silo

How Financial Firms Turn the Web from a Liability Into an Asset

A CLOUD BROWSER BUILT FOR COMPLIANCE & CONTROL

WEB OF RISKS

Introduction

In addition to keeping company assets and clients safe from online exploits, buy side and sell side firms must navigate an increasingly complex compliance landscape to stay on the right side of regulators when they use the web. This poses a particular challenge for the Chief Compliance Officer and IT Administrators in investment firms.

Expectations of “anytime, anywhere” access, expanded use of social media, and migration of apps to the cloud have introduced a myriad of new risks to the firm. While the web has become an irreplaceable tool for firms, it also represents existential risk - financial, reputational, and regulatory.

How can firms balance the security and governance requirements of the web with the user need for access and productivity? With Silo, the Cloud Browser, a secure, virtual browser in the cloud, built for both isolation and good governance. With Silo, employees get access to the web without exposing the firm. IT and compliance teams get total command and control of what users do online.

FALSE SENSE OF SECURITY

Web Activity Is Hard to Govern

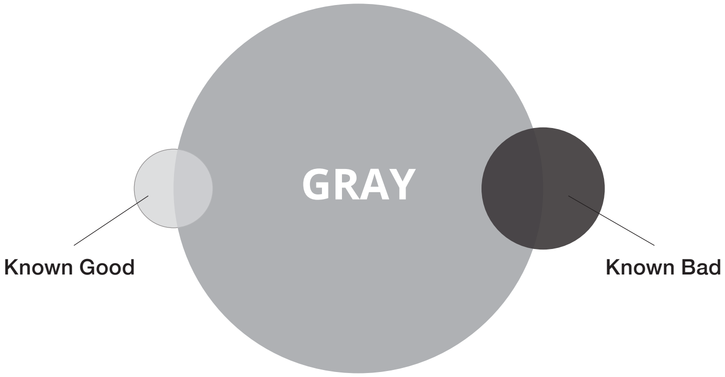
While the web is essential for productivity, when users go online, it also creates compliance and security risk. Financial Services firms are particularly vulnerable. Almost 80% of data security incidents in the finance industry are web-related, according to industry observers.[1]

Domain filtering isn’t effective

The traditional method of managing access based on list-based categorization isn’t scalable. There are more than 1.9B websites, with nearly 400 new websites added every minute.[2] Classifications change as sites become more interactive, allowing users to post and chat, creating ad-hoc social networks.

Although blacklists are a common approach to restrict access to “risky” sites, even sites categorized as “safe” may be vulnerable to exploits if they run Flash, Java, Visual Basic or other web-based scripts. Today, 1 in 13 web requests lead to malware (up from 1 in 20 in 2016).[3]

Moreover, blocked sites, including social media sites, may actually be relevant for research purposes, and could help analysts develop important insights into consumer habits/trends. Blacklists and whitelists define a narrow sliver of the web, while users spend most of their time in “gray” areas where the majority of risks live.



Not just site vulnerability - online behavior creates risk

In regulated industries like financial services, not just the sites users visit, but also user activities online create risk. Every comment posted online represents a potential compliance violation. Similarly, every client record or sensitive data element accessed from a web-connected device increases the risk of data leakage.

Growing complexity puts compliance officers in a tough position, where they need to preserve access while containing risk. According to Accenture, 9 out of 10 financial services industry executives expect compliance costs to continue increasing.[4]

COSTLY POINT SOLUTIONS

Current Solutions Aren't Working

Firms have turned to a patchwork of point solutions trying to get back in control of the web. The suite of technology that firms need to manage for security and compliance online is daunting:

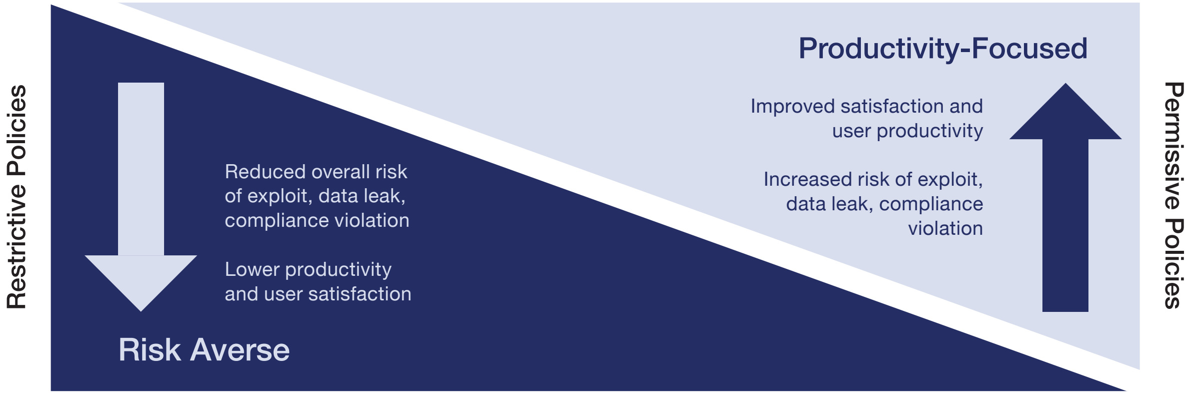
- **At the endpoint:** AI-enabled anti-virus solutions, CASB agents to collect local device statistics
- **At the network:** SIEMs to collect and detect network anomallies, VPNs for remote access
- **At the gateway:** Firewalls, proxies, Secure Web Gateways, including URL forwarding and API-based scrapers to collect 3rd party site log data

According to Cisco, nearly half of the security risk that organizations face stems from having multiple security vendors and products.[5] Customers are trying to manage an "arsenal of tools that may obfuscate rather than clarify the security landscape."[6] Multiple vendors not only add to the complexity, but also to the costs. Cybersecurity spending has increased 35x over the last 13 years, while the number of reported incidents continues to rise.[7]

RISKY COMPROMISE

The Tradeoff Between Compliance and Productivity

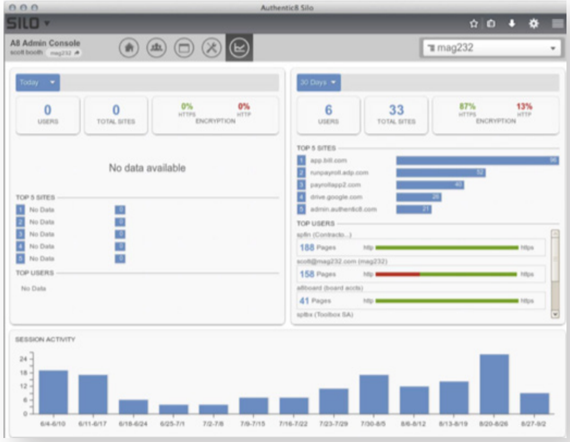
Firms are forced to install and manage solutions that either place barriers in front of the user (restricting their behavior), or function as safety nets for the organization (detection and analysis solutions). Neither approach is ideal, both involve trading security/compliance for productivity. For each site, action, or service, firms need to assess where the user places them on the risk continuum.


Restrictive Policies
Reduced overall risk of exploit, data leak, compliance violation
Lower productivity and user satisfaction
Risk Averse
Productivity-Focused
Improved satisfaction and user productivity
Increased risk of exploit, data leak, compliance violation
Permissive Policies

BACK IN CONTROL

A Cloud Browser Built for Security and Governance

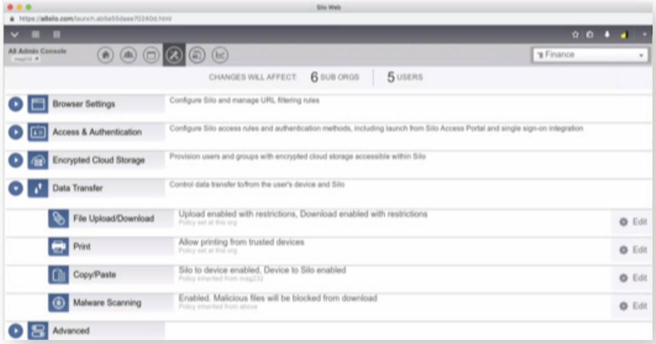
Organizations need a solution that doesn't force them to trade lower risk for increased productivity. Silo is a cloud browser built for security and governance. As a cloud-based virtual browser, it executes all web code on a remote host and delivers an encrypted remote display to the user. This way, it eliminates the organization's exposure to public web code.



Each Silo session is built with embedded, IT or compliance-defined policies, which govern device access, websites, content types, credentials, data operations, and more. All user actions are logged and encrypted, which facilitates compliance reviews and post-issue remediation.

Users get a secure, compliant, and personalized browser for increased productivity online. Admins get a centralized, managed browser that gives them control and oversight of user activities online.

Admins can manage users, web app entitlements, data policies and more from a single, intuitive web console. Authorized admins can audit users by group or subgroup.


Silo Web
https://a8silo.com/launch.ab5e55daee70240d.html
A8 Admin Console
Finance
CHANGES WILL AFFECT: 6 SUB ORGS 5 USERS
Edit

Browser Settings — Configure Silo and manage URL filtering rules

Access & Authentication — Configure Silo access rules and authentication methods, including launch from Silo Access Portal and single sign-on integration

Encrypted Cloud Storage — Provision users and groups with encrypted cloud storage accessible within Silo

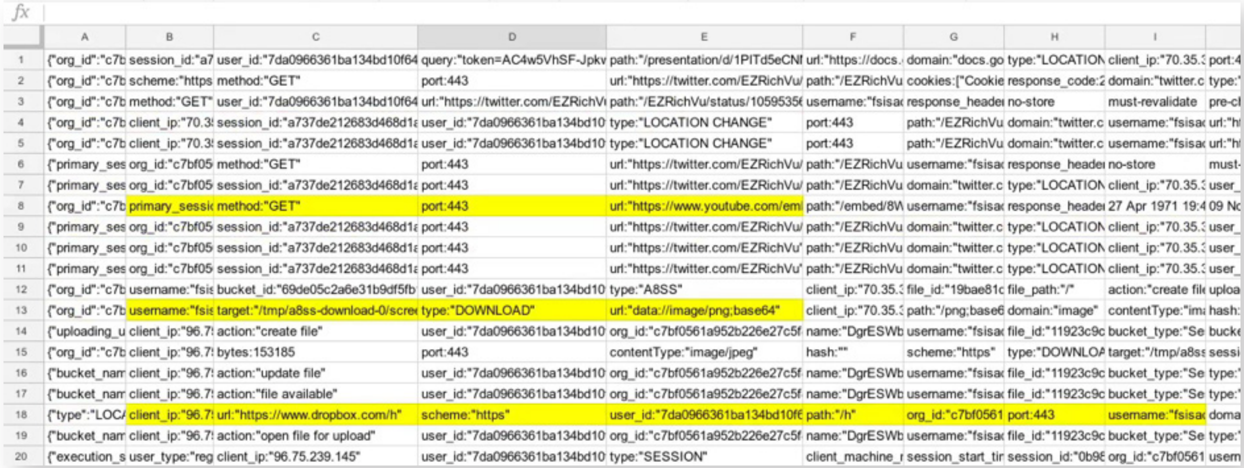
Data Transfer — Control data transfer to/from the user's device and Silo

- File Upload/Download — Upload enabled with restrictions, Download enabled with restrictions (Policy set at this org)
- Print — Allow printing from trusted devices (Policy set at this org)
- Copy/Paste — Silo to device enabled, Device to Silo enabled (Policy inherited from mag232)
- Malware Scanning — Enabled. Malicious files will be blocked from download (Policy inherited from above)

Advanced

Policies cover anything done in the browser, including URL categorization. So in scenarios where the user visits an authorized site with malware, or where users need access to a site normally blocked, the firm can maintain access without incurring risk.

And through it all, admins get encrypted, comprehensive and centralized audit logs of everything done in the browser.



	A	B	C	D	E	F	G	H	I	
1	{"org_id":"c7b	session_id:"a7	user_id:"7da0966361ba134bd10f64	query:"token=AC4w5VhSF-Jpkv	path:"/presentation/d/1PITd5eCNI	url:"https://docs.	domain:"docs.go	type:"LOCATION	client_ip:"70.35.3	port:4
2	{"org_id":"c7b	scheme:"https	method:"GET"	port:443	url:"https://twitter.com/EZRichVu/	path:"/EZRichVu	cookies:["Cookie	response_code:2	domain:"twitter.c	type:"
3	{"org_id":"c7b	method:"GET"	user_id:"7da0966361ba134bd10f64	url:"https://twitter.com/EZRichVi	path:"/EZRichVu/status/1059535	username:"fsisa	response_header	no-store	must-revalidate	pre-cl
4	{"org_id":"c7b	client_ip:"70.3	session_id:"a737de212683d468d1a	user_id:"7da0966361ba134bd10	type:"LOCATION CHANGE"	port:443	path:"/EZRichVu	domain:"twitter.c	username:"fsisa	url:"ht
5	{"org_id":"c7b	client_ip:"70.3	session_id:"a737de212683d468d1a	user_id:"7da0966361ba134bd10	type:"LOCATION CHANGE"	port:443	path:"/EZRichVu	domain:"twitter.c	username:"fsisa	url:"ht
6	{"primary_ses	org_id:"c7bf05	method:"GET"	port:443	url:"https://twitter.com/EZRichVu/	path:"/EZRichVu	username:"fsisa	response_header	no-store	must-
7	{"primary_ses	org_id:"c7bf05	session_id:"a737de212683d468d1a	port:443	url:"https://twitter.com/EZRichVu/	path:"/EZRichVu	domain:"twitter.c	type:"LOCATION	client_ip:"70.35.3	user_
8	{"org_id":"c7b	primary_sessi	method:"GET"	port:443	url:"https://www.youtube.com/em	path:"/embed/8W	username:"fsisa	response_header	27 Apr 1971 19:4	09 No
9	{"primary_ses	org_id:"c7bf05	session_id:"a737de212683d468d1a	port:443	url:"https://twitter.com/EZRichVu/	path:"/EZRichVu	domain:"twitter.c	type:"LOCATION	client_ip:"70.35.3	user_
10	{"primary_ses	org_id:"c7bf05	session_id:"a737de212683d468d1a	port:443	url:"https://twitter.com/EZRichVu"	path:"/EZRichVu	domain:"twitter.c	type:"LOCATION	client_ip:"70.35.3	user_
11	{"primary_ses	org_id:"c7bf05	session_id:"a737de212683d468d1a	port:443	url:"https://twitter.com/EZRichVu"	path:"/EZRichVu	domain:"twitter.c	type:"LOCATION	client_ip:"70.35.3	user_
12	{"org_id":"c7b	username:"fsis	bucket_id:"69de05c2a6e31b9df5fb	user_id:"7da0966361ba134bd10	type:"A8SS"	client_ip:"70.35.3	file_id:"19bae81c	file_path:"/"	action:"create file	uploa
13	{"org_id":"c7b	username:"fsis	target:"/tmp/a8ss-download-0/scree	type:"DOWNLOAD"	url:"data://image/png;base64"	client_ip:"70.35.3	path:"/png;base6	domain:"image"	contentType:"ima	hash:
14	{"uploading_u	client_ip:"96.7	action:"create file"	user_id:"7da0966361ba134bd10	org_id:"c7bf0561a952b226e27c5f	name:"DgrESWb	username:"fsisa	file_id:"11923c9c	bucket_type:"Se	bucke
15	{"org_id":"c7b	client_ip:"96.7	bytes:153185	port:443	contentType:"image/jpeg"	hash:""	scheme:"https"	type:"DOWNLOA	target:"/tmp/a8ss	sessi
16	{"bucket_nam	client_ip:"96.7	action:"update file"	user_id:"7da0966361ba134bd10	org_id:"c7bf0561a952b226e27c5f	name:"DgrESWb	username:"fsisa	file_id:"11923c9c	bucket_type:"Se	type:"
17	{"bucket_nam	client_ip:"96.7	action:"file available"	user_id:"7da0966361ba134bd10	org_id:"c7bf0561a952b226e27c5f	name:"DgrESWb	username:"fsisa	file_id:"11923c9c	bucket_type:"Se	type:"
18	{"type":"LOCA	client_ip:"96.7	url:"https://www.dropbox.com/h"	scheme:"https"	user_id:"7da0966361ba134bd10f6	path:"/h"	org_id:"c7bf0561	port:443	username:"fsisa	doma
19	{"bucket_nam	client_ip:"96.7	action:"open file for upload"	user_id:"7da0966361ba134bd10	org_id:"c7bf0561a952b226e27c5f	name:"DgrESWb	username:"fsisa	file_id:"11923c9c	bucket_type:"Se	type:"
20	{"execution_s	user_type:"reg	client_ip:"96.75.239.145"	user_id:"7da0966361ba134bd10	type:"SESSION"	client_machine_r	session_start_tir	session_id:"0b9	org_id:"c7bf0561	usern

Silo has been adopted across hundreds of highly regulated, closely monitored and security-sensitive IT environments, including federal government agencies, global law practices, and leading Wall Street firms.

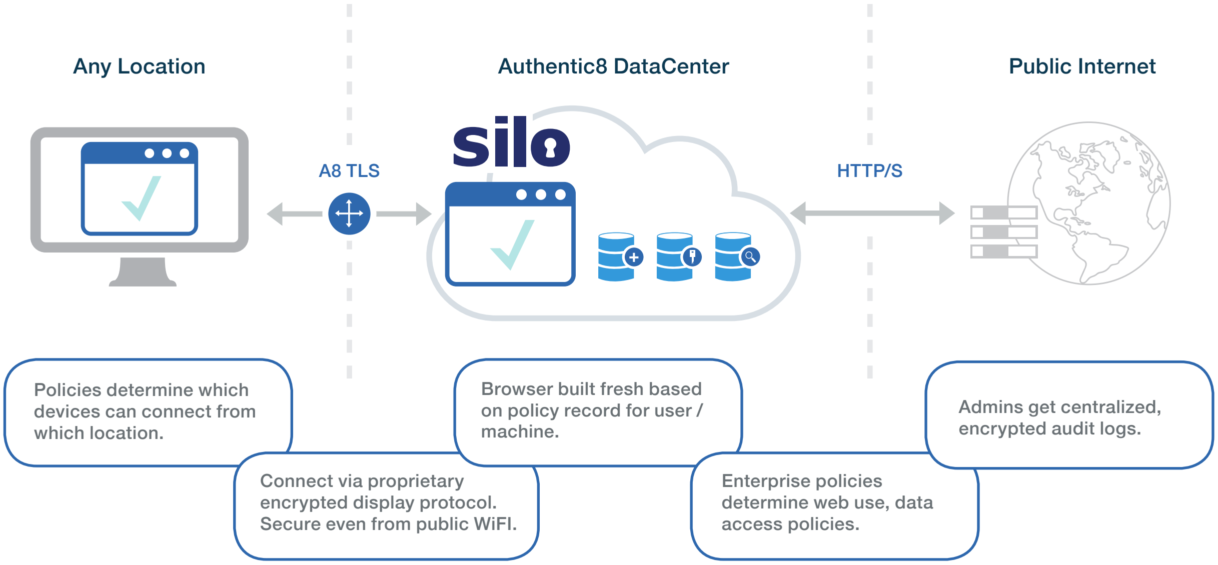
For buy side and sell side firms, Silo lets you determine how your users interact with the web — without the risk. It provides

- an easy way to allow users access to personal webmail, social media, and online storage.
- a secure way to browse the web and view and download attachments, completely free from the risk of embedded malicious code.
- a centralized panel to provision and manage access and user privileges across authorized cloud-based applications.
- comprehensive policies to enable or block key browser functionality like copy/paste as well as the ability to upload/download files, mitigating DLP risk.
- "Anytime, Anywhere" access — a single browser instance in the cloud keeps policies intact, regardless of where the users are located or which device they use to access the web.
- fully encrypted logs into all user activity during a web session and the ability to log it for centralized audit and compliance review.

READY FOR COMPLIANCE

Flexibility That Fits Your Firm's Specific Needs

Founded in 2010, Authentic8 pioneered the cloud browser. Built on a distributed cloud infrastructure, Silo protects commercial and government organizations around the world as they access the web. Our patents address the core configurability that organizations need to ensure the browser makes the web available without being compromised – by bad actors or employee mistakes. Firms deploy Silo with different policies and points of integration, based on firm policies and user roles.



Policies determine which devices can connect from which location.

Connect via proprietary encrypted display protocol. Secure even from public WiFI.

Browser built fresh based on policy record for user / machine.

Enterprise policies determine web use, data access policies.

Admins get centralized, encrypted audit logs.

LESS COMPLEXITY. LOWER COSTS.

Silo Saves Money

Any Information Officer, Compliance Officer, Security Officer or other risk-aware leader needs to ask how additional solutions make their organization more efficient. Firms can't continue investing in new tech and people to run it. The time has come for IT to gain leverage from their solutions, not more obligation.

Silo simplifies the IT stack in current organizations. When they remove the risk of the web, firms can make more rational technology decisions.

- **At the Endpoint:** if users never touch the public internet, 0-day exposure drops to near-zero. "Next Gen" A-V or sandboxing can be deprecated. Windows Defender is sufficient.
- **At the Network:** Firms are spending increasingly on break-inspect network infrastructure to supervise TLS connections. Deploying Silo allows firms to recoup 100% of these funds. Break-inspect infrastructure is not required.
- **At the Gateway:** The conditional white/black listing and disposition of sites is effectively eliminated. Silo includes full categorization and white/blacklisting capability. Customers allow internal sites at their firewall, and redirect all other sites to Silo.

And Silo reduces hard and soft costs. Authentic8's annual customer impact survey showed that our customers experienced a

- 53% reduction in time spent responding to security incidents
- 34% reduction in time spent managing exception requests
- 46% less time on log analysis and reporting
- At least 30% reduction in bandwidth consumption

FREQUENTLY ASKED QUESTIONS

Common Questions from Financial Services Firms

Silo executes all web code in an isolated cloud container. That frequently leads to questions about aspects of usability and corporate policy. Here are a few common questions and their answers.

What about performance?

Silo runs on high-performance servers over high capacity data links. Rendered data is compressed and converted, and delivered over a proprietary streaming protocol. While Silo is subject to the network integrity of the last mile to your organization, browser responsiveness is often better than local rendering. Try it for yourself!

Who controls my policies and configurations?

Authorized administrators control all configuration of the account profile. Administrator roles can be delegated and restricted at various nodes in the organizational structure. Varying levels of administrative permissions can be assigned based on the role of the user.

Does Authentic8 have access to our data?

We encourage our regulated customers to encrypt their log data with a public key they control. We do not touch customer data for any reason other than to comply with law enforcement. See www.authentic8.com/privacy-policy for more detail.

Can you abide by EU data privacy laws?

Authentic8's privacy controls fulfill the requirements of the European Union's Data Protection Directive (Directive 95/46/EC) and meet the requirements of the General Data Protection Regulation (GDPR). In addition to the inherent data controls, Silo can also be configured to limit access to specific geographies.

How does it fit in my existing infrastructure?

Silo's tight integration with your existing IT infrastructure and cybersecurity tools helps you protect and maximize existing investments and enables your firm to flexibly deploy the cloud browser for a broad range of use cases.

BACK IN CONTROL ON THE WEB.

Conclusion

In regulated investment firms, the local browser has become the compliance blind spot. Silo is a cloud-based browser that enables compliance and IT functions to take back control and ensure regulatory compliance, oversight, and security for users accessing the web. It provides a platform to centrally and comprehensively enforce policies, protect proprietary information and ensure anonymity when users go online, all while preserving user access and maximizing productivity.

www.Authentic8.com

COMPANY HISTORY

Authentic8 is a company with history rooted in another. Postini was founded in 1999 by the Authentic8 co-founder, and the core business and technology team were key Postini personnel. Postini pioneered the idea that a cloud-based service could solve security and compliance problems with email, and back in 1999 this was heresy. But the model won out.

Authentic8 was founded in 2010 around a different idea, but the parallels with Postini are many. The company addresses a real problem with an innovative approach. The thesis is simple: as business apps move to the cloud, the browser becomes more important than ever. Yet it's an unmanageable resource. Silo was conceived to change that.

We have headquarters and Federal Operations in California, Washington DC and Berlin Germany. For further content use web, email or phone (US, International).

[1] Among others, see Verizon Data Breach Investigation Reports 2014-2018 - https://enterprise.verizon.com/resources/reports/dbir/; also Adam Stone: When is the network not really the network? C4ISRNET - https://www.c4isrnet.com/show-reporter/disa-forecast-industry/2018/11/05/when-is-the-network-not-really-the-network-2/ (11/5/2018)

[2] Internet Live Stats - http://www.internetlivestats.com/total-number-of-websites/

[3] Symantec 2018 Internet Security Threat Report - http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf

[4] Accenture: 2017 Compliance Risk Study: Financial Services - https://www.accenture.com/us-en/insight-compliance-risk-study-2017-financial-services#search

[5] Cisco: 2018 Annual Cybersecurity Report - https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf

[6] Cisco: 2018 Annual Cybersecurity Report - https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf

[7] Cybersecurity Ventures: 2018 Market Report - https://cybersecurityventures.com/cybersecurity-market-report/