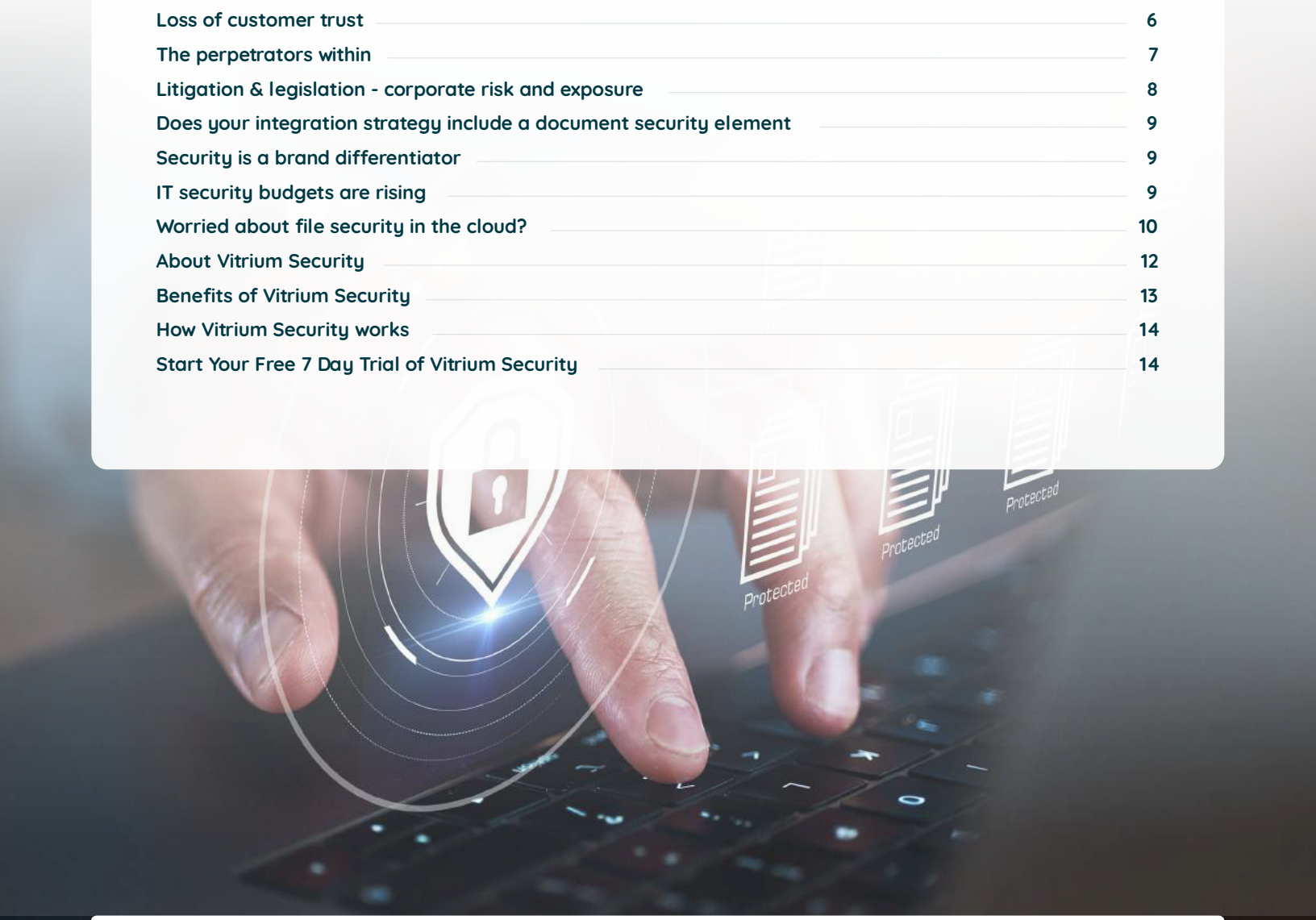
vitrium

White Paper

Why Invest in Document Security

+1 (604) 677-1500
+44 (20) 3321-9377
sales@vitrium.com
vitrium.com

Table of Content



Introduction to Document Security

Globally, the number of cyber attacks on businesses average 117,339 per day[1], and the frequency and severity of these attacks are increasing. Many of these preventable attacks cause significant loss to these organizations.

If you have experienced a loss of revenue or a decrease in customer confidence due to information theft, the contents of this white paper will serve to refresh some steps that can be taken to avoid that from occuring in the future. If that is not the case, and you are preemptively considering a document security solution for your business to mitigate concern about the security of your company's content, then this white paper will be equally helpful in outlining some reasons to consider implementig a document security solution.

Time for a change.

Be proactive and secure your company's confidential and revenue generating content.

Impacts to Revenue and Bottom Line

The impact of an incident can be felt all across the top line - immediately. Revenue streams tied to intellectual property can disappear. Or, in cases where sensitive customer information has been compromised, a reputation hit and a high customer turnover are the direct and indirect consequences respectively.

The bottom line also takes a hit. Valuable intellectual assets can be lost (or worse, sold and used by competitors), investigation and legal services needed, capital costs incurred to reinvest in infrastructure to repair the breach, plus PR and marketing to repair and rebuild the company's sales pipeline, reputation and brand. All of which can significantly impact the bottom line for years to come.

Digital content can be copied or leaked within seconds

Digital content can be copied within the span of a few seconds and quickly distributed, where the number of copies grows exponentially. Small thefts, plagiarism, and copyright violations happen all the time and most of the time the impact is insignificant. But the potential damage from a major document theft of leak can be substantial.

For most companies, that risk escalates with the volume of content stored and shared.

The best way to counter such a risk is to ensure that you have a proactive plan to properly monitor and secure information from internal and external threats; a plan that includes document-level protection. Even if a document is shared away from a protected network, or onto multiple devices, your valuable or sensitive documents have protection at the file level.

Cost fallout of a document or file leak can be felt for years

Experiencing a significant document leak, or even a major data breach, can have dire financial consequences in companies operating in a variety of industries.

• In August 2016, French naval contractor DCNS had secrets about its Scorpene submarines being built in India leaked [2]. The leak contained more than 22,000 pages outlining details of six submarines DCNS had designed for the Indian Navy, including combat capabilities. The contract with the Indian government was worth $38 billion, and may affect DCNS's ability to gain or see out contracts with countries like Australia, Poland, Norway, Chile, and Malaysia. Officials believe it was a case of economic warfare by sophisticated hackers, looking to take advantage of business' inability to secure sensitive and confidential documents at a file level. **File security controls such as encryption and digital rights management (DRM) could have mitigated costly risks of a document leak such as this.**

• Also in August of 2016 the **Federal Reserve fined Goldman Sachs $36.3 million** for failing to have policies and training to prevent use of leaked confidential documents [3]. This was in addition to a $50 million fine levied by the New York State Government for the same incident. A junior Goldman Sachs banker took confidential information from his previous employer, the Federal Reserve Bank of New York, after receiving the information from a former co-worker, still under Fed employment. The stolen documents exposed the Fed's private insights about regulatory matters, and Goldman Sachs used the information in presentations to current and prospective clients. Even though what Goldman Sachs did was illegal, the Fed could have **taken steps to protect its documents and keep its former employee from maliciously obtaining crucial information regarding its operations.**

• In late 2014, the Sony Pictures Entertainment cyber attack was in the news [4]. While the costs are still to be tallied, estimates of the impacts are in the billions and it's considered to be one of the largest in history. Not only emails and data were taken during the network intrusion, but unsecured documents of all kinds, including confidential contracts with talent, employee payroll and benefit information, and home addresses. It is likely to take years to determine the full impact. While it is yet to be determined if another government was to blame, the fact remains, **if huge companies with their enormous security budgets and infrastructure are vulnerable, all companies, large, small, and in-between, are vulnerable.**

• In 2013, when Target reported that the credit card information of 110 million customers was around in cyberspace [5], **its fourth quarter profit fell almost 50%, second quarter profit for 2014 sank by 62%,** full-year earnings forecast has been lowered and total expenses related to the breach stand at $148 million including related expenses.

• Home Depot's data breach left almost 60 million payment cards vulnerable to misuse [6]. **Investigation-related costs are pegged at $62 million.**

Data Breaches are expensive

The average cost of an incident is $3.5 million2

For many companies it's difficult to calculate the direct and indirect impacts of a data breach or document loss. It can vary widely depending on the nature of the incident.

The 2016 Cost of Data Breach Study: Global Analysis[7] reported that the average total cost of a data breach was $4 million, representing a 29% increase since 2013.

Many companies (not just the mega corporations) can benefit from taking the threat to their content seriously. Hackers will probe your security with various recon and vulnerability scans, and target businesses in industries that are known to be less likely to deploy multi-layered security technologies and have less robust governance.

They will specifically go after the valuable information contained in documents that are less protected, in transit, shared, synced to apps, or on devices.

Data Breaches are expensive

The average cost of an incident is $3.5 million2

Potential costs of a document leak

- Loss of customers and/or revenue
- Loss of intellectual property, digital assets, or trade secrets
- Investigative (forensic) services fees
- Legal costs (suits, counter-suits, class-action)
- Infrastructure repair and upgrades
- PR communications services - damage control
- Marketing - rebuilding brand reputation, trust, & sales pipeline

Exercise

Estimate your potential costs in each of these areas assuming a small, medium, or large incident with your most valuable or sensitive documents.

- What would even a 10% loss of revenue mean?
- How much risk is your organization willing to assume in light of the potential top-to-bottom-line cost estimates?

For many companies, it's becoming a necessity to ensure all corporate data and content is safe - wherever it ends up.

Loss of customer trust - negative brand capital never fully goes away

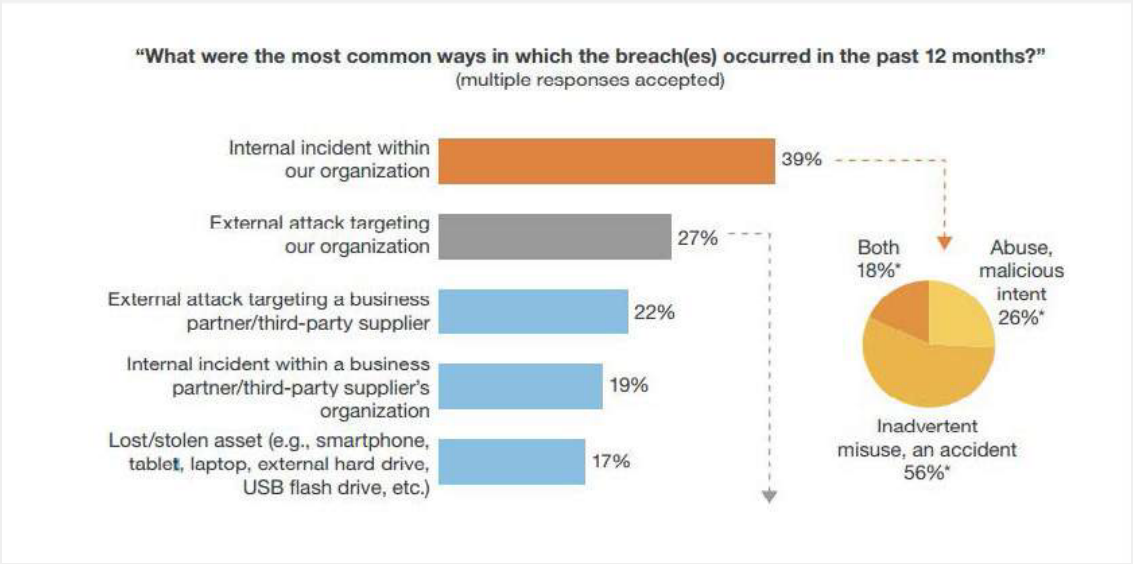
Dropbox's data breach put the private data of 6.9 million customers at risk in 2012[8]. Soon afterward, quite a few companies, including Morgan Stanley, restricted employee access to the file hosting service.

A recent survey reveals that **86% of customers were 'not very likely' or 'not at all likely' to do business with a company that had failed to protect credit/debit card details** and 82% wouldn't trust a company whose data breach involved home address, email addresses or telephone numbers[9]. **In this era where the story lasts 'forever', this kind of public flogging can have negative brand impacts lasting as long as the story is searchable online, creating an brand deficit that any future marketing must overcome.**

The perpetrators within

Digital documents hold all kinds of information – corporate data and customer related - within them.
Do you have adequate restrictions and policies in place regarding who can and cannot access sensitive or revenuegenerating documents?

FIGURE 1 Internal Incidents Are A Common Cause Of Breach



Forty percent of external attacks were carried out via a software exploit, while 38% reported some type of user interaction (watering hole attack, phishing, malicious link, or email attachment).

***Base:** 358 North American and European network security decision-makers who have experienced data breaches in the past 12 months (20+ employees)

***Base:** 184 North American and European network security decision-makers who have experienced the specified breaches (20+ employees)

***Base:** 156 North American and European network security decision-makers who have experienced the specified breaches (20+ employees)

Source: Forrester's Business Technographics® Global Security Survey, 2015

The Forrester report, Understand the State of Data Security And Privacy: 2013 to 2014[10] states that **insiders are responsible for 39% of all incidents of data breaches occurring in a company.**

Most mistakes are inadvertent and stem from an unfamiliarity or poorly understood data use and governance policies. These risks are exacerbated by the BYOD culture of storing data across various devices. However, breach incidences also include data abuse by unscrupulous insiders. If you cannot change the way you work, you can strike a balance between security and access to continue delivering a good reader experience.

Defining data and roles for users in an easily understandable way that doesn't interfere with experience or ability to work doesn't have to be challenging. It is an initiative that can be successful if you leverage the right document security tools.

Litigation & legislation - corporate risk and exposure

No matter how it happened, in your customers' minds, it's your fault. Cybersecurity is now a persistent legal risk as it is becoming more common for class action suits to be filed against corporations who do not institute sufficient information protection measures.

> If we're going to beconnected, then we need to be protected. As Americans, we shouldn't have to forfeit our basic privacy when we go online to do our business. Each of us as individuals have a sphere of privacy around us that should not be breached, whether by our government, but also by commercial interests.
>
> **- President Obama --**
> January 2015

Companies may find that they are more legally vulnerable now than in the past. For example, Target's data breach exposed the company to class action litigation[11] as a result, and Home Depot[12] is also experiencing similar pains due to their breach.

In addition, the legislative environment is becoming more and more concerned with personal privacy. In light of the recent large data breaches, fomer US President Obama proposed two new laws[13] to deal with personal privacy, whether or not these become law, corporate decision makers should be aware the environment is less and less tolerant. **In many states, and federally, legislation is being proposed and implemented to harden privacy laws.**

Also, companies are experiencing additional costs in data loss ("cyber") insurance coverage[14]. Sales have risen by more than 30% in recent years, as it becomes more and more necessary for companies to cover their increased risk and take cyber threats seriously.

Does your integration strategy include a document security element?

Governance and risk officers are demanding that IT have at least some data and content loss prevention controls in place. Without such controls, securing investment for integration can be an uphill task. By making data (and content) security, privacy and governance key elements of any integration strategy, you can move forward with your integration goals. **Given that, on an average, 32% of business-critical processes involve file transfers, a suitable document-level protection solution is vital to any integration strategy.**

Security is a brand differentiator

A document protection system is a competitive differentiator. **Information security is not just a window dressing when presenting your business case** but a critical factor that customers and clients peruse to justify buying from or partnering with you.

With incidences of leaked documents and information breaches making headline news and an understanding among consumers that cyber crimes are becoming more frequent, impactful and sophisticated, **you have an opportunity to make a strong business case for document-level protection. In fact, you can also push document security to the forefront as a profit protector and generator before the executive board. The business value of document security can become a source of competitive advantage.**

IT security budgets are rising

According to Forrester Research, at 17%, data security accounted for the second largest portion of the IT security technology budget in 2013, after network security. 35% of firms planned to increase their spending in this area in 2014. Gartner, in its 2013 Global Risk Management Survey[15] also reports an increase in IT security budgets.

The rise in IT security spending is not just a response to the increasing incidence of data breaches suffered by big companies, but a necessity given the increasing work collaboration between peers and business partners in today's corporate landscape. Forrester report Market Trends: Secure File Sharing and Collaboration in the Enterprise, Q1 2014[16] states that **97% of information workers collaborate with peers on a daily basis; 76% with clients or customers; and 64% with partners, vendors and suppliers.**

Aiding collaboration are multiple devices, with 61% of workers using some kind of mobile device – smartphone, tablet or laptop – for work. 53% use three or more devices to accomplish their jobs. Also, file sharing occurs most commonly through USB flash drives, email and CD/DVDs. **The ubiquity of sharing devices in a collaborative work environment poses the inevitable risk of failures in secure data handling these documents.**

Worried about file security in the cloud?

Companies have voiced their concern about the security of cloud-hosted files. **There are some who argue that the widely distributed nature of cloud computing makes it a risky proposition as far as security is concerned.** The counterargument is that security in data centers surpasses those on the public cloud.

Also, instances of brazen data breaches have involved laptops being stolen from cars or bars and disgruntled employees making off with gigabytes of data on USB drives. **Google and Microsoft have publicly declared that the cloud is now safe enough[17].**

The ubiquity of sharing devices in a collaborative work environment poses the inevitable risk of failures in secure data handling documents.

2013 cloud security report Targeted Attacks and Opportunistic Hacks[18] reached the following conclusions after examining the frequency and nature of security incidents occurring in the cloud hosting provider (CHP) and enterprise data center environments of 1,801 organizations:

- The cloud is as safe as enterprise data centers.
- Attacks in the cloud are crimes of opportunity while those in data center environments are targeted and sophisticated.
- In both environments, web application attacks are most frequent. Enterprise data center customers are more likely to be at the receiving end of these attacks (15 per cent) than CHP customers (3 per cent).

The study also found that though financial services represent a most attractive target for attacks, they are not a target of opportunity but of choice. Media organizations, on the other hand, accounted for a higher number of incidents in the study. They tend to be less stringent about implementing security measures despite the fact that their content assets are of great interest.

Other industries of interest to attackers include IT services, e-commerce, manufacturing and energy. A different report by Alert Logic State of Cloud Security Bulletin: Information Security in the Energy Sector[19] revealed that companies in the energy sector are lucrative targets for cyber attacks.

In some instances, the attacks intend to steal consumers' personal information, but in most cases, the attackers are gunning for confidential, proprietary and valuable private sector files on survey, geological, research and technology-related data as well as intellectual property and details about financial deals that can later be sold to competitors, used in negotiations, media leaks, or even for extortion.

Document protection is an issue of corporate value. Compromising on corporate value can have a disastrous effect on your bottom line, reputation and competitive advantage.

Learn more about how a document security solution like Vitrium Security can help in protecting your organization's digital assets. Learn more in the next few pages.

1 See Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015. PWC.com

2 See France's DCNS says India submarine data leak may be "economic warfare. Reuters. 2016.

3 See Federal Reserve Fines Goldman Sachs $36 Million in Document Leak. NewYork Times, 2016

4 See The cyberattack on Sony Pictures made employees collateral damage. WashingtonPost.com

5 See Target's Cyber Attack Fallout Cost $148M in Q2; $38M to Insurers. CarrierManagement.com

6 See Home Depot Confirms Data Breach, Investigating Transactions From April Onward. Forbes.com

7 See 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute. IBM.com

8 See Dropbox confirms security breach. Information-Age.com

9 See 86% of customers would shun brands following a data breach. RealWire.com

10 See Understand The State of Data Security and Privacy: 2015 to 2016. Forrester

11 See One Year Later: Consumers Can Protect Against Target in Data Breach Lawsuit. AboveTheLaw.com

12 See Home Depot facing dozens of data breach lawsuits. Fortune.com

13 See Obama to Call for Laws Covering Data Hacking and Student Privacy. NYTimes.com

14 See AIG: Cyber insurance sales have risen by 30%. SCMagazineUK.com

15 See IT Security Budgets Rise as Data Breach Fear Spreads. Gartner Blog

16 See Market Trends: Secure File Sharing and Collaboration in the Enterprise. Q1 2014, Forrester

17 See Google, Microsoft agree: Cloud is now safe enough to use. CNET.com

18 See 2013 State of Cloud Security Report from Alert Logic. SiliconAngle.com

19 See Attackers Ramp Up Threats to the Energy Sector. InfoSecurity-Magazine.com

About Vitrium Security

We invite you to explore some of the benefits of using Vitrium Security.

Our popular document protection software can help you limit the risk of your content being copied, leaked, shared, or stolen. Your PDF and Office files are instantly protected, ready to be distributed, and easily viewed by your audience. You can choose to publish the secured content to a user portal, send via email, or post to your own website, document management system, learning management system (LMS), eCommerce site, or other portal. Whatever method you choose, the files always remain secured no matter where they go.

Vitrium Security is trusted by hundreds of companies around the world to protect their documents and millions of readers have accessed our secure documents.

Benefits of Vitrium Security

Easy to use, for you and your audience.

Vitrium's intuitive software lets you manage your files, set up users and groups (this can also be managed through a separate system or database), define DRM policies, choose your distribution method, and access real-time analytical reports. Your audience easily accesses your content on any device, without the need for plug-ins or apps.

Distribute your files with confidence.

Your files are secured with Vitrium's **military grade 256-bit AES encryption** , and the layers of protection travel with your file, online or offline, so that even in case of theft or leak, your content remains secured. After uploading your files to Vitrium Security, you will have access to a secured PDF or a secured Weblink to share with your audience.

Your content, your power to decide.

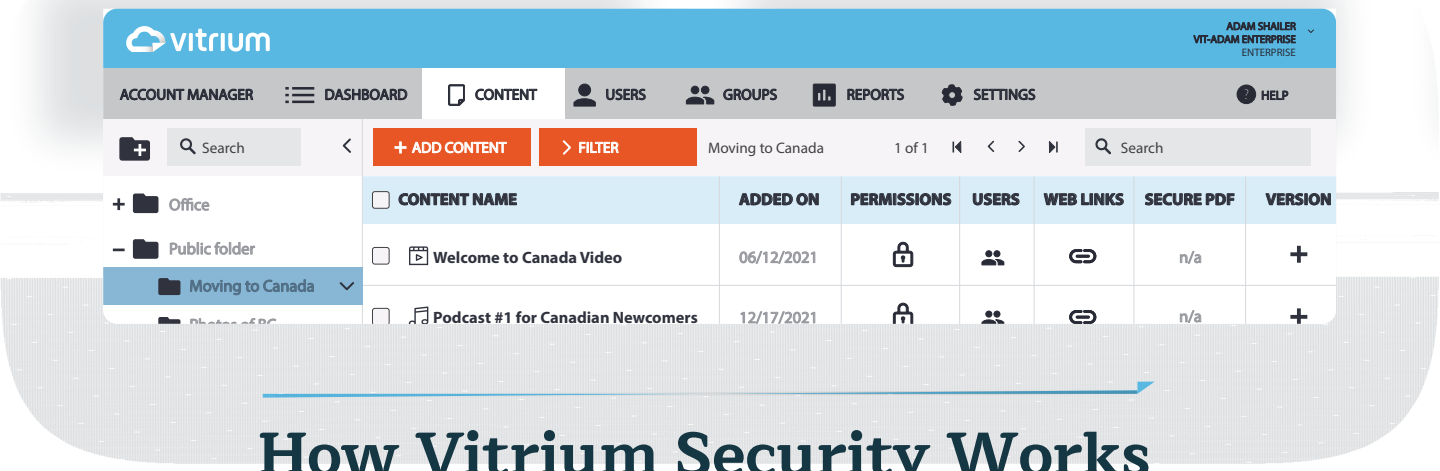
Vitrium Security gives you full control over your content - you can block printing & copying, set browser limits, apply dynamic watermarks, set expiry dates, and more. You can also retain this control after the content has been distributed as you can revoke a document at any time, replace the content, or deactivate a user – all within the Vitrium admin panel.

Set up your own customizable content portal.

Securely distribute your documents via Vitrium Security's customizable user portal, where authorized audience accesses all documents associated with their account in one place. Provide the best experience to by customizing with your colors and logo, and a customizable URL.

Improve the way you do business.

With Vitrium Security's dashboard and analytical reports, you can track the activity of your users and their behaviors, providing you insight into your business. Know which files are being accessed, what pages are being read, and which users are truly engaged. With Vitrium's new User Portal, your document store is instantly created and tracked.



How Vitrium Security Works

Add Files

Add your files to Vitrium's cloud-based ontent security software. We also offer an installed, on-premise version. Acceptable file formats include PDF, Word, Excel and PowerPoint. Video and images to come in 2017.

Add Users & Groups

Select the audience for your content. Decide who can access your secured files, place them in user groups, or leave them as individual recipients. Vitrium can also be integrated with your own user credential system.

Apply Security & Controls

Protect your files with military-grade 256-bit AES encryption and control access by setting various limits – viewing, browser, date, IP address limits and more. Block printing & copying, and insert dynamic watermarks.

Share With Users

Publish and share secured content as attachments or secured weblinks in a customizable user portal, through your own web portal, eCommerce site, or any other system such as document management system, association management, ECM, LMS, or via email.

We can help you integrate Vitrium Security with any system you might be using.

Next Steps

To learn more about Vitrium Security visit www.vitrium.com and start using Vitrium Security today.

Schedule a Demo

Visit www.vitrium.com/demo