opentext™

Product overview

OpenText Hightail security features

Files stored and shared with Hightail are secured, controlled and managed at the user, enterprise and cloud levels

Controls, including passwords and permissions, **help protect sensitive files**

IT teams can set global controls and configure rules for enterprise data sharing

Security and access controls to data centers are consistent with the highest industry standards

Information is potentially placed at risk every time digital files are shared. Whether a company's employees use email or look to bypass its limitations with unsanctioned file sharing and collaboration tools, the inadequate security and compliance standards of these methods cause a serious risk.

OpenText™ Hightail™ solves this problem with an enterprise-grade service that lets users easily collaborate on shared files, while providing IT staff with the required security infrastructure, comprehensive controls and data tracking capabilities.

User-level security

Enterprise users need to collaborate with other users within and outside the organization without security concerns hampering their productivity. Hightail's robust security infrastructure and advanced, simple security controls allow users to work productively without hassle.

Email limits the amount of control users and IT can exercise over shared data. When collaborating in Hightail, users can protect information with access codes and specify permissions at a granular level, for example, allowing certain users "view only" access or giving others the ability to modify content.

The security features on Hightail are available across the web, desktop and mobile apps, providing a familiar experience no matter which device is being used. Enterprises can leverage existing single sign-on (SSO) infrastructure, so users don't need to remember another username and password or add another layer of security with two-factor authentication. Hightail mobile products leverage device/operating system-dependent security measures, such as PIN protection, encrypted local storage and data wipe, which can prevent unauthorized access should a device fall into the wrong hands. These user-level features allow businesses to strike the appropriate balance between productivity and IT control with minimal maintenance overhead.

Enterprise-level security

Hightail integrates seamlessly with existing infrastructure and applications while providing IT with granular control capabilities. Enterprises can quickly get started using Active Directory/LDAP via SAML 2.0 integration to enable SSO, while SAML provisioning support automates user account set up. Alternatively, IT can enable two-factor authentication enterprise-wide and even set a required implementation date for all users across the organization. In managing accounts, Hightail provides administrative flexibility by allowing IT admins to set global controls.

The Admin Console allows account administrators to create date-based reports for all account and user activity, which helps limit exposure and provides an audit log for reporting. The console also provides at-a-glance monitoring of the most recent activity.

Cloud-level security

Hightail is trusted by millions of professionals for user and IT-level controls and rigorous security measures. Reliable and resilient architecture ensures Hightail services are always available to users. Data is secured at all layers, including network and application levels, to ensure end-to-end security for corporate information.

Physical security

Hightail uses data centers that maintain stringent physical security measures and certifications and offer physical controls to mitigate environmental risks. Hightail continuously monitors all operational systems 24x7x365.

Network security

Hightail provides multiple solutions to address network security threats as information flows back and forth from data centers to customer and third-party systems. Hightail monitors its entire network, including the production application and underlying infrastructure components at all times. Realtime alerts are sent to the on-call operations staff members for resolution and all incoming and outgoing traffic between the production environment and other networks—corporate and untrusted—is monitored by ISP-grade firewalls.

To protect the systems from DoS/DDoS (denial of service) attacks and ensure availability, Hightail employs carrier-grade network equipment and redundant internet links. To ensure the reliability of the network infrastructure against increasingly sophisticated hacking methods, Hightail performs weekly vulnerability scans and engages third-party security firms to perform penetration and application vulnerability testing.

Application security

The Hightail application is designed with security as a key consideration at every stage. The web application is multi-tiered into logical segments (front-end, mid-tier and database). This guarantees maximum protection while giving developers the flexibility of a multi-layer architecture.

The Hightail application development goes through multiple checks and balances to ensure that development or testing processes do not impact the production systems and data. These checks include putting every change through a formal release engineering process, maintaining physically and logically separated development environments and performing full functional testing of all changes in a QA environment before deployment to production. Following this rigorous development and release process allows Hightail to deliver new features and improvements while maintaining a solid and secure foundation.

Data security

Other sharing and collaboration tools lack data encryption, allowing hackers to sniff packets out of the network and directly intercept the data. Hightail encrypts data in transit by providing up to 256-bit AES encryption along with support for forward secrecy, ensuring that deciphering intercepted information is impossible now and in the future. 256-bit AES encryption and dynamic key management ensure every access is logged, providing full auditing. Hightail also uses redundant encrypted storage, meaning that copies of every file are stored on multiple servers to safeguard against data loss.

Compliance

Hightail's end-to-end security features meet stringent compliance requirements and allow organizations to meet a number of industry regulations as they extend their IT infrastructure into the cloud. Hightail obtains a third-party audit to attest to its compliance with SSAE 16 security and confidentiality principles and confirm the design and effectiveness of its controls.

Hightail complies with the EU-US Privacy Shield framework so that it maintains proper collection, use and retention of personal information. Hightail's security features also enable organizations to meet a variety of industry regulations, such as the Gramm-Leach-Bliley Act (GLBA).

Enterprise-grade security, now and in the future

Collaboration solutions can increase productivity but make business information vulnerable through unsanctioned applications and uncontrolled communication tools, such as email. Hightail provides a solution that satisfies IT requirements, not just in terms of robust security and granular control over enterprise data, but by providing an intuitive collaboration experience that results in quick and easy user adoption.

Hightail recognizes that the challenge of maintaining security is ongoing and continually evaluates its security infrastructure to anticipate potential new dangers.

Feature	Description
User-level security offerings	Space permissions [view/modify], access code protection, verify recipient identity and download tracking
Enterprise-level security offerings	SAML 2.0 integration and provisioning and usage reports [audit log]
Network security offerings	24x7x365 monitoring, ISP-grade firewalls, DoS/DDoS protection, vulnerability scanning and penetration testing
Application security offerings	Multi-tiered DMZ configuration, formal release engineering process and full-functional QA testing
Data security offerings	Redundant encrypted copies, 256-bit AES encryption and dynamic key management

opentext™

- Join the conversation
- Keep up to date
- Learn more

OpenText Hightail components

Secure file sharing	• Share files in any format (up to 500GB) and control access to content with password protection, permission settings and expiration dates • Comply with SSAE 16 standards, enabling organizations to meet industry regulations; 256-bit data encryption
Unlimited storage	• Get unlimited content storage
Organization and archiving	• Organize work into projects, workspaces and file groups for teams and archive completed files
Visual file previews	• Gain instant access to high-resolution previews for images and streams for video files
Precise feedback	• Collect feedback from multiple reviewers with in-line comments on images and timestamped feedback on videos and audio, all in one place
Realtime conversations and notifications	• See all comments in context as they occur and receive realtime email notifications for project updates
Guest access	• Allow external collaborators to view, comment and download content without requiring log in credentials
Version control	• Work off the latest file and access archived versions and comments in the visual version carousel
Set tasks and follow-ups	• Set targeted @mention notifications and flag key tasks with due dates
Manage approvals	• Use one-click approvals, routing and requests system
Activity and team dashboards	• Monitor team activity and outstanding to-dos in one place
Discussion boards	• Kickoff a new brief, provide project-level updates or discuss a new direction on Space level discussion boards
SAML and Active Directory	• Gain easy access through single sign-on and integration with an existing directory service
Two-factor authentication	• Add another layer of security to accounts by requiring two forms of user identification
Priority support	• Access a dedicated support line for help when required

opentext.com/contact Twitter | LinkedIn

Copyright © 2019 Open Text. All Rights Reserved. Trademarks owned by Open Text.
For more information, visit: https://www.opentext.com/about/copyright-information (11/2019)13876EN