vitrium

e-Book

Top 6 Reasons To Protect Your Documents



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

Table of Content

Protect Revenue Generating Assets 3

Increased Risk with Mobile Devices & BYOD Initiatives 4

Copyright Infringement & Piracy are Rampant 7

Privacy, Legal, or Compliance Obligations 9

Maintain Control & Understand Who's Accessing Your Content 9

Keep Your Trade Secrets and Other Confidential Information Safe 10

DRM & Document Security Misconceptions 11

What Industries Most Need Document Protection? 16

What Are the Main Benefits of Document Protection? 17

Why Choose Vitrium Security? 18

How Vitrium Security Works 19

01

Protect Revenue Generating Assets

You spend a great deal of money and time creating content, publications, e-learning and training materials, standards, market reports, forecasts, newsletters, and other assets that you own.

Having someone take these assets and use them for their own means without permission is theft.

Yet, online appropriationg of documents and content is common. Material that is copyrighted, patented or trademarked belongs to the owner of the copyright and that owner has a reasonable expectation to protect that asset. A good document security system, like Vitrium Security, can help protect these assets and revenue streams by allowing content owners to control who has access to their documents, when they have access, and track who accessed them.





A good document security system can help protect assets and revenue streams by allowing content owners to control who has access to their documents, when they have access, and track who accessed them.

02

Increased Risk with Mobile Devices & BYOD Initiatives

Documents and data get around more than ever before thanks to an explosion of digital technology in the past decade.

However, while the commercial applications of devices have been important to this trend, it is the increase in **consumer use of technology** that has largely driven increases in the number of files that are transferred across the Internet every day.

Many publishers and creators worry about video, audio and software piracy, but the most danger comes from the internal and external theft and transfer of documents.

Not every person is capable of – nor interested in – torrenting a ripped Blu-Ray Disk or getting the latest game for their hacked console. However, **more and more people are turning to e-books** and have since become familiar with ways to get their hands on text documents.



“Many publishers and creators worry about video, audio and software piracy, but the most danger likely comes from the theft and transfer of documents.”

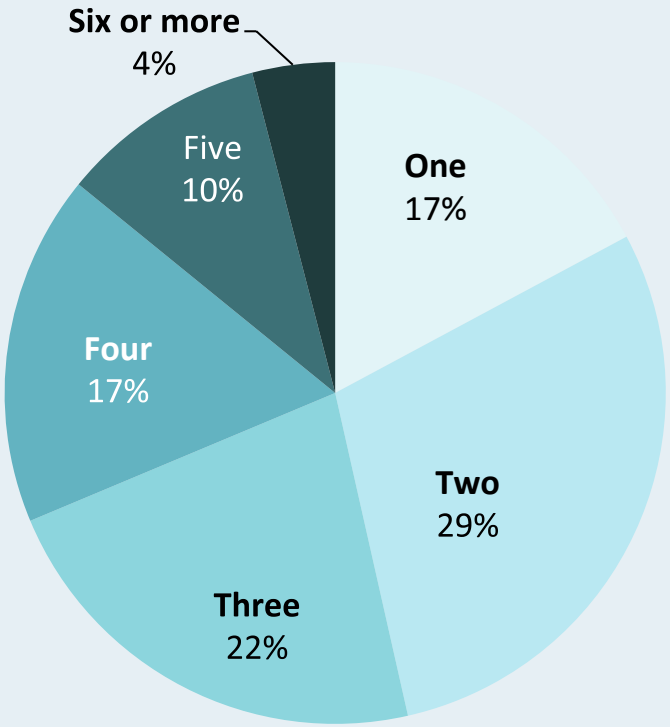
02

Increased Risk with Mobile Devices & BYOD Initiatives

Additionally, the past few years have seen an enormous explosion in the number of devices that readers are using both personally and at the workplace (many of which they choose themselves), resulting in an enormous market for digital documents, and huge potential for these documents to be shared on many devices.

Forrester Research Inc, surveyed 4,106 info workers at SMB's and found that over 53% use more than 3 devices at work.

Interestingly, in the same study when workers were asked how they decided on a technology to use, it's no surprise that the "accessibility of the tool by all recipients" had the greatest response, followed by "the sensitivity of the information". It makes sense – you want a new tool to be easy, accessible, and to ensure that if your information is being shared, it's going to the right people.



Number of devices used for work

Base: 4,106 North American and European information workers at SMBs and enterprises

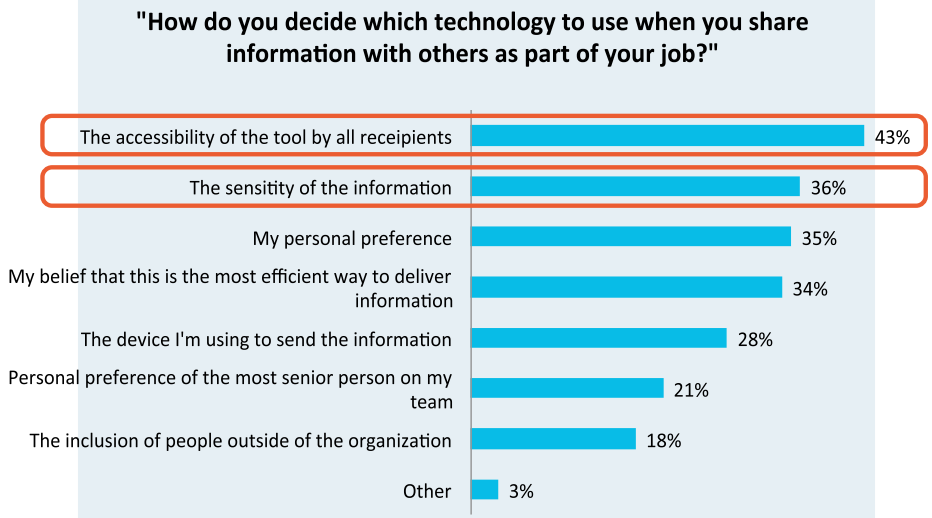
Source: Forrsights Applications And Collaboration Workforce Survey, Q4 2013 | Forrester Research Inc. | 109821

02

Increased Risk with Mobile Devices & BYOD Initiatives

All of this activity and variability creates a potent need for digital rights management on documents that companies produce for readers. Commercial entities should understand that their documents, data and content are easier than ever to download and view. Companies that share content digitally are at risk for piracy and losses that can undercut their entire operations.

It's a C-suite issue, not just an IT issue1. Departments need to realize responsibility for the information in the documents they handle, but executives need to understand the business case for protecting important intellectual and monetized document assets and lead document protection planning from the top down, tasking IT with the means and ways to employ appropriate tools and countermeasures.



Base: 3,665 North American and European information workers at SMBs and enterprises

Source: Forrsights Applications And Collaboration Workforce Survey, Q4 2013 | Forrester Research Inc. | 109821

03

Copyright Infringement & Piracy are Rampant

Online piracy is an issue that is getting a lot of attention these days, and well it should. The data out there says a lot! And plenty of folks don't see a problem with it. Your valuable documents are also valuable to those who don't have the best intentions, or just don't care.





It's a C-suite issue, not just an IT issue. Executives need to understand the business case for protecting important intellectual and monetized document assets, and lead protection programs from the top down, tasking IT with the means and ways to employ appropriate tools and countermeasures.

03

Copyright Infringement & Piracy are Rampant



70%

of Online Users Find Nothing Wrong in Online Piracy



71,060 jobs/yr

lost in the United States every year due to Online Piracy



$2.7 billion in workers' earnings are lost each year due to Online Piracy



22% of all global Internet bandwidth is used for Online Piracy



67%

of Digital piracy sites are hosted in North America and Western Europe



98.8%

of Data transferred using P2P networks is copyrighted



91.5%

of files available for download on Cyberlockers sites (Rapidshare, Megaupload,etc) are copyrighted material



1/10,000

pieces of the most popular content on the OpenBitTorrent tracker is non-copyrighted



146 Million/day

Websites hosting pirated content receive more than 146 million visits per day

Source: www.go-gulf.com/blog/online-piracy/

04

Privacy, Legal, or Compliance Obligations

Many organizations and companies are required by law to protect sensitive information, and most of us would agree that if our private financial, health, legal or other personal data were spread out into the world we'd be very upset, and possibly vulnerable to attacks. Think about it. Is there information in your company's documents right now that might hurt someone if it got into the wrong hands? It's imperative we all do what we can to protect sensitive information – even if it's not ours.



Most of us would agree that if our private financial, health, legal or other personal data were spread out into the world we'd be very upset, and possibly vulnerable to attacks.

05

Maintain Control & Understand Who's Accessing Your Content

Sometimes documents get passed from person to person without any intent to harm a company's revenue, but yet this lack of control can mean that companies lose the ability to track the location of their owned materials. It can also be the case that documents, like board minutes, or technical schema, that are distributed widely can end up in the hands of folks who do intend to do some harm or profit from it somehow without your consent. Document control and protection systems, like Vitrium Security, can allow you **to track where the document goes, revoke access and even expire (digitally shred) the document wherever it might end up.**



Document control and protection systems, like Vitrium Security, can allow you to track where the document goes, revoke access and even expire (digitally shred) the document wherever it might end up.

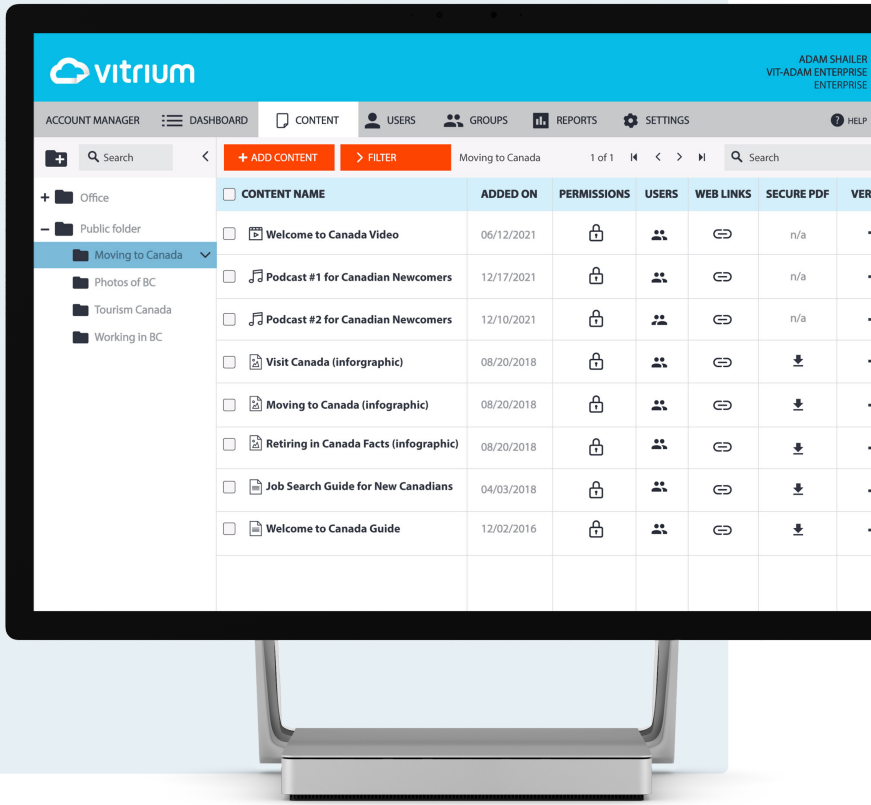
06

Keep Your Trade Secrets and Other Confidential Information Safe

We all know it's a competitive world, but in some industries, out-competing your competition is essential to survival. Any leak of critical information, such as; drilling sites (oil & gas, or mining industry), financial investment advice, research documents, sensitive healthcare information, inventions and creative patents, IT protocols and technical schemata, could be catastrophic to the business.

Document protection plans incorporating a tool like Vitrium's cloud-based, or on-premise installed, Vitrium Security solution, enables entrepreneurs, CEOs, researchers and analysts, IT departments, and publishers of any stripe, to block copying and printing, or limit viewing of the document for a certain period of time.

Vitrium Security solution, enables entrepreneurs, CEOs, researchers and analysts, IT departments, and publishers of any stripe, to block copying and printing, or limit viewing of the document for a certain period of time.

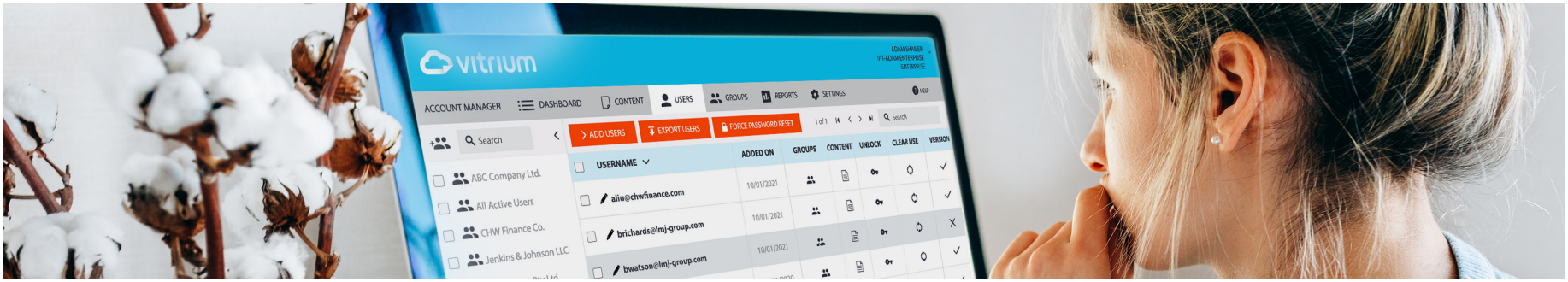


DRM & Document Security **Misconceptions**



01 Security Misconceptions

The higher the level of protection the more disruptive it is for the end user



It's a fact that the more secure a document is, the more barriers there are to accessing the document and the fewer options the reader has for copying, printing and otherwise interacting with the file. Software requirements are sometimes difficult to download and install, especially in environments that are IT restricted, and can make legitimate users irritated. Reader loyalty is important to content producers too, and who needs the hassle of readers complaining? More and more, DRM software companies are trying to find a balance between providing content owners the protection they need while at the same time ensuring the end user (or reader) has a good experience. Make sure, when you are looking for DRM software, that the solution offers readers a seamless, non-intrusive experience, and just enough security to make sure the documents go where they are meant to and nowhere else.

When you are looking for DRM software, that the solution offers readers a seamless, non-intrusive experience, and just enough security to make sure the documents go where they are meant to and nowhere else.

02 Security Misconceptions

DRM is not needed in today's world

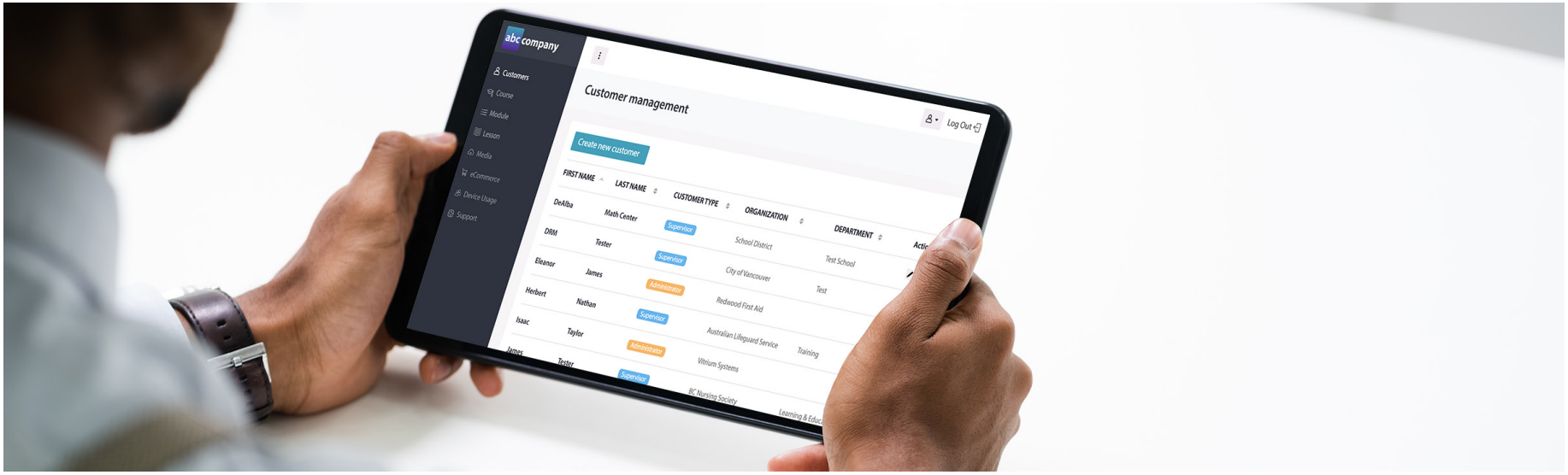


Companies and organizations need to digitally share information that is sensitive, and may be under legal obligation to protect this vital data, like financial, legal, or health care data. Additionally, there are trade secrets that companies don't want competitors to learn, board minutes and notes, legal contracts and documents, and a whole variety of information that shouldn't be shared with the wild wild web, or other individuals who are not authorized to access the information. In this digital age companies have a need to distribute these documents somehow and should reasonably expect there to be a mechanism to do so. Finally, companies invest a lot of time, effort and money into producing materials that are copyrighted, trademarked and produce revenue for them, such as training materials, eBooks and other documents. **They should also reasonably expect some protection of these assets, just as you would lock your car, or insure your house.**

Companies invest a lot of time, effort and money into producing materials that are copyrighted, trademarked and produce revenue for them, such as training materials, eBooks and other documents. They should also reasonably expect some protection of these assets.

03 Security Misconceptions

DRM it’s too expensive



That depends on how you look at it. Like car insurance, it can save you a lot if you get in an accident. With the costs of copyright infringement or patent lawsuits ranging from $350,000 - 5,000,000, its no wonder companies want to avoid having to take legal action.

Companies find that investing in document protection as part of their risk mitigation efforts not only prevents costly legal fees, but prevents revenue loss, blow-back from leaks, and other damaging consequences that can have huge impacts on the bottom line. A good DRM system is much more prudent to take some reasonable steps to prevent these consequences before they happen.

Trying to avoid this issue by using printed materials has its own costs. Printing, mailing and storing documents can still be copied and stolen, and a company is likely to save in just storage and efficiencies by adopting a digital document strategy.

Choosing to not protect documents can result in greater risk with intellectual assets. For example, an educational institute, or monetized corporate training program that sells its materials to students, might find its revenue stream diminished by students simply sharing these materials, or worse yet, selling these documents and pocketing the money.

04 Security Misconceptions

Security can be broken



We can't deny that at times, secured content can get broken into. Just as a determined thief can circumvent the locks on a house, we've seen that determined hackers or technically savvy individuals can circumvent even the strictest security policies of a document or IT firewall. The higher level of security a document has, the less likely it will be broken or "hacked" into, but the downside is that it can become disruptive to the reader - resulting in more steps to unlock a document or download apps or plugins to view the documents. At Vitrium, we have strong encryption (256bit) options, and lighter weight options (128 bit encryption, or "social DRM") for all security needs while maintaining a hassle-free experience for readers.

Find the right balance between reader experience and the security you need.

When you are choosing a service to protect your documents, it serves you well to think about the impact of the tool on your users balanced against the level of protection you need, or must, provide.

What Industries Most Need **Document Protection?**

These days everyone should be thinking about what they are sharing online, how someone could play with your sensitive information, and to what end any potential leak could damage you personally, your business, or your reputation.

Better search and other technologies make it easier for us to find information online, but it's getting easier for hackers, pirates, and competitors to find our files too. It's more important than ever to think about whether your company, firm, or organization could be a gold-mine of data and files, and develop a plan for protecting that information now.

Industries in most need of document protection:

Industries	Types of Documents
Publishing	eBooks, manuscripts, draft work
Research, Development, Sciences, Pharmaceuticals	Abstracts, reports, studies, analysis, dissertations
Associations	Membership data, confidential & paid reports
Education / eLearning	Learning materials, eBooks
Corporations & Business	Corporate training materials, financial documents
Financial	Investment reports, tax info, statements, personal and / or business data
Management Consulting	Confidential market data and analysis
Legal	Contract, wills, agreements, and any sensitive legal documents
Healthcare	Confidential patient information, reports
Oil & Gas, and Mining	Drilling sites, maps, specs and plans
Non-profit	Member data, confidential and paid reports
Manufacturing and Technology	Innovations, patents, design specs or sensitive trade secrets
Advertising & Design Agencies, Architecture	Design briefs, compositions, plans, or sensitive trade secrets
Any Industry and Company	Confidential materials to send to the Board

Not mentioned? There are thousands of companies who can benefit from protecting their files – why not get in touch with us and surprise us with your use case!

What Are the Main Benefits of Document Protection?

01 Protect Confidential, Sensitive or Revenue-Generating Content

Whether you have confidential information contained in financial reports, product sheets, board materials or you earn revenue from published content such as eBooks, training materials, or research reports, you'll want to protect that content with some level of encryption and control to prevent document or data leaks, protect your IP, or preserve your revenue streams.

02 Control Access and Set Limits

A good document protection solution will go beyond just encrypting your documents. It can also offer a variety of access control and rights management benefits such as the ability to apply password-protection or other credential unlocking options. It can offer the ability to set different limits on who can access your content and how with device limits, expiry dates, print limits, and more.

03 Track Activity and User Behavior

A third benefit of document protection is the ability to track user and file activity. Understand who's opening your documents, which documents are being accessed the most, how much time is being spent on them, and what's the read-through-rate. This kind of granular analytical data provides incredible insight for an organization and can be used to make strategic decisions.

Why Choose Vitrium Security?

Vitrium Security is one of the most powerful and easy to use document security, analytics, and digital rights management (DRM) solutions on the market today - trusted by companies around the world, and accessed by over a million users. Below are three reasons why organizations consistently choose Vitrium over other systems:



Security That Travels With the Document

Documents that are secured with Vitrium technology are protected no matter where they go – whether saved to a local computer or device, shared with external audiences, or uploaded to the cloud, the security stays with the document.



Access Anywhere With No Plug-ins or Apps Required

Unlike other document security solutions, Vitrium Security offers a hassle-free experience for users to view the secured content – documents can be opened on any type of device, without the use of plug-ins, apps or 3rd party software to download.



Multiple Distribution Options

Post your secured content to a customizable user portal, send via email with secured web links or attach as a secured file, save to an internal network or document management system, or post to a website, eCommerce system, LMS, ECM, or other web portal.



Vitrium Security is trusted by hundreds of companies around the world to protect their documents.

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.

Learn More

www.vitrium.com/contact-us

Schedule a Demo

www.vitrium.com/demo