

# Why Automation Needs Accountability

How Jitterbit layers security, governance and compliance throughout the Harmony platform

## Is Your Security Keeping Up With Technology?



80%

IT leaders who say AI integration vulnerabilities are a top security concern<sup>1</sup>



32%

of orgs admit not prioritizing security over convenience<sup>2</sup>



"[We] observed adversaries leveraging access to cloud-based SaaS applications to facilitate lateral movement, extortion and downstream targeting of third parties."<sup>3</sup> — CrowdStrike



31%

of orgs experienced former employees accessing SaaS apps/data<sup>4</sup>



ONLY 38%

orgs that say they're effectively securing their cloud resources<sup>5</sup>



"Credentials are the #1 way attackers gain access to systems."<sup>6</sup> — 1Password



42%

SaaS apps that are "shadow IT"<sup>7</sup>

\$4.4M

global average cost of a data breach<sup>8</sup>

## Three Key Security Layers

Based on NIST, CISA, CSA, and CERT recommendations, Jitterbit's security framework consists of:

### 1. Logical Security

Security measures taken within the Harmony platform

MFA ●	WAF	Access Control	IDS & IPS	Secure Database
DDoS Monitoring & Mitigation ▲	FIPS 140-2 Auth ■	SSO	E2E Encryption	

- Increases the security of an account by 99%<sup>9</sup>
- ▲ DDoS attacks up >350% YoY in Q1 '25<sup>10</sup>
- Companies with full encryption strategies experience 42% lower data breach costs<sup>11</sup>

### 2. Logical Security

Internal policies and operational best practices

Personal Policy	Penetration Testing ●	OWASP Checks ▲	SSO
FIPS 140-2 Auth	Secure SDLC ■	E2E Encryption	

- Testing on Application, Product & Network Levels
- ▲ Vulnerabilities regularly checked for and mitigation prioritized
- Security practices built into each phase of development lifecycle

### 3. Physical Security

The secure hosting of Harmony on cloud infrastructure

Intrusion Detection	Video Surveillance	Secure Cloud Redundancy ▲	Biometric Controls
---------------------	--------------------	---------------------------	--------------------

- ▲ Harmony features multi-region replication across 3 geographically distinct clouds, with each availability zone an independent failure zone. It can tolerate natural disasters, system failures and more without shutdown.

## Our Security Is Certified ...



Jitterbit has earned an industry-first ISO 42001 certification for AI that is designed, developed and deployed responsibly across the full automation lifecycle. [Learn more about ISO 42001 here.](#)

## ... And Compliant.

The Jitterbit Harmony platform meets the highest global security standards, and is accredited by/certified compliant with the following standards:



For an in-depth look into our industry-leading security, visit the dedicated [Jitterbit security page](#).

#### Sources:

- Jitterbit 2025 Automation Benchmark Report
- EntryCare – Access Control Statistics: Trends & Insights
- CrowdStrike 2025 Global Threat Report
- Security Magazine – Thirty-one percent of former employees still have company SaaS access
- Artic Wolf – The State of Cybersecurity 2023 Trends
- 1Password – Single sign-on isn't enough: closing the SSO security gap
- Josys – Shadow IT Definition: 2024 Statistics and Solutions
- IBM Cost of a Data Breach Report 2025
- National Cybersecurity Alliance – What is Multifactor Authentication (MFA) and Why Should You Use It?
- Cloudflare DDoS Threat Report
- IBM Cost of a Data Breach Report 2025