compliance, and operational integrity by monitoring and reviewing activities that occur within the network and systems.



Quarantine Emails

Log, block or quarantine emails containing sensitive data triggers and delete or release them based upon data severity.



Flexible Deployment Options

The Inspector can be deployed inline, as a virtual machine (VM), as a SaaS offering, or cloud premises, depending on the enterprise architecture.

Endpoint Protection For MacOS, Windows, and Linux

Network Inspection/DeviceControl/LocalDiscovery/Printer/Applications/Copy Controls
File Classification/Fileshare/USB/Harddrives/Optical Drives



Network Inspection

Monitor and analyze network traffic to prevent unauthorized transmission of sensitive or confidential data outside the organization's network perimeter.



Device Control

Prevention of unauthorized device connections to mitigate data breaches and malware threats. Inspect the files being transferred to a USB.



Local Discovery

Scan, identify, and apply appropriate security measures to secure sensitive data on laptops, workstations, VDIs and other devices within an organization's network by scanning and applying appropriate security measures.



Optical Character Recognition (OCR)

Extract text and data from images, scanned documents, and non-text files. Analyze OCR results for sensitive information identification. Integrates with DLP and data classification systems for comprehensive data protection.



Printer DLP

Ensure sensitive data security by preventing unauthorized printing, access, leakage, or exposure through printed materials to maintain confidentiality, integrity, and compliance.



Application Controls

Prevent unauthorized software usage by enforcing policies to restrict applications and executables, and analyze application behavior for security risks.



User Justification

Sending a confidential file can be justified by providing users with an optional remedial action, enhancing investigational needs and user accountability.



Copy Controls

Clipboard actions and content aware inspection of sensitive data to educate the users on data handling.



Fileshare Auditor

Monitoring and auditing user activities on file shares for security and compliance. Tracking file access, modification, and transfer events. Real-time alerts and reporting on suspicious file activities for proactive response.



File Classification

Automatic file classification containing sensitive data, tagging and labeling for visibility, and policy-based enforcement for data handling and company policies.



USB Encryption

Encrypt data on USB drives for security, preventing unauthorized access or theft of sensitive information during storage or transport.



Entra ID Sync

Effortlessly configure and deploy user or group-based rules while keeping user, machine, and group identities up to date.



GTB Technologies®
Data Security that Works®

GTB Technologies Inc.

Enterprise Data Security Suite

Features Overview

Endpoint Protection		Content-Aware Reverse Firewall	
Data Loss Prevention		Flexible Deployment Options	
Fingerprint Detection		Multi-Threaded Technology	
File Classification		Email Classification	
Optical Character Recognition		Incremental Scanning	
Device Control		Manual labeling	
File Audit		Automatic labeling	
Generative AI		Enterprise Workflow	
Application Control		Simple Installation	
Centralized Management		Role-Based Controls	
Entra ID Sync		SaaS Email DLP	
Advanced Audit		AI protection	
Insider Risk Management		Communication Compliance	

SCHEDULE A DEMO



**Contact Us for more information Email: info@gttb.com - Call: +1 800 626.0557
visit our website www.gttb.com**