EXECUTIVE SUMMARY

Maintaining the security of confidential business information is a top priority for all companies. When trusting that crucial data with a third party Software as a Service (SaaS) provider, it's important to ensure they match and exceed your requirements.

When scrutinizing the security capabilities of a SaaS provider, the best way to start is to know the questions you need to ask and what to look for in their answers. This whitepaper is a guide to understanding and exploring the multiple security layers of cloud-based sharing service, including:

• What to look for in an information security program
• The importance of application architecture for a secure environment
• How to think about data security
• Correctly assessing systems and network security
• Key areas to focus when determining data center security

In each section, we use Hightail’s own security architecture, controls, and practices to illustrate and explain the different components of cloud application and data center security.

While your IT department may already have standard procedures when it comes to enforcing security policies and evaluating vendors, by focusing on the most important aspects of what a secure sharing service looks like, you can get a step ahead and streamline your selection process.
## Table of Contents

### I. Information Security Program
1. What is your Incident Response Plan?
2. What are your staff's qualifications?
3. What is your InfoSec organizational structure?
4. Describe your InfoSec policies.
5. What is your privacy policy?
6. Do your employees acknowledge policies or sign confidentiality agreements?
7. What is your change control process?
8. What certifications or 3rd party attestations do you have?
9. Do you have a Disaster Recovery Plan?
10. What are your notification procedures?

### II. Application Architecture and Security
1. Describe your application's architecture and different tiers.
2. Describe your coding practices.
3. How do you test your application?
4. Do you perform web application vulnerability testing?

### III. Data Security
1. How do you protect user authentication information?
2. How are User Files stored? What level of encryption?
3. Is the system multi-tenant?
4. How is account information stored?
5. Are User Files accessed by the vendor?
6. Who has access to User Files?
7. When are files deleted?
8. How is disk media destroyed when decommissioned?
9. How is data transferred (both account information and User Files)?
10. Is data backed up or copied?

### IV. System & Network Security
1. Who has access to productions systems?
2. How do personnel authenticate? How do you manage accounts?
3. How are password policies enforced?
4. Is access to the system logged?
5. How often do you patch production systems?
6. What are the standard builds based on?
7. How is your production network segmented from your corporate, QA and development environments?
8. Do you perform vulnerability scans and penetration testing?
9. What type of firewalls do you use?
10. How are system/network monitoring, logging and alerting setup?

### V. Data Center Security
1. What are the physical access requirements for the data center?
2. How is the data center access list maintained and controlled?
3. Who has access to the data center?
4. Is data center physically monitored (cameras, guards, etc.)?
5. Where are data centers located?
6. What redundancy and availability does the data center provide?
7. What type of certification does the data center have?

### VI. Conclusion: Security Assessment for Cloud-Based Providers

### VII. Relevant Links
# I. Information Security Program

An Information Security Program, also referred to as Information Security Governance, dictates how a company sees information security, how it prepares for and how it ensures that security practices are enforced. To understand how one company’s InfoSec Program differs from another, consider the following:

- Does it look like information security is considered an enterprise-wide issue?
- Are company executives accountable for security?
- Is information security in the company viewed as a business requirement or an inconvenience?
- Does the company show a good understanding of different types of risks?
- Are roles, responsibilities, and segregation of duties clearly defined?
- Are adequate resources committed to information security?
- Is the company’s staff aware and trained on info security policies and procedures?
- Are there stringent requirements when it comes to the company’s development processes?
- Are security policies as well as the infrastructure reviewed and audited on a regular basis?

To gain a better understanding of a cloud provider’s information security program, here are some questions you should ask and what to look for in their answers.

1. What is your Incident Response Plan?
2. What are your staff’s qualifications?
3. What is your InfoSec organizational structure?
4. Describe your InfoSec policies.
5. What is your privacy policy?
6. Do your employees acknowledge policies or sign confidentiality agreements?
7. What is your change control process?
8. What certifications/3rd party attestations do you have?
9. Do you have a Disaster Recovery Plan?
10. What are your notification procedures?

1. **WHAT IS YOUR INCIDENT RESPONSE PLAN?**

**What it means:** An incident response plan is a key document that helps guarantee that the company will survive any glitch, emergency, or disaster that come in its way.

**What to look for:** At Hightail, our Incident Response Plan is available on our company intranet for all employees to see. It details the Security Incident Response Team (SIRT), which is comprised of Members and Contingent Members from various groups within the company and contains information about the potential risks and what actions should be taken if faced with such risks.

A good incident response plan, like the one Hightail has, spells out what to expect in case of a disaster (i.e. data breach, hack attempts, natural disasters, etc.), who is part of the team that will take the lead in countering such threat, how the team members will communicate with each other and with the company, a clear list of roles and responsibilities for each team member, and should also indicate how often the plan will be revised and updated.

2. **WHAT ARE YOUR STAFF’S QUALIFICATIONS?**

**What it means:** Simply having a security policy in place doesn’t make a solution secure. You want to make sure that key employees are qualified to respond to security incidents and to carry out the incident response plan.

**What to look for:** Look for companies that, like Hightail, take security seriously by providing corporate security awareness training to all employees and more specific security training to employees in the Engineering and Operations groups. After all, these are the employees who most likely will be called upon when a security threat is identified. Also, not all companies have the habit of doing background checks, but at Hightail we believe that you should...
perform full background checks on employees prior to granting them access to financial or customer data.

3. WHAT IS YOUR INFOSEC ORGANIZATIONAL STRUCTURE?
What it means: You want to ask the cloud provider about the organizational structure of their information security team. It doesn’t need to be a formal org chart but you should ask about roles and responsibilities within the organization and understand who reports to whom when it comes to information security.

What to look for: Beware of information security organizational charts that depict IT or the IT manager as the main security person of the company, or security teams reporting to someone in the IT department. Here’s what Hightail’s information security organization looks like:

As you can see, Hightail’s InfoSec org chart has the Security & Risk Management Team reporting directly to the Senior Manager of Security and Risk Management who, in turn, reports to the VP of Operations. This ensures that there is one person (the Sr. Manager of Security and Risk Mgmt.) responsible for overseeing all security practices, policies, and guidelines and that this person is not reporting directly to an IT manager. This separation is important because security usually has two sides: the infrastructure component and the information component.

By removing the Security Manager from under IT we guarantee independence and unbiased operation when it comes to securing our environment. The VP of Operations is the top-level executive in charge of security and reports directly to the CEO.

4. DESCRIBE YOUR INFOSEC POLICIES
What it means: Is there a process for reviewing, updating, communicating your information security policies?

What to look for: Having an information security policy that is never reviewed will not be of much help two years down the road when new technology, infrastructure modifications, and other factors haven’t been incorporated into the policy. The robust Information Security Program Hightail has put in place includes an annual review of the Information Security Policy and requires immediate updates when there is a change in the security environment (i.e. infrastructure or controls). Not only the security policy is available on the intranet for all employees, changes to the security policy are communicated immediately to all company employees.

5. WHAT IS YOUR PRIVACY POLICY?
What it means: Understanding how the cloud provider collects, uses, and shares information about your company is an important aspect to consider when evaluating solution providers.

What to look for: Clear, comprehensive, easily accessible privacy policy that is updated regularly and complies with national as well as local regulations. Please see Hightail’s privacy policy online as an example. For questions about this privacy policy or more details concerning how your information is gathered and used, feel free to contact our privacy group at privacy@hightail.com.

6. DO YOUR EMPLOYEES ACKNOWLEDGE POLICIES OR SIGN CONFIDENTIALITY AGREEMENTS?
What it means: Acknowledgement of security policies is a process in which employees have to sign
a document stating they are aware of the company’s security policies. Confidentiality agreements protect not only the company but also the company’s customers from having its confidential or trade secret information disclosed without the company’s consent. A strong information security program will contain guidelines related to confidential information and how the policy is enforced.

What to look for: As you ask vendors about their security policies, don’t forget to inquire about how employees are made aware of it and whether there is a process for ensuring employees sign off on such policies. At Hightail, for example, every new employee signs a document stating they have received and are aware of the company’s security policy. In addition to that, every time the security policy is updated, employees have to re-acknowledge the information security policy stating they are aware of the changes made. The process of asking employees to acknowledge the security policy helps keep all employees aware of the policy and further enforces a culture where information security is paramount.

As for confidentiality agreements, although in many companies this is standard practice (at Hightail all new hires are required to sign a confidentiality agreement), you should confirm with the vendor that this is indeed part of their hiring practices.

7. WHAT IS YOUR CHANGE CONTROL PROCESS?
What it means: A change control or change management process is a set of procedures put in place to ensure that changes to the IT infrastructure (software and hardware) are handled in a way to minimize potential impact to production systems.

What to look for: Companies should have a formal, documented process for handling changes. As an example, at Hightail the process for handling changes to systems and supporting infrastructure is part of Hightail’s Change Management policy. The procedures related to change management are formally documented and are available to company’s personnel to promote adherence to standard Change Management processes.

Also, it might be useful to ask the vendor how they track change requests, and how they manage the implementation and closing of such requests. There are many software applications available to handle change management, like Hightail’s intranet-based project management application for tracking of change management processes and documentation. This application helps track change details, responsibilities, and status of change requests and is Hightail’s primary Change Management system, used to facilitate change requests for both Hightail’s application and to supporting systems and infrastructure.

8. WHAT CERTIFICATIONS OR THIRD-PARTY ATTESTATIONS DO YOU HAVE?
What it means: Certifications are a good way to get a third-party validation that the vendor you are talking to has security as top-of-mind.

What to look for: Although many certifications are now standard when it comes to cloud-based application providers, you should verify that the vendor is indeed certified. A good starting point is Hightail’s own list of certifications, which include a Service Organization Control (SOC) 2 Type 2 attestation, TRUSTe certification, US-EU Safe Harbor compliance, and PCI compliance.

But what do they mean? Here’s a brief explanation:

SOC Report: It stands for Service Organization Control and reports on an organization’s internal controls. You will see companies talking about SOC 1 and SOC 2 reports, which can be confusing. SOC 1 is a report that conforms to what is called an SSAE 16 audit and the main scope is the certification of internal controls over financial reporting. The SOC 2 report was formerly called SAS 70 and was created with data centers and SaaS (Software as a Service) providers in mind and so it includes a comprehensive set of criteria (known as Trust Services Principles, or TSP) that verify and certify the security of a service organization’s systems, the availability of the company’s systems, the processing integrity of such systems, the confidentiality that the organization’s systems
processes or maintains for user entities, and the privacy of personal information that the organization collects, uses, retains, discloses, and disposes of for user entities.

For SOC 2 there are two types of reports, called Type 1 and Type 2. A Type 1 report speaks about the adequacy of the vendor’s controls while the Type 2 report certifies not only the adequacy but also the efficacy of such controls.

**TRUSTe**: TRUSTe is a leading online privacy solution provider that many eCommerce sites rely on. If a company has the TRUSTe logo on their site it means their privacy policies went through great scrutiny to ensure they meet and maintain a high standard of privacy protection.

Companies using TRUSTe must adhere to certain privacy principles and comply with their verification and consumer resolution process. As an example, Hightail being a member of TRUSTe not only agrees to post our privacy policy online in an easily accessible way but also strive to adopt and implement privacy principles that reflect fair privacy practices.

**US-EU Safe Harbor**: As data protection and privacy policies differ between the United States and the European Union, the US-EU Safe Harbor Framework was created to ensure that US-based companies could certify to the European Union that their organizations provide adequate privacy protection conforming to EU regulations.

**PCI**: PCI Compliance refers to the Payment Card Industry Data Security Standard (PCI DSS), which is a set of requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. If your cloud provider requires credit card payments, then it is a good idea to ensure they are PCI compliant.

9. **DO YOU HAVE A DISASTER RECOVERY PLAN?**

**What it means**: A Disaster Recovery Plan documents the actions to be taken in case of a disaster so that the IT infrastructure can quickly recover and support business functions.

**What to look for**: Ask the vendor if they have documented Disaster Recovery Plan. Hightail’s own Disaster Recovery Plan includes the use of highly redundant and fault tolerant systems to maintain maximum uptime and additional plans are in place to recover from various disaster scenarios.

10. **WHAT ARE YOUR NOTIFICATION PROCEDURES?**

**What it means**: Many states have security breach notification laws but you should ensure the cloud provider has clear policies and procedures for notifying customers in case of a data breach and in case where systems are down.

**What to look for**: At Hightail affected customers are notified by the Hightail customer support team as appropriate. All Hightail customers are able to get a real time update on the application status by visiting our support site. Additionally, users can subscribe to receive real time updates proactively by clicking on the “Subscribe” button located on the above page. To do this, users simply create an account on the Hightail support site. Upon doing this, users will be notified through email of any changes to the status of the Hightail service. Through this same mechanism, users can also be made aware of any planned maintenance windows allowing them to get the most out of the Hightail service with minimal disruption to their business processes.
II. Application Architecture and Security

All security policies are useless unless the application’s architecture was built with security in mind. It is pointless to train employees and put physical controls in place if the software in question can be easily exploited due to poor design or lack of appropriate security related coding practices.

As you look at different cloud content collaboration solutions, here are some key questions to ask about their application architecture and security:

1. Describe your application’s architecture & different tiers.
2. Describe your coding practices.
3. How do you test your application?
4. Do you perform web application vulnerability testing?

1. DESCRIBE YOUR APPLICATION’S ARCHITECTURE AND DIFFERENT TIERS

What it means: Software applications developed based on best-practices have multiple “layers” that separate the presentation, application processing, and data management functions in a logical way. This not only helps developers make changes to one layer without affecting the whole system, but it also helps when it comes to building secure applications.

What to look for: The Hightail web application is multi-tiered into logical segments (front-end, mid-tier and database), each independently firewallled from each other in a DMZ configuration. This guarantees maximum protection while giving developers the flexibility of a multi-layer architecture. Look for solutions that have been architected with this configuration in mind.

2. DESCRIBE YOUR CODING PRACTICES

What it means: According to the Software Engineering Institute at Carnegie Mellon, “easily avoided software defects are a primary cause of commonly exploited software vulnerabilities”. Such vulnerabilities are created by software ‘bugs’ in most part due to poor software development practices. Part of a thorough security evaluation includes inquiring about the vendor’s coding practices.

What to look for: At Hightail, we leverage industry standard programming techniques such as having a documented development and quality assurance processes and also following guidelines such as the OWASP ESAPI library, to ensure that the applications meet security standards. In addition to that, all our code is peer reviewed prior to being released to QA, which minimizes the number of bugs that have to be sent back to the developer for fixing.

3. HOW DO YOU TEST YOUR APPLICATION?

What it means: Part of secure coding practices include a thorough Quality Assurance (QA) process that involves testing changes made to the application prior to making it available in production systems.

What to look for: Ask the vendor if they have a formal Quality Assurance program. At Hightail, all application changes undergo both automated and manual testing including full functional testing in a QA environment and full performance testing in a staging environment before full deployment to production. The Quality Assurance Team also deploys to half of the production system and performs a full regression testing before full production deployment is carried out. This thorough testing process ensures that if anything fails during any step, the production system is not compromised.
4. DO YOU PERFORM WEB APPLICATION VULNERABILITY TESTING?

**What it means:** Web based applications should be routinely tested for security vulnerabilities. As web servers get upgraded, patches are applied, or changes are made to the application, it is important to look for ways in which security could be compromised and fix any loopholes.

**What to look for:** Vendors should have the habit of performing security reviews in their web applications, even in their own the data centers. At Hightail, web application security is evaluated bi-weekly by the Security & Risk Management team in sync with the application release cycle.

This vulnerability testing includes the use of commonly known web application security toolkits and scanners to identify application vulnerabilities before they are released into production. Hightail also leverages external 3rd parties for periodic vulnerability assessments and penetration testing, which ensures our environment is secure and web transactions can occur without risks.
III. Data Security

Data Security relates to the methods in which data stored and transferred to/from the application is secured. The ability to protect customer data while in transit or at rest is a key element for a secure SaaS application and something that should be well understood.

Although data security is a lengthy topic worthy of many books, we provide you with the following questions that will give you a good understanding of how secure (or not) your data might be with the cloud provider:

1. How do you protect user authentication information?
2. How are User Files stored? What level of encryption?
3. Is the system multi-tenant?
4. How is account information stored?
5. Are User Files accessed by the vendor?
6. Who has access to User Files?
7. When are files deleted?
8. How is disk media destroyed when decommissioned?
9. How is data transferred (account info & User Files)?
10. Is data backed up or copied?
11. Is customer data (account info or User Files) ever on removable media?
12. Is customer data (account info or User Files) ever on desktops or laptops?

1. HOW DO YOU PROTECT USER AUTHENTICATION INFORMATION?

What it means: User authentication means the ability to validate a user’s identity prior to granting access to the system. Typically user authentication is followed by user authorization, which means giving the user access only to the areas, files, or features the user is authorized to have. Protecting user authentication information means having a secure way to store data that can be used to validate a user such as usernames, passwords, and other identifying information used by the application.

What to look for: The most secure applications don’t store user passwords in the same server where the application resides. At Hightail not only passwords are stored in a secure location separately from the application, all user passwords are protected with cryptographic hash algorithms.

2. HOW ARE USER FILES STORED? WHAT LEVEL OF ENCRYPTION?

What it means: Using a secure data center or hosting provider is of no value if customer files are easy to identify and read. Cloud-based providers that take security seriously should offer some kind of encryption for the data they store.

What to look for: The most secure providers will give you some form of encryption for the data they store, which is called “encryption at rest”. At Hightail, data at rest is stored using 256-bit AES encryption (AES is the encryption algorithm adopted by the US Government and the 256-bit key is the highest form of security that can be used with this algorithm) and in addition all customer files are stored within file systems on dedicated systems called FTFs (short for “File Transfer Fabric”). File names are replaced with random strings so that no file is identifiable by name.

3. IS THE SYSTEM MULTI-TENANT?

What it means: With the advent of cloud computing, it became important to have a way to separate data from multiple customers accessing the same application. While the application is the same for all customers, their data has to be segregated in the back-end. The ability to serve multiple customers with the same application is therefore called as “multi-tenant”
and it means that in the application’s database each customer (aka tenant) data is kept separate.

What to look for: Although multi-tenancy is becoming the standard when it comes to cloud computing, you should ask the vendor if they follow this type of database architecture that ensures data for each ‘tenant’ (i.e. customer) is kept separate. As an example, Hightail uses a true multi-tenant architecture meaning there are no specific resources assigned to any specific customers. We have multi layered and multi-tier security provisioning segregating customer data even with the same organization.

4. HOW IS ACCOUNT INFORMATION STORED?
What it means: Account info be considered sensitive data and protected accordingly to prevent identify theft.
What to look for: Ensure that the vendor treats account information seriously and find one that, like Hightail, stores it in a secure, redundant, highly available database system with access restricted to authorized members of the Operations Group.

5. ARE USER FILES ACCESSED BY THE VENDOR?
What it means: All the security controls in place will not do you any good if the vendor has access to your files and can read your confidential data.
What to look for: You want a vendor that cannot view your data, in any circumstance. For example, although Hightail cooperates with government and law enforcement officials and private parties to enforce and comply with the law, its employees or representatives may access, but not view the contents, of User Files when complying with a legal obligation, such as responding to a search warrant. For more details about how Hightail handles customer confidential information, check out our Privacy Policy online.

6. WHO HAS ACCESS TO USER FILES?
What it means: The more people inside the vendor’s organization with access to User Files, the greater the potential for data breach. Good vendor security policies will limit who can access user files and in which circumstances.
What to look for: Make certain only people from a small group, especially related to security or operations, can have access to user files. At Hightail, only authorized members of the Operations group have access to systems that host customer data.

7. WHEN ARE FILES DELETED?
What it means: Deleted files by the user are typically held in the cloud-based system for a number of days prior to being actually deleted to help recovery efforts in case of accidental deletion.
What to look for: Although it is typical for user-deleted files to be held in the server prior to being purged, look for policies like the one at Hightail where files are deleted from all disks no more than 7 days after expiration or active deletion by the user.

8. HOW IS DISK MEDIA DESTROYED WHEN DECOMMISSIONED?
What it means: As with any hardware part, hard drives get old and have to be replaced. But the risk with disk media is that you can’t simply throw them in the garbage bin otherwise people might still be able to pull out confidential data that was stored there.
What to look for: There are many secure ways of handling the replacement of storage devices. At Hightail, disks removed from production systems are destroyed onsite and disposed of by a 3rd party vendor. Make sure the vendor you are talking to follows a similar procedure.

9. HOW IS DATA TRANSFERRED (ACCOUNT INFORMATION AND USER FILES)?
What it means: Data transferred over the internet is typically in what it’s called "plaintext", meaning there is no encryption or any security that makes it more difficult to read messages sent from one computer to another. Data transferred over the internet without any type of protection can be victim of Packet Sniffing, which is the act of intercepting communication on the internet using either a hardware or software “sniffer” to read the data being transferred between two computers.
What to look for: Any vendor operating a cloud application should offer some type of encryption for data transfers. Look at how Hightail handles data transfers for an example: At Hightail, data transferred between client and server over the untrusted Internet is 128-bit SSL/TLS encrypted (at minimum). If supported and enforced by the client browser, data is then encrypted via 256-bit SSL/TLS. Note that some vendors claim their encryption at transfer is 256-bits at all times but beware that this is only possible if the client browser supports it.

10. IS DATA BACKED UP OR COPIED?

What it means: Security to your files on a cloud server also means having access to them if disaster strikes. Backup policies and procedures are a key aspect of ensuring continued service.

What to look for: Ask about backup policies and where files are stored. At Hightail, all files that are uploaded to our storage platform are copied to a second storage node for redundancy and availability. User Files are not backed up outside of the storage fabric and all copies are removed upon expiration or deletion by the user.

11. IS CUSTOMER DATA (ACCOUNT INFO OR USER FILES) EVER ON REMOVABLE MEDIA?

What it means: Storing customer data on removable media adds another potential risk for data theft.

What to look for: As you look into the vendor’s storage and backup procedures, make sure that no customer data is ever stored on removable media. Hightail does not allow the storage of any customer data on removable storage media at any time.

12. IS CUSTOMER DATA EVER ON DESKTOPS OR LAPTOPS?

What it means: Despite the rise of the mobile workforce and of companies allowing employees to work from remote sites, if customer data like account information or user files are at any time stored in laptops, the potential for a security breach is increased. Also, storing customer data in desktops, even at the vendor’s offices, is another practice that should be avoided.

What to look for: The simple answer is to use Hightail as an example, where no customer data is ever stored on desktops or laptops.
IV. System & Network Security

System and Network security policies and controls constitute the backbone of any security installation and are of utmost importance. By understanding what are the key elements of system and network security you will be better prepared for analyzing different vendors and understanding their particular strengths.

Let’s narrow down the questions you should ask cloud vendors about system and network security into the following:

1. Who has access to production systems?
2. How do personnel authenticate? How do you manage accounts?
3. How are password policies enforced?
4. Is access to the system logged?
5. How often do you patch production systems?
6. What are the standard builds based on?
7. How is your production network segmented from your corporate, QA and development environments?
8. Do you perform vulnerability scans & penetration testing?
9. What type of firewalls do you use?
10. How are system/network monitoring, logging and alerting setup?

1. WHO HAS ACCESS TO PRODUCTION SYSTEMS?

What it means: Production systems are at the heart of the solutions provider operations and represent the physical servers that run the application and store user data. Gaining physical access to the production system is a serious security matter.

What to look for: At Hightail, only authorized members of the Operations Group have access to production systems. This means that no other employee, contractor, or anyone outside this restricted group can walk into the place where the production systems reside. When asking about access to production systems, look for policies indicating a small group of trusted individuals that must follow strict protocol when accessing the systems.

2. HOW DO PERSONNEL AUTHENTICATE? HOW DO YOU MANAGE ACCOUNTS?

What it means: User authentication is one of the potential “weak links” in a security configuration since if the authentication method or process can be fooled the intruder will be able to access the system and data.

Ensuring a secure authentication procedure together with strong account management is imperative to providing a secure cloud-hosting environment.

What to look for: Among the many configurations out there, you can use Hightail as a good guideline. For example, all production systems at Hightail are accessed through bastion hosts and remote access to the bastion hosts requires multi-factor token-based VPN access.

Beware of vendors who do not make use of bastion hosts or token-based VPN access to their systems.

3. HOW ARE PASSWORD POLICIES ENFORCED?

What it means: Good password policies will require users to login using a strong password and will have strict settings related to password expiration and password length.

What to look for: Requiring users to create yet another password to access a cloud based content collaboration solution might leave you open to unnecessary risks and present another layer of complexity to the use of the application. Instead, look for systems like Hightail that rely on password policies enforced by central authentication directories like LDAP or Microsoft Active Directory.
This minimizes setup time, ensures the cloud content collaboration solution follows pre-established password policies, and makes it easier for users to use the system.

4. IS ACCESS TO THE SYSTEM LOGGED?
What it means: Keeping track of who accessed the system and when is a good practice that can not only avoid security breaches but can also help determine whether a breach occurred and how.

What to look for: Access to the production system should always be logged. At Hightail production system access (successes/failures) is logged locally and in a central log repository. Access to the central log repository is restricted to appropriate personnel in the Operations Group.

5. HOW OFTEN DO YOU PATCH PRODUCTION SYSTEMS?
What it means: Software vendors routinely release patches and updates to ensure security vulnerabilities are corrected, thus minimizing the chances the production system will be victim of an attack.

What to look for: Hightail follows a strict process in which standard security patches are applied within 30 days of release and critical patches are applied as appropriate to the risk. Beware of vendors who don’t have a set process for handling patches.

6. WHAT ARE THE STANDARD BUILDS BASED ON?
What it means: Standard builds help ensure that all software developers making changes to the application have their code compiled using the same parameters, thus minimizing errors and giving a more rigid, but secure, approach to new software releases.

What to look for: Ask the vendor about their software development practices and if standard builds are used. At Hightail, as an example, all systems are built based on a standard build configuration defined by the Operations team and vetted by Security & Risk Management. Changes to the standard build configuration follow the standard change management procedure.

7. HOW IS YOUR PRODUCTION NETWORK SEGMENTED FROM YOUR CORPORATE, QA AND DEVELOPMENT ENVIRONMENTS?
What it means: Having the production network isolated from corporate, QA and development environments is critical to ensuring proper security so that if one of the networks is breached, the production network will not be compromised.

What to look for: Security-conscious vendors will understand the importance of segmenting their networks. At Hightail, the production network segments are logically isolated from other Corporate, QA, and Development segments behind a firewall.

8. DO YOU PERFORM VULNERABILITY SCANS AND PENETRATION TESTING?
What it means: In order to ensure a network is secure, routine tests should be performed. Vulnerability scans look for weaknesses in the network that are usually found when the network administrator neglects to install the latest patches and software updates. Penetration tests are another method of ensuring network security by simulating an attack to the network to uncover any problems related to system configuration, hardware or software flaws, or even operational weaknesses.

What to look for: Routine infrastructure vulnerability scans and penetration testing should be required from all vendors. At Hightail vulnerability scans are performed and reviewed weekly and third parties are engaged periodically to perform both penetration and application vulnerability testing.

9. WHAT TYPE OF FIREWALLS DO YOU USE?
What it means: Firewalls maintain a network secure from outside would-be invaders but not all firewalls are created the same. The most common types of firewall are the Packet Filtering Firewall, Application/Proxy Firewall, Reverse-Proxy Firewall, and Packet Inspection Firewalls.
What to look for: Every firewall has its benefits and disadvantages, so the best firewall for a particular vendor will depend on the type of service and how the software provider’s network is configured. High-tail, for example, leverages highly recognized (industry-standard) enterprise firewalls for filtering traffic between the production environment and untrusted or other internal corporate networks.

10. HOW ARE SYSTEM/NETWORK MONITORING, LOGGING AND ALERTING SETUP?
What it means: As part of good network security procedures, monitoring the network means being constantly aware of network activity. Reviewing network log files and having an alert procedure is a critical part of keeping a network safe.

What to look for: At Hightail, the production application and underlying infrastructure components are monitored 24x7x365 by dedicated NMS (Network Management Systems). Critical alerts generated by these systems are sent to 24x7x365 on-call Operations staff members and escalated as appropriate to Operations management.
V. Data Center Security

Physical security is important to keep corporate data safe. Therefore, a data center’s physical security is paramount when dealing with a cloud-based solution provider. Not all SaaS vendors use the same data centers and not all data centers are equally secure.

With the following questions you can easily determine whether the vendor’s data center conforms to basic security standards:

1. **What are the physical access requirements for the data center?**
   - **What it means:** Gaining access to a company’s servers means the person can put his or her hands directly onto the server and thus either copy data, extract a piece of hardware, or damage it. No firewall, anti-virus, or other software protection will suffice if your server is not physically protected in the data center.
   - **What to look for:** You want to make sure that there are physical barriers to accessing the data center with strict procedures, controls, and safeguards in place. For example, physical access to Hightail’s San Jose facility requires visitor sign-in for badge assignment in the lobby, and biometric hand scans with PIN are required through three points for access to cages where production systems are racked. At our UK facility, physical access to our servers requires badged entry and access is restricted to only authorized 3rd party managed service employees that assist with the management of production systems from a “remote hands” perspective.

2. **How is the data center access list maintained and controlled?**
   - **What it means:** Access to a data center should be strictly controlled since gaining physical access to production systems is a great threat to security.
   - **What to look for:** You want strict access control and routine audits. At Hightail, access to the data center is controlled by designated person(s) within the Operations team and is routinely audited by the Security & Risk Management team.

3. **Who has access to the data center?**
   - **What it means:** Although controlling and maintaining the access list is critical, knowing who exactly has access is also important. The bigger the list, the more vulnerable the data center is.
   - **What to look for:** At Hightail, only authorized employees and data center support staff have physical access to data centers, and access is granted only to appropriate Hightail staff commensurate to their expected job duties.

4. **Is data center physically monitored (cameras, guards, etc.)?**
   - **What it means:** Secure data centers will have physical monitoring, which means that all physical access is monitored to prevent security incidents.
   - **What to look for:** At Hightail data centers, all access areas are controlled and the data center facilities are physically monitored and staffed with security around the clock, 24 hours a day, every single day of the week year round which should be mandatory for any cloud service provider.
5. WHERE ARE DATA CENTERS LOCATED?

What it means: Data center location can impact data access speeds.

What to look for: North American companies should look for vendors who use data centers in the USA while companies in Europe should look for data centers in their regions for faster data access. Hightail has two data centers, one located in San Jose, CA (USA) and the other in London, UK.

6. WHAT REDUNDANCY AND AVAILABILITY DOES THE DATA CENTER PROVIDE?

What it means: Not all data centers are created equal. Some provide only access to servers with no backup or redundancy in place while others provide additional security and redundant systems in order to keep the services available in case of power or hardware failure.

What to look for: Ask vendors what type of power redundancy and cooling systems are supplied by their data centers. Knowing which “tier” their data center is classified as can give you a good indication of how secure it is. For example, at Hightail the production systems are co-located in San Jose, CA are within a Tier IV data center that maintains multiple active power and cooling distribution paths, redundant components and fault tolerance providing 99.995% uptime availability SLA (Service Level Agreement). Systems residing in the UK are co-located within a Tier III data center that maintains multiple active power and cooling distribution paths (with one patch active at a time), redundant components and fault tolerance providing 99.982% availability SLA.

7. WHAT TYPES OF CERTIFICATIONS DOES THE DATA CENTER HAVE?

What it means: After looking at certifications from a software application perspective (as discussed earlier in section I: Information Security Program), data center certifications can help determine whether the appropriate controls and reporting mechanisms of the data center conform to industry standards.

What to look for: Although the majority of security controls are of responsibility of the application vendor, ask if the data center(s) being used has a SOC (Service Organization Controls) report or ISO certification. At Hightail, the data center located in San Jose, CA maintains a current SOC 1 report and the UK facility is covered under an ISO 27001 certification, which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System.
VI. Conclusion:
Security is Crucial

Security is a critical consideration when evaluating any cloud-based service. Understanding the various security requirements can be daunting but this whitepaper should help you ask the right questions and interpret the answers of any provider you consider.

Of course, security is only part of the equation when thinking about sharing services. There are many other questions to ask including:

- How easy is the solution to use? Is there a steep learning curve?
- Will users have to change how they normally work to use the new service?
- Does it offer additional features like e-signatures as part of the primary application?
- Does it integrate with your existing software, like Microsoft Outlook and SharePoint?
- Is the setup and administration of the solution going to be an added burden for the IT staff or is the solution easily configurable and requires little maintenance?

A major advantage over other sharing services is that Hightail adapts to how you already do things, rather than forcing you to implement a new enclosed system. Seamless integration with Microsoft tools lets users access and share work from Outlook or SharePoint. A range of secure Hightail apps allow access to files from anywhere, including desktop or mobile device.

From the IT perspective, Hightail provides all the necessary security and controls without burdening account administrators with endless maintenance. Active Directory integration takes the effort out of initial setup and ongoing provisioning, while Hightail also allows you to set sharing policies and track usage.

To learn more about how Hightail can help your business share information more effectively without compromising your data security visit www.hightail.com.

MAKE YOUR BUSINESS MORE EFFECTIVE
WITH HIGHTAIL

Hightail is the trusted sharing solution for more than 42 million people around the world, including professionals at 98% of the Fortune 500.

Hightail is designed to help users work together more effectively by providing a simple way to share files and folders with both colleagues and external partners. It allows everyone to work together in the same place and make changes to files that are instantly updated. You can also digitally sign documents and return them right away.
VII. Relevant Links

Hightail
http://www.hightail.com

Privacy
http://www.hightail.com/aboutus/legal/privacy
privacy@hightail.com

Application Status
http://support.hightail.com/ts/Site-Status/bg-p/SiteStatus

Security still the 'No. 1 obstacle' to cloud adoption

Security is driving cloud adoption