IDC [Quanta]

SECURITY OVERVIEW

What your security team needs to know

Security teams need more than promises – they need architecture, controls, and evidence. IDC Quanta is designed to meet the demands of the most rigorous security review processes.

IDC core security commitments

1. **Your data is never used to train AI**
   Customer data is never used to train any AI model – IDC's or any third party's.
2. **End-to-end encryption**
   AES-256 at rest with AWS KMS-managed keys, TLS 1.3 in transit. Keys managed through a dedicated key management service.
3. **Secure document ingestion**
   Every upload passes malware scanning and prompt-injection detection before it reaches the AI model.
4. **Tenant isolation**
   Enforced through application-layer controls and access policies. Your data cannot bleed into another organization's environment.

Infrastructure & availability

Hosting: AWS (primary, Bedrock for AI) + Azure (AI services) + Snowflake (data)

Uptime: Designed for high availability and resilience

Residency: US-based infrastructure; regional compliance via contractual mechanisms (DPAs, SCCs)

Testing: Annual 3rd-party pen test + continuous vulnerability scanning (Nessus Tenable, Straiker.ai)

BC/DR (Business Continuity / Disaster Recovery): Business continuity plan in place; Druva SaaS backup & disaster recovery

BITSIGHT SECURITY RATING

800

/ 250–900 scale as of July 1, 2026

Compliance status

Framework	Status
GDPR	Compliant
CCPA	Compliant
SOC 2 Type I [1]	Compliant
ISO 27001:2022	In progress
EcoVadis 2025 (ESG)	Bronze level

[1] *SOC 2 Type II certification in progress*

Partner certifications

Infrastructure partners – all active

AWS: SOC 1/2/3, ISO 27001

Azure: SOC 2, ISO 27001/27017/27018, EU Data Boundary

Snowflake: SOC 2 Type II, ISO 27001, PCI DSS

FrontEgg, Langfuse, Datadog, Grafana, Sumo Logic: SOC 2 (each)

Data ownership

Customers retain ownership of their data – there is no transfer of your background IP rights to IDC. Staff access is strictly limited, logged, and audited.

Customers may request deletion of their data at any time.

Access & identity controls

SSO: SAML 2.0 / OIDC – Okta, Azure AD, Google Workspace

MFA: Enforceable org-wide (TOTP + SSO-driven)

Audit logs: All user activity captured and reviewable

Zero trust security stack

24 vendors · 11 domains · 360° coverage

Human risk Adaptive Security	**Backup & recovery** Druva	**Monitoring & SOC** Sumo Logic, 7AI (24/7 MDR)	**GRC & compliance** Drata
Data classification M365	**Identity & access** Entra ID, AWS IAM	**Network security** Zscaler, CheckPoint, Meraki	**Cloud security** Orca, GuardDuty
Endpoint protection SentinelOne, JAMF, Intune, Automox	**Risk & exposure** Qualys, Axonius, CyCognito, BitSight	**Run-time protection** Azure & AWS Bedrock Guardrails, Straiker.ai	

Need help?

Self-serve certs, policies & reports: trust.idc.com

Email IDC Security questions to: cybercompliance@idc.com