Cybersecurity Management

Intralinks Secure Document Exchange

Today's cybercriminals are bolder and more malicious and opportunistic than ever. Organizations are on hyperdrive to protect their IP and networks while adapting to increasingly complex regulatory requirements. Security and IT teams now need to regularly transmit confidential information for various purposes — to resolve and report security breaches, satisfy audits, respond to numerous authorities, and more. It's too dangerous and inefficient to rely on email or point solutions — that only risks more loss of data, customers, revenue and reputation.

Intralinks empowers CISOs, CIOs and CTOs to facilitate secure information sharing with internal and external collaborators and stakeholders including consultants, vendors, auditors, customers regulators, lawyers and federal and other authorities. Intralinks is the trusted partner for all types of companies that need to exchange confidential documentation for countless business purposes while navigating evolving data security challenges and regulatory demands.

Intralinks can help manage several cybersecurity-related processes, including:

INCIDENT RESPONSE

When a breach occurs or is suspected, IT security needs to investigate, document and resolve, and mitigate future incidents. This involves relaying confidential information securely and efficiently to lawyers, security consultants, law enforcement and more.

THIRD-PARTY PENETRATION TEST REPORTING

Results from these assessments may include details on issues and vulnerabilities that should not be exposed to the public (including competitors). Reports should be viewable, editable or downloadable only by those who are allowed to do so.

ONSITE AUDIT

Governance, risk and compliance (GRC) professionals need to gather numerous documents – policy statements, screenshots, log files, user guides, employee records and more – for internally or externally conducted audits. Given the sensitive nature of information, these documents as well as the audit results need to be centralized in a secure location.

SECURITY COLLATERAL AND DOCUMENTATION

GRC and IT security teams often collaborate on creating security collateral and documenting security activities. This can involve many types of files — documents, spreadsheets, PDFs, videos, photos, audio, etc. — which need to be centralized, secured, moderated and monitored.

SECURITY POLICIES AND PROCEDURES

The changing cybersecurity landscape requires corporate security procedures to keep evolving. New and updated policies and procedures must be restricted to select GRC professionals and collaborators as they are formulated. The ability to control information access at granular levels – who can view, edit, download, etc. – is extremely critical.

REMOTE AUDIT

Increasingly more common are assessments that involve digital transmission of security documentation to various external collaborators for remote review. This information needs to be secured and encrypted as it moves within and across the organization's firewall.

Why Intralinks for Cybersecurity Management

At Intralinks, security is at the heart of everything we do. Our multi-disciplinary security approach ensures our clients have the processes, controls and reporting required to safeguard their data and operations while exceeding regulations and reducing risk.

Independently verified and certified

More than 450 independent, client-led security audits and penetration tests of our data centers have been conducted since 2014. Numerous certifications are available to support regulatory and risk assessments.

Bank-grade security

Rely on multiple layers of protection at the data center, employee, product and individual file/document levels; two-factor authentication, SSO, DDoS protection and more.

Pioneer of the virtual data room (VDR)

Our 25+ year legacy in secure document sharing and VDRs means we have facilitated some of the most complex, high-value financial transactions.

Financial and operational security

Intralinks is backed by parent company SS&C, a USD 6 billion revenue company with a 30+ year history in fintech.

Intralinks Security Highlights

- Granular user permissioning
- Detailed compliance reporting
- Information rights management (IRM)
- Redaction – AI-assisted if needed
- Watermarking
- Encryption at-rest and in-transit (AES-256 bit)
- Single sign-on (SSO)
- Two-factor authentication
- Globally distributed architecture
- Enterprise security extensibility
- DDoS protection and web application firewall
- Secure DNS/website cloaking capabilities
- Assignable functional security control
- RTO in 5 hours
- ISO 27001: 2013; ISO 27701: 2019 ***the FIRST VDR provider****
- SOC-3; SOC-2 Type II (SAS 70 Type II) since 1999
- TISAX certified
- PCI DSS: SAQ-D attested
- GDPR, CCPA, HIPAA, FINRA, SEC, AICPA, FISMA, FDA 21 CFR Part 11, Ministry of Defense (UK) compliant
- SSAE 16/SOC 1/SOC 2 (US & UK); ISAE 3402 (UK)
- Privacy Shield certified
- 21 CFR Part 11 validated for electronic records
- MASS 201 CMR 17.00
- European Data Protection Directive 95/46/EC certified
- NQA certified
- ANAB accredited

Trust our brand, service and the security we consistently deliver.

USD 35 trillion+

worth of sensitive, high-value transactions were facilitated by Intralinks in the last 25+ years

6.6M+ professionals

use Intralinks for capital markets transactions and regulatory compliance

857K firms in 147 countries and 76 industries

including all of the major banks and many of the Fortune 1000 trust Intralinks

Contact us for more information at **intralinks.com/contact**