DFIN

Arc Suite

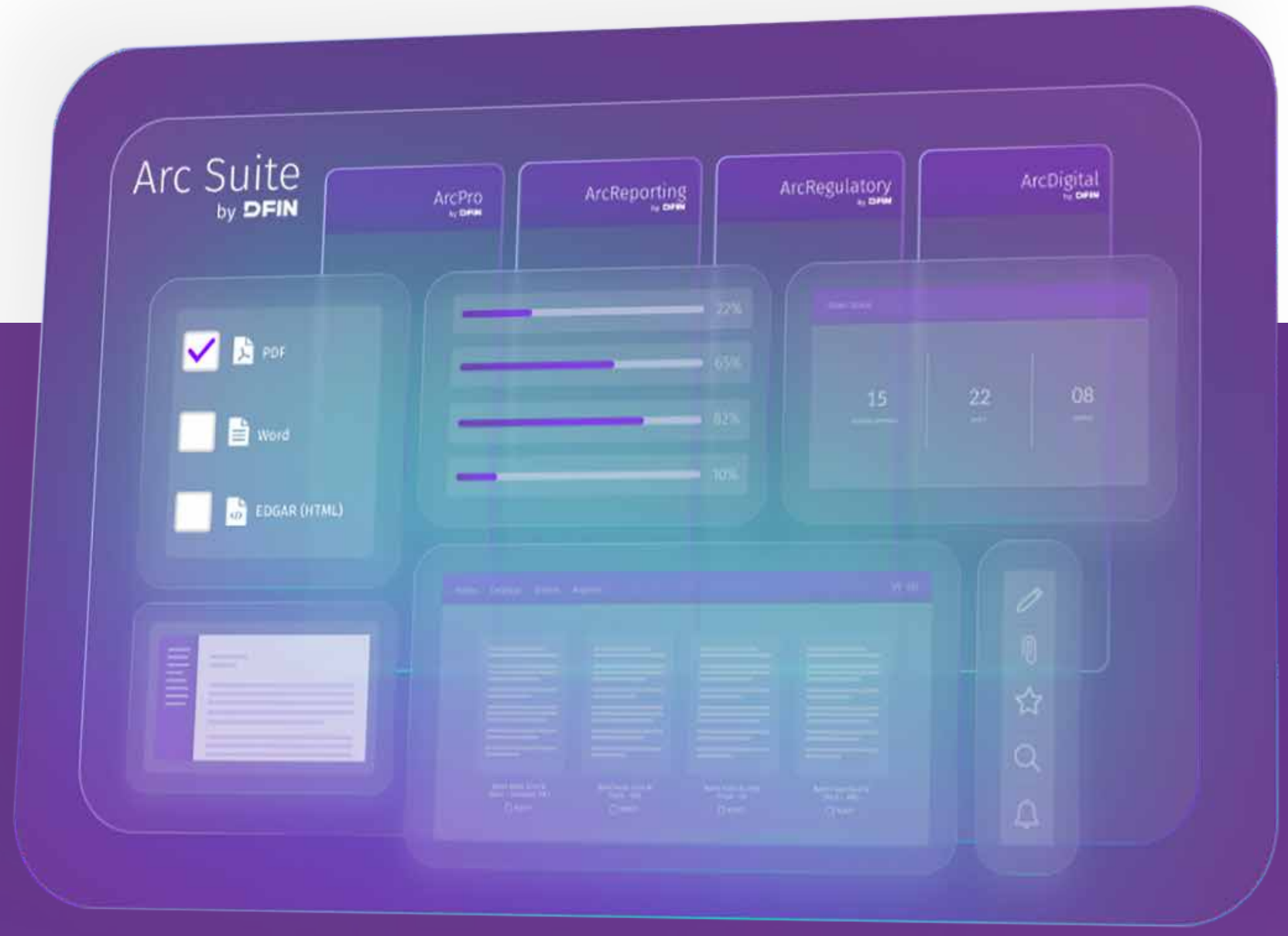
by DFIN

Product Security Overview

Arc Suite. Four purpose-built products. One powerful end-to-end solution.

DFIN's Arc Suite consisting of four innovative products – ArcPro, ArcReporting, ArcDigital and ArcRegulatory – supports the full range of front, middle and back office operations with cloud-based proprietary tools to keep you ahead of evolving global regulatory deadlines and guidelines.
As the leading global risk and compliance solutions provider, DFIN is the only company to o¬ffer regulatory, reporting, legal, filing and distribution solutions through one integrated platform. We provide the financial industry with the experience and expertise of an established market leader.

The following information provides a high-level overview of DFIN security measures in place for Arc Suite products.



DFIN'S CYBERSECURITY OVERVIEW

The **DFIN Information Security Program** is designed to ensure data protection, enterprise cybersecurity, and supply chain security throughout the environment. The program is based on business requirements derived from:

Assessing

security risks to the organization.

Complying

with the legal, statutory, regulatory, and contract requirements that DFIN and its business partners, contractors, and service providers must satisfy.

Delineating

the principles and objectives for operational information processing.

Information Security for Arc Suite products is achieved by implementing a set of controls, which consist of policies, processes, procedures, organizational structures, and software functions.

Controls have been established to minimize risk and protect information assets required to meet the operational, financial, and regulatory requirements to safeguard client data and privacy. Information security is characterized as the preservation of:

SECURITY

to protect assets from external and internal threats

AVAILABILITY

to prevent disruption of service and productivity

CONFIDENTIALITY

to prevent unauthorized disclosure of sensitive information

CONTROLS APPLIED TO OUR PRODUCTS

Organizational Controls

DFIN's robust organizational controls ensure that security is addressed as a part of all software development at DFIN by integrating security practices and generating security and compliance artifacts throughout the process. The **advantages** in doing so are:

- Reduction in vulnerabilities, malicious code, and other security issues.
- Mitigation of potential impacts of vulnerability exploitation through the product's lifecycle.
- Evaluation of root causes for vulnerabilities to avoid future occurrences.

DFIN leverages independent SOC2 Type II auditing and reporting, internal audit, an expert-staffed Security Operations Center (SOC), Governance, Risk and Compliance team and a security awareness program with training for DFIN staff to ensure application and data security.

Secure Software Development Life Cycle (S-SDLC), Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), secure software release management, and vulnerability management help to ensure Venue application security.

From an accountability perspective, security awareness, data privacy, ethics, and code of conduct are instilled into DFIN team members.

DFIN Security Team

- Led by Dannie Combs – SVP, Chief Information Security Officer
- Enterprise Security team supporting Security Incident and Response, Application Security, Network Security and Security Governance, Risk and Compliance, further supporting:
  - The use of security tools and utilities to scan and monitor DFIN assets
  - In-house Cyber Defense team complimented by retained third-party cybersecurity services
  - Policy management – comprehensive policies including Information Security Policy and Security Awareness annual employee training
  - Security monitoring and logging
  - Cybersecurity incident response

Application Development

- Code reviews are performed multiple times throughout the development process
- Rigorous QA testing process in place to identify potential issues early in the development process including SAST and DAST testing
- DFIN embraces modern SDLC and Continuous Integration/Continuous Deployment best practices aligned to a multi-environment (integration, Quality Assurance, Staging and Production) release promotion process

Infrastructure

- Comprehensive Network & Infrastructure Security controls are in place (firewalls, IDS & IPS, logging, and security monitoring)
- Regular network and server vulnerability scans
- Regular OS patching (Microsoft security patches are applied each month)
- Regular backup schedule
- Hosted via a mix of both Microsoft Azure and on premise

Penetration Testing

- Annual 3rd party Penetration Testing
- Findings are reviewed and remediated according to DFIN policy
- 3rd party is brought back to validate that the remediation was effective
- Executive Summary Report is available for customer review

Incident Response

- Incident response plans are routinely tested through live simulations and tabletop exercises
- We employ a team of in-house Cyber Threat Analysts who investigate anomalies and conduct “red team” “hunts” proactively seeking out vulnerabilities
- DFIN partners with leading cybersecurity incident response and advisory services firms as needed to ensure we are well-positioned to quickly identify, respond, contain, and recover from a cybersecurity incident

Endpoint Security

- Endpoint Protection & Response and Next-Generation Antivirus technologies protect DFIN’s servers as well as the workstations used by our associates as they process client data. These advanced endpoint technologies help to:
  - Detect and prevent malware and fileless non-malware attacks (which is a critical [but not sole] capability to reduce the risk of ransomware)
  - Protect against new and emerging threats to include memory-based attacks, PowerShell exploits, and more
  - Enable DFIN Cyber Defense rapidly and systematically isolate systems of interest away from all other DFIN assets

Security Operations Center

- DFIN's Security Operations Center provides advanced security monitoring capabilities:
  - Whether on-prem or hosted in the Cloud, DFIN system logs are aggregated, correlated, and monitored 24x7x365. Anomalies are alarmed and thoroughly investigated
  - Our monitoring platform Identifies malicious behavior and TTPs (Tactics, Techniques, and Procedures) known to be used by threat actors
  - Our Cyber Defense team monitors connections into DFIN's VPN, Azure instances, and other critical services that may originate from high-risk ISPs and/or geographic

AT101 SOC2 Audit

- Annual SOC2 Type II audit conducted for DFIN Global Capital Markets Observation period runs May 1st through October 31st
- Continuous control framework assessments are conducted by DFIN Governance Risk and Compliance team

DFIN Protect

- The DFIN Protect Program ensures our associates are provided timely, relevant security awareness training:
  - Enterprise communications routinely sent addressing topics that range from timely threat advisories to cybersecurity best practices
  - Phishing Simulation campaigns are conducted no less than monthly | Results are reported to Executive Management
  - Topical security awareness training target today's cyber threats, to include Phishing Awareness, Social Engineering, and more

Arc Suite

by DFIN

In Summary

DFIN understands the importance of maintaining comprehensive and robust Information Security Program that spans network, system, application, and data security singularly focused on safeguarding our products and our client's data. DFIN aims to be a trusted partner to our clients.

CONTACT US

dfin@dfinsolutions.com
+1 800 823 5304