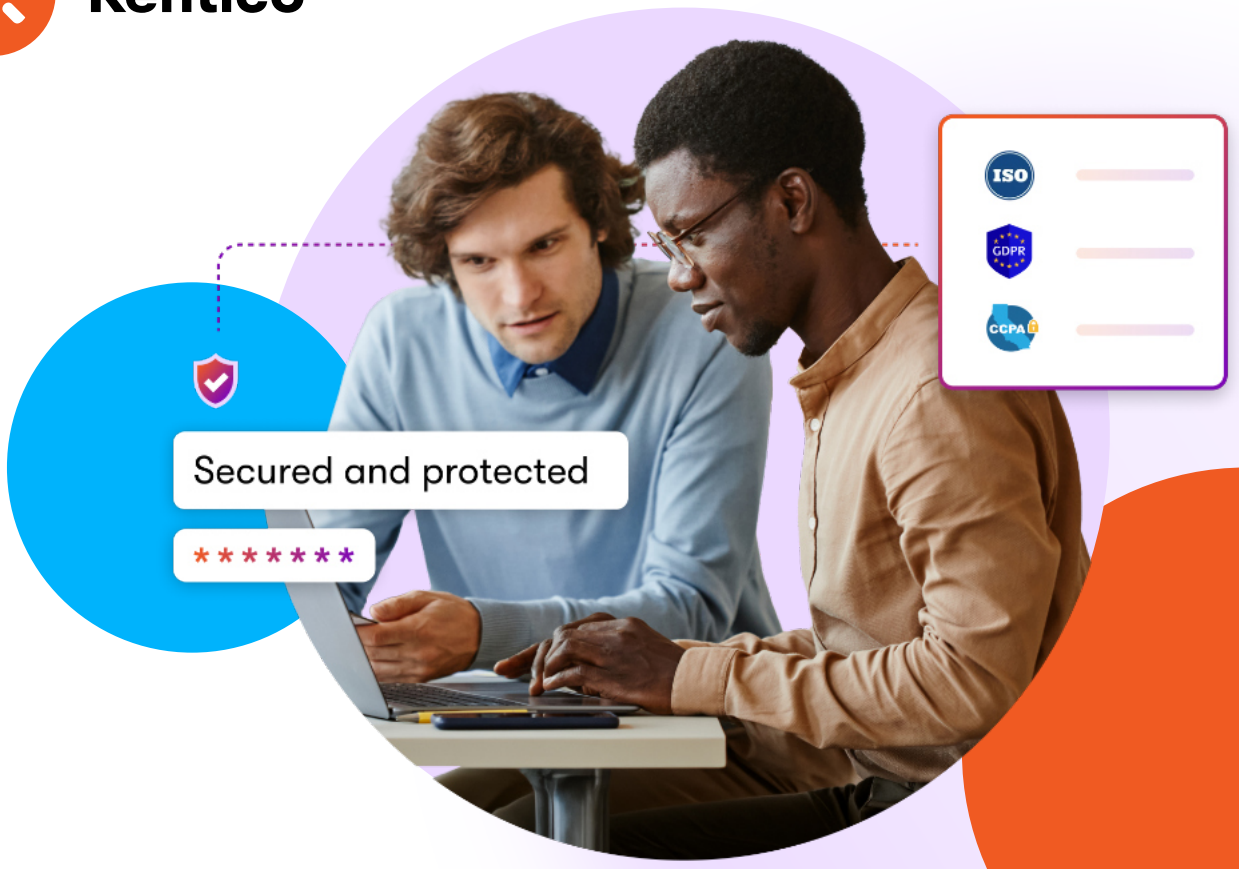
Kentico



Ebook

Security First Marketing.

A 2026 guide to protecting your MarTech ecosystem, including AI

kentico.com

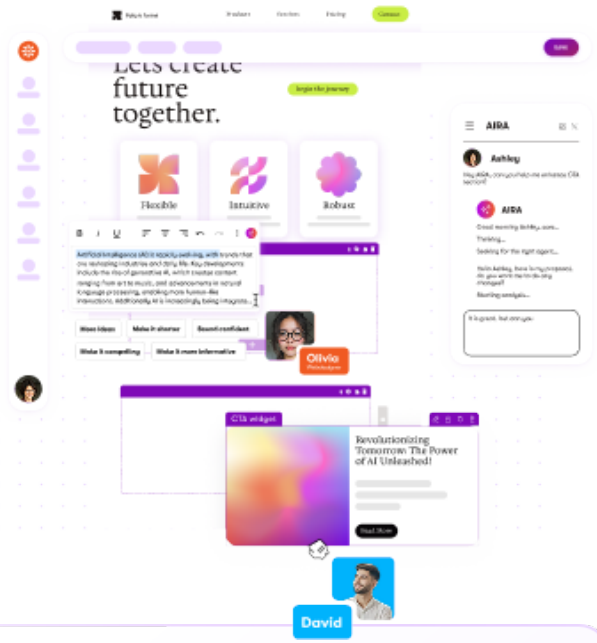
What's Inside.

Why It Matters.

Marketing teams in 2026 hold more customer data and use more tools than ever, and a new risk has joined the familiar list: ungoverned AI.

When a marketer pastes customer data into a public AI chatbot to write campaign copy, that data may leave your jurisdiction, be logged by the AI provider, or violate GDPR. This isn't a hypothetical. It's happening to marketing teams everywhere.

Security is no longer just an IT concern. It's a trust signal, and trust is what every marketer is ultimately selling.



The Risks in Your Stack.

Unauthorized access
Over-provisioned users, weak permissions, and outdated roles can give the wrong people access to sensitive customer data, campaign systems, or publishing tools.

Third-party and integration risk
Your martech stack depends on vendors, plug-ins, APIs, and connected platforms. If one integration is vulnerable, your customer data and digital experience may be exposed.

Shadow AI
When teams use unmanaged AI tools with customer data, campaign plans, or proprietary content, that information can leave your approved security environment without visibility or control.

Human error
Most breaches still involve people a misconfigured form, the wrong file shared externally, an accidental upload, or sensitive data pasted into the wrong tool.

Data leakage
Unsecured APIs, misconfigured permissions, and disconnected systems can quietly expose customer data long before anyone notices.

Compliance exposure
Privacy regulations such as GDPR make data protection a business-critical issue. Non-compliance is not just a legal concern it can damage revenue, reputation, and customer confidence.

“Security is often an implicit expectation everyone wants a secure solution, but specific requirements are rarely defined.”

Matěj Groman.
Security Specialist, Kentico

The 10-Control Security Checklist for Marketing Teams.

Marketing teams now manage customer data across dozens of platforms, integrations, AI tools, and campaign systems. This checklist is designed to help marketing and IT teams quickly identify gaps that could expose customer data, disrupt operations, create compliance risks, or damage brand trust. Even a single weak point, an unmanaged AI tool, outdated permissions, or unsecured API can create risk across your entire MarTech ecosystem.

Use this checklist quarterly with your IT and security teams to validate that the fundamentals are in place.

1.	Data encryption	**AES-256 at rest, TLS 1.2+ in transit, OAuth 2.0 on APIs.** Protects customer and business data both in storage and while moving between systems
2.	RBAC & least privilege	**Every user has access to exactly what their role requires, no more.** Ensures employees and partners only have access to the systems and data required for their role.
3.	MFA & SSO	**Multi-factor auth enforced; SSO via enterprise IdP (e.g. Azure AD).** Reduces the risk of compromised passwords leading to unauthorized access.
4.	Vendor vetting	**Security certifications reviewed before any integration is onboarded.** Reduces the risk of data breaches and other vulnerabilities.
5.	AI tool governance	**All AI tools inventoried; data stays inside your approved environment.** Keeps customer, campaign, and proprietary data inside approved and governed AI environments.
6.	Incident response plan	**Written, tested procedure. All team members know who to call.** Ensures teams can respond quickly and minimize disruption if a security event occurs.
7.	Security training	**Phishing, social engineering, and shadow AI awareness, annual minimum.** Helps employees recognize phishing attempts, social engineering, and unsafe AI usage before mistakes happen.
8.	API security	**Authenticated connections with rate limiting, logging, and anomaly alerts.** Protects customer data flowing between platforms and integrations.
9.	Penetration testing	**External pen test within last 12 months. Findings tracked and patched.** Identifies vulnerabilities before attackers do and validates that security controls are working effectively
10.	Data minimisation	**Only necessary data collected; automated retention and deletion active.** Reduces compliance and exposure risk by collecting and retaining only the data you truly need.

AI Governance for Marketers.

Using AIRA & the Agentic Marketing Suite responsibly.

Not all AI tools are built the same. Many consumer AI platforms process data outside your organization's approved environment, potentially storing prompts, logging inputs, or using submitted content for model training.

For marketing teams handling customer, campaign, and business data, that creates real compliance, privacy, and governance concerns.

AIRA, Kentico's built-in AI, was designed differently.

Runs within your environment
Powered through Microsoft Azure and operating within your Kentico ecosystem.

Governed by your permissions
AIRA only accesses content and data users are already authorized to see through RBAC controls.

No external AI training on your content
Your customer and business data is not used to train public AI models.

Auditable and traceable
AI-assisted actions remain visible and trackable for governance and compliance oversight.

Human-led decision making
AI helps accelerate workflows, but marketers remain in full control of approvals, publishing, and customer-facing decisions.

The Agentic Marketing Suite extends these capabilities with specialized AI agents for content strategy, customer journey optimization, campaign management, SEO & GEO analysis, and experimentation; all operating within your governed platform environment.

"Security is at the core of everything we do. We embed it into our development lifecycle, run external pen tests, and operate a bug-bounty program."

Matěj Groman.
Security Specialist, Kentico

XPERIENCE BY KENTICO: BUILT-IN SECURITY

What's included on day one

- AES-256 encryption at rest, TLS 1.2+ in transit
- SSO + MFA via Azure AD and enterprise IdPs
- RBAC, Workspaces, and Page ACLs for granular access
- OAuth 2.0 + OpenID Connect for secure API integrations
- GDPR & CCPA consent and data deletion tools
- ISO 27001 & SOC 2 Type II certified (SaaS)
- Automated zero-downtime security patches
- Continuous threat monitoring
- Instant restore + automatic backups (SaaS)
- AIRA AI: governed, auditable, inside your environment

5 Questions to Ask Before Deploying Any AI Tool:

Before introducing any AI solution into your marketing operations, make sure your team can clearly answer these five questions:

1. **Does our data remain inside approved and governed environments?**

   Understand where customer and business data is processed, stored, and retained.

2. **Is AI activity logged and auditable?**

   Teams should be able to trace AI-assisted actions for governance, compliance, and operational oversight.

3. **Can we control what data the AI can access?**

   AI tools should align with existing user permissions, RBAC policies, and security controls.

4. **Does the platform support compliance requirements?**

   Ensure the solution aligns with regulations such as GDPR, CCPA, and any industry-specific standards your organization follows.

5. **Is there human oversight before customer-facing actions occur?**

   AI should accelerate marketing workflows not replace accountability, approvals, or final decision-making.

The right AI tools should help your team move faster while strengthening governance, transparency, and customer trust.

Kentico

Compliance Map.

Standard	What it Protects	Kentico
ISO 27001	Info security governance and operational controls	Kentico SaaS certified
SOC 2 Type II	Platform security, availability and operational reliability	Kentico SaaS certified
GDPR	Customer privacy rights and personal data protection in the EU	Built-in consent, deletion workflows
CCPA	Consumer privacy and data management requirements in California	Opt-out & deletion request support
HIPAA	Protection of sensitive healthcare and patient-related data	Supported on self-hosted deployments
OWASP Top 10	Common Web application and API security risks	Aligned in Kentico development lifecycle

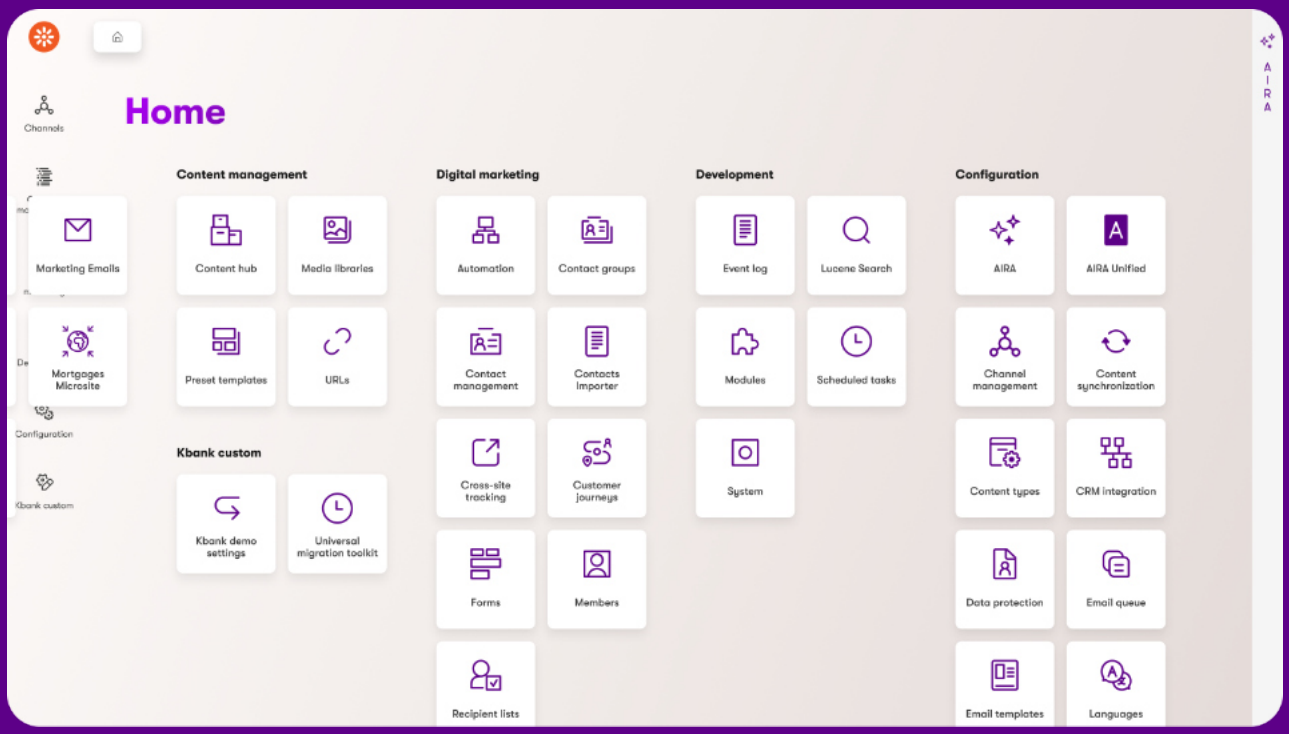
Key Takeaways.

- AI governance matters. Every AI tool your team uses should operate within approved, auditable, and secure environments.
- Most security incidents are not caused by sophisticated attacks; they come from weak processes, misconfigured systems, unmanaged integrations, and human error.
- A fragmented MarTech stack increases operational and security risk. Unified platforms help reduce complexity, improve visibility, and strengthen governance.
- Security and compliance should be continuous operational disciplines, not annual checklist exercises.
- The strongest marketing organizations are building teams, workflows, and technology ecosystems that are secure, governed, AI-ready, and built to scale customer trust.

Ready to strengthen your MarTech security? Talk to a Kentico expert →

About Kentico.

Kentico is a content management system with built-in digital marketing, native commerce, and AI agentic capabilities that help deliver personalized customer experiences through websites, microsites, emails, apps, digital kiosks, and other channels. It replaces multiple disconnected tools with a unified solution that reduces technology complexity and improves team productivity.



Empower your team to create engaging experiences while eliminating time-consuming tasks with a comprehensive platform that is easy to learn and use, powered by built-in AI agentic capabilities that streamline marketing workflows. Tailor content, commerce experiences, and delivery to individual preferences and develop consistent interactions across multiple digital touchpoints, reaching your customers on their favorite channels, anytime, anywhere. Kentico consolidates multichannel content management, digital marketing, and commerce capabilities in a single solution, your team achieve more with fewer processes and less technology.

H.Q
Kentico software s.r.o.
Nové sady 996/25
602 00 Brno
Czech Republic

CZ
Kentico software s.r.o.
FLEKSI BETA
Beta Building
Vyskocilova 1481/4
140 00 Praha 4-Michle

US
Kentico Software, LLC
15 Constitution Drive,
Suite 2C
Bedford, NH 03110
United States

UK
Kentico Software Ltd
One London Square
Cross Lanes
Guildford, Surrey,
GU1 1UN
United Kingdom

APAC
Kentico Software Pty Ltd.
83 Mount St, Level 4
North Sydney, NSW 2060
Australia

Germany
Kentico Software GmbH
c/o Schnorbus Helmhold
Wardemann PartGmbB
Kanalstraße 2
41460 Neuss

kentico.com