GTB Technologies
Data Security that Works™

Endpoint Protector

Control, Protect, Discover, Classify, Audit.

Identify and protect the full range of file types and data streams

- ✔ Identify data on all storage formats
- ✔ Enable the redacting of images containing high priority sensitive data

Control the Endpoint

Keeping a handle on the mountain of business data a company interacts with is no easy task. The responsibilities of protection, detection and classification all require significant investments in network tools and manpower. In today's business environment, the challenge of data loss prevention is only exponentialized by the growth of data endpoints on the network periphery.The mobile work-force and the ever-growing number of portable devices outside the company's firewall have created a tough environment for enterprises wanting to protect their data from leak and theft.

The Data Protection solutions of GTB identify sensitive client and company information in the full range of data types including text, graphs and even image files.

What is GTB Endpoint Protector?

A content aware reverse firewall at the endpoint
The GTB Endpoint Protector client monitors 1/0 activity, enforcing policies created in the management console. All data is intercepted and inspected by GTBs'intelligent engines. Various enforcement actions can then be taken, such as blocking, alerting, classify, watermark, encryption, etc.

GTB's Application and Device Control solution is an effective way to stop complex threats, protect sensitive data from ex-filtration and identify unauthorized applications.GTB's Application Control Firewall easily shows which applications are being used by trusted & untrusted insiders.

GTB's Endpoint Classification provides an overarching data classification tool that spans every level of an organizations digital infrastructure, down to the individual user endpoint. Accurate Data Discovery at the Endpoint gives dynamic organizations the ability to diversify their operative tools and tactics while achieving the highest standard of data protection for all their data assets.

Highlighted features:

- Provides complete access control addressing all removable media Manages detailed file auditing
- Offers on line, wireless and offline protection modes
- OFF _LINE DETECTION with Off-Premises Fingerprint detection, no network connection required, No other solution can!
- Only solution supporting accurate partial file match on unstructured 'fingerprint' data!!
- Retail POS system data control
- Drip DLP, OCR, Watermark
- Monitor and Control the transfer of files-based usage including number of files, file size.
- Monitor user behavior using proprietary advanced threat detection techniques.
- Prevent the sharing of data to unauthorized devices or users.
- Understand, Control, Inventory and Report on files are being copied to USB devices.
- The system makes comprehensive enterprise reporting possible on file-owners, locations, file types. Template policies included.
- Feather lite agent
- Deployed and managed by the GTB Central Console, an enterprise data security command center.
- Shares management extensions and policies with all of GTBs Data Protection facets.
- Performs data classification automatically, based on file content.
- Centrally manages data security policies and controls across unstructured, semi-structured and structured repositories.
- Compatible with all Window systems for PC's and Servers.
- Multi-threading technology that can achieve scan speeds of 1 Gigabyte per minute.
- Integrates with GTB Enterprise DRM for File level access controls.
- Scans images with the ability to redact sensitive data via OCR.
- Highly rated by Forrester,Gartner, IDC, and other research firms.

Classification, Analysis and Remediation

- Control sensitive data with customized classification values.
- Send alerts when data is saved or moved in contradiction of policies.
- User Based / Automatic
- Classification Classify emails
- Classify files
- Index & mine data/ data sets.
- Move, Copy, Delete, Redact or apply Enterprise DRM to sensitive data.
- Generate digital signatures to protect documents when in transit to the Internet or to USB devices and Printers. User Based /
- Automatic Classification
- Watermark- automatically

Endpoint Protection & Oversight

- Configurable risk dashboards simultaneously showing different reports from discovery, network and endpoint
- Single user interface for all network incidents occurring on the endpoint, as well as for systems management
- Discovery of confidential data on endpoint devices, including reporting on Access Control Lists (ACLs) for files that violate policy