Kentico


Ebook

# Security-first marketing.

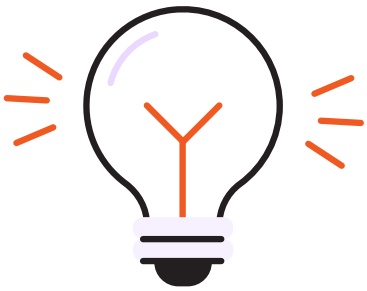
## A guide to protecting your MarTech ecosystem

kentico.com

# Table of contents.

In our fast-evolving digital world, marketing and technology are inseparable. Businesses rely on sophisticated MarTech ecosystems to engage customers, personalize experiences, and drive growth. However, as the number of marketing tools and integrations increases, so do security vulnerabilities. Cyberattacks, data breaches, and compliance failures pose significant risks—not just to IT teams but to marketers handling customer data daily.

This guide explores the critical security challenges in MarTech, outlines best practices for securing your stack, and highlights how choosing the right technologies can protect your business. By adopting a security-first approach, you can safeguard customer trust, ensure compliance, and reduce risks—without slowing down innovation.



Did you know?

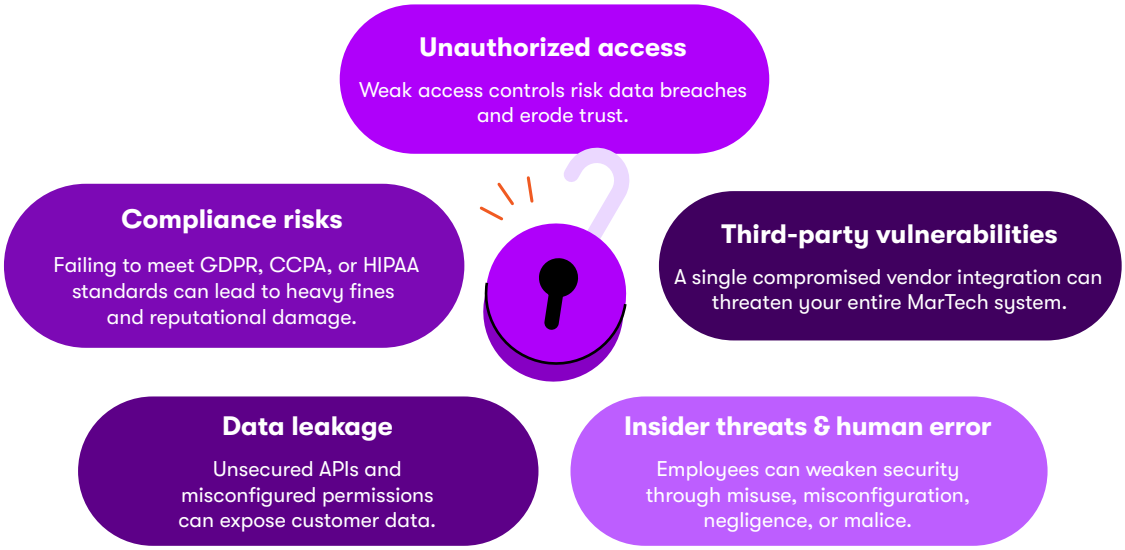
- Under GDPR, failing to erase customer data on request can cost up to €20M or 4% of global revenue. (IT Governance)
- The average company has more than a half a million sensitive files, over 100,000 of which are accessible by every employee. (Varonis)

# Understanding security risks in the MarTech ecosystem.

The MarTech ecosystem is the backbone of modern marketing, powering everything from customer relationship management (CRM) and automation tools to analytics platforms and customer data hubs.

These systems help businesses personalize experiences, optimize campaigns, and drive growth. But they also present a growing security challenge—each tool, integration, and data flow is a potential entry point for cyber threats.

Understanding these risks is the first step in securing your MarTech ecosystem.




**Next, we'll cover best practices to safeguard your systems and data.**

> ***While security might seem like just another box to tick in procurement, its true impact becomes evident when issues arise. At Kentico, we prioritize security not just because of compliance requirements, but as an ongoing commitment—aligning with industry standards like NIST and OWASP while guiding customers toward best practices that keep their platforms resilient in the long run.”***

**Matěj Groman.**
Security Specialist, at Kentico

# Best practices for securing your MarTech stack.

Securing your MarTech ecosystem requires a proactive approach. From protecting customer data to managing third-party risks, these best practices will help safeguard your business against cyber threats.

### Data protection & privacy

- Use encryption to protect sensitive data from unauthorized access, both in transit and at rest.
- Minimize data collection—gather only what's necessary to reduce exposure risks, and automatically remove unnecessary or outdated data on a regular basis.
- Conduct regular audits to review security measures, check for vulnerabilities, and ensure compliance with regulations like GDPR and CCPA.

**Encryption** – A method of scrambling data so only authorized users can read it.

**Data in transit** – while being sent or received.

**Data at rest** – when stored in databases or cloud systems.

**GDPR, CCPA** – data privacy laws that protect personal data, giving users control and requiring business transparency.

## Access management & authentication

- Use Role-Based Access Control (RBAC) to limit data access based on job roles.
- Enforce Multi-Factor Authentication (MFA) for employees and third-parties.
- Secure API connections by restricting access, monitoring usage, and using industry-standard authentication methods.

**RBAC:** A method of restricting system access based on roles within the organization.

**MFA:** A security method requiring two or more verification factors (e.g., own password + one-time code).

**API:** A feature that enables different software tools to communicate.

## Network & infrastructure security

- Protect cloud-based MarTech tools with encryption, access controls, and security monitoring.
- Deploy firewalls, endpoint security, and VPNs to safeguard remote work environments.
- Regularly conduct penetration testing to detect and fix security gaps before attackers do.
- Ensure the infrastructure is up to date and configured to meet your security standards.
- Regularly perform disaster recovery drills to prepare for disruptions and security incidents.
- Configure a robust backup solution to ensure you can recover from data loss.

**Firewall** – A security barrier that blocks unauthorized access to a network.

**Endpoint security** – Protection for individual devices against cyber threats.

**VPN** (Virtual Private Network) – A tool that encrypts internet connections for secure remote access.

**Penetration testing** – A simulated cyberattack used to find and fix security weaknesses.

**Disaster recovery drill** – A simulation of responses to cyberattacks or system failures to ensure preparedness and minimize downtime.

## Email & communication security

- Implement DMARC, SPF, and DKIM to prevent email spoofing and domain impersonation.
- Use secure collaboration tools with strong access controls.

**DMARC, SPF, DKIM** – Email security protocols that prevent fraud and domain spoofing.

**Spoofing** – Faking an email, website, or phone number to deceive users.

**Domain impersonation** – Creating a fake version of a trusted domain to steal data.

## Third-party risk management

- Vet all MarTech vendors for security compliance before integrating their tools.
- Ensure third-party services follow best practices, including data encryption and regular updates.
- Include data protection clauses in vendor agreements to enforce security standards.

**Data protection clauses** – Legal terms in vendor contracts that define how data is stored, processed, and secured to ensure compliance and minimize risk.

### Educate on security threats

- Train teams on phishing, social engineering, spoofing, domain impersonation, and malware.
- Ensure everyone understands their role in preventing breaches.
- Simulate incidents to test responses.
- Encourage unique, secure passwords and good password hygiene.
- Make it easy for employees to report suspicious activity.

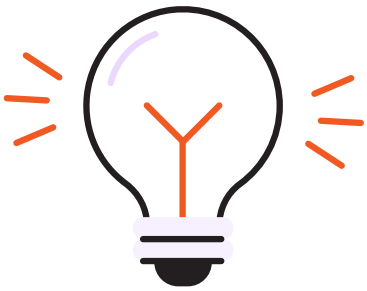
**Phishing** – A cyberattack where criminals impersonate legitimate sources to steal data.

**Social engineering** – Manipulating people into revealing confidential information through deception.

**Password hygiene** – Creating and regularly updating strong, unique passwords to protect against unauthorized access.

**Report suspicious activity** – to the IT/Security Team or your Security or Compliance Officer.

By integrating these best practices into your security strategy, you'll strengthen your stack and reduce the risk of cyber threats.



## Did you know?

- 82% of breaches involve human error. From stolen credentials and phishing to misuse and mistakes, people are a major factor in security incidents. (Verizon)
- 94% of organizations agree that customers won't buy from them if they don't believe personal data is properly secured. (Cisco 2024)

> ***Security is often an implicit expectation—everyone wants a secure solution, but specific requirements are rarely defined. Many follow security guidelines because regulations or company policies demand it, rather than from a clear understanding of their own security needs.”***

**Matěj Groman.**
Security Specialist, at Kentico

# Choosing the right technologies to ensure security.

Security isn't just an IT responsibility—it's a shared one. As marketers handle growing amounts of customer data, manage an increasing number of tools, and rely on automation, the risk of security gaps grows. Many marketers are using 10-20 different tools to meet the demands of modern marketing—each tool serving a specific function like email campaigns, analytics, or customer engagement. However, this leads to fragmented systems, data silos, and increased vulnerability. When tools are added quickly to meet customer expectations or hit KPIs, without proper security checks, critical gaps can easily form.

In this section, we'll discuss how to evaluate MarTech solutions with security in mind. Prioritize security-first platforms that protect customer data, reduce complexity, and ensure smooth, secure operations across your tech stack. By choosing the right tools and ensuring proper integration, you can safeguard your systems, reduce security risks, and maintain compliance.

# Here are the key areas to assess:

## 1. Data protection & encryption

a. **End-to-end encryption** – Encrypts data at rest and in transit (AES-256 for stored data, TLS 1.2+ for transmitted data).

b. **Secure API connections** – APIs should use OAuth 2.0, API keys, and rate limiting to prevent unauthorized access.

c. **Data anonymization & masking** – Protects sensitive customer data from exposure.

## 2. Access control & user security

a. **Role-Based Access Control (RBAC)** – Ensures users only access data relevant to their role.

b. **Multi-Factor Authentication (MFA)** – Requires extra authentication steps to prevent unauthorized logins.

c. **Single Sign-On (SSO) Integration** – Allows secure login across platforms with enterprise identity providers, (e.g. Microsoft Azure).

## 3. Compliance & certifications

(Especially important for regulated industries)

a. **SOC 2 Type II** – Ensures the vendor follows strong data security and privacy practices.

b. **ISO 27001** – Global standard for information security management.

c. **GDPR, CCPA, HIPAA Compliance** – Essential for handling customer data legally.

d. **Data processing agreement (DPA)** – Defines how the vendor processes and protects your data.

## 4. Security monitoring & incident response

a. **Audit logs & activity monitoring** – Tracks who accessed what data and when.

b. **Security information and event management (SIEM) integration** – Detects and responds to security threats.

c. **Automated threat detection & anomaly monitoring** – Uses AI or automation to flag suspicious activity.

## 5. Third-party risk & integrations

a. **Vendor security transparency** – Vendors should provide security policies, encryption details, and compliance reports.

b. **Secure third-party integrations** – Requires strong API authentication, least-privilege access, and integration monitoring.

c. **Regular security updates & patching** – Ensures ongoing protection against vulnerabilities.

! Not all security features come built-in. While certain platforms provide a strong foundation, achieving the right level of protection often requires customization, configuration, or additional development work.

- Built-in security is a starting point—evaluate encryption, access controls, and compliance support.
- Customization may be required for advanced protections like API security, monitoring, and authentication.
- IT and security teams should be involved to configure and maintain the best security posture.

**Bottom Line:** A secure platform is a big plus, but true security requires ongoing implementation, monitoring, and adaptation.

By understanding and applying these security principles, marketers can help protect customer data, maintain compliance, and prevent costly cyber threats—without slowing down operations.

# The security advantages of a unified CMS.

As marketing teams increasingly rely on a growing number of tools, a unified CMS with integrated marketing functions offers significant security advantages. By consolidating essential functions within a single platform, you reduce reliance on multiple third-party systems, minimizing vulnerabilities and ensuring consistent security standards across your tech stack.

This approach streamlines compliance, strengthens access controls, and improves overall data protection. A unified system not only simplifies security management but also helps reduce the complexity and risks that come with app proliferation.

## Key benefits include:

### 1. Reduced attack surface

- Minimizing unnecessary third-party integrations reduces potential entry points for attackers.
- Less reliance on external tools decreases complexity and third-party risk (fewer vendors with varying levels of security to vet and secure).

### 2. Consistent security standards

- A centralized CMS provides a unified approach to data protection, access controls, and compliance across all marketing functions.
- Role-based access controls (RBAC) and Single Sign-On (SSO) reduce credential sprawl and ensure strong authentication.

## 3. Built-in compliance & data governance

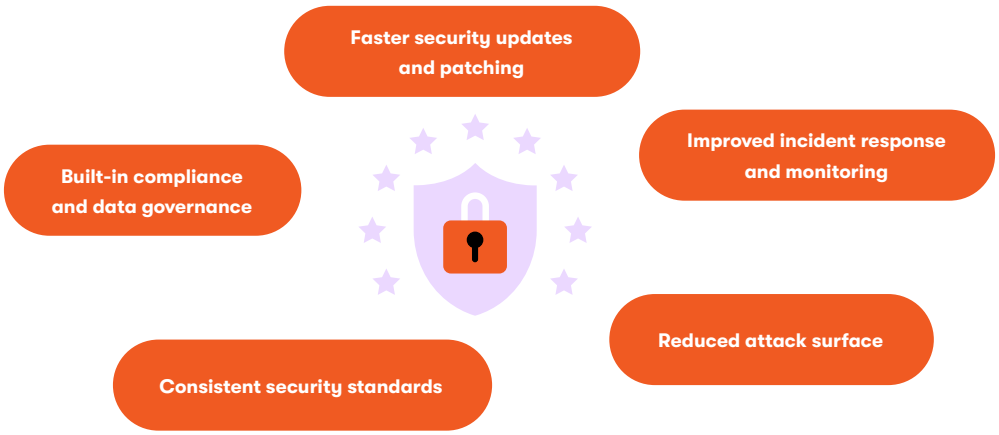
- If the CMS follows GDPR, CCPA, ISO 27001, or similar standards, all integrated marketing tools inherit those protections.
- Data remains within the secure ecosystem and is only accessible via APIs when explicitly permitted, reducing the risk of data leakage.

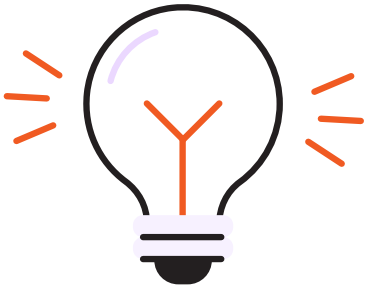
## 4. Faster security updates & patching

- Centralized security updates ensure all components receive patches promptly—no outdated third-party plugins creating vulnerabilities.
- Fragmented MarTech stacks, like best-of-breed composable solutions with multiple third-party integrations, may delay security patches, increasing exposure to threats.
- Tracking and maintaining various security components can be more challenging compared to managing a single security feed from one vendor.

## 5. Improved incident response & monitoring

- Comprehensive logging enables real-time detection of security events across CMS and marketing tools.
- Integration with SIEM solutions to track user activities and detect threats from one central dashboard is much easier for a single application compared to multiple different services.





**Did you know?**

- 29% of data breaches in 2023 were caused by vulnerabilities in third-party vendors, partners, or service providers. (SecurityScorecard)

- 1 in 3 breaches involved shadow data—untracked, unsecured information in forgotten databases or cloud storage. (IBM)

# Creating a security-first culture in marketing teams.

Protecting customer data isn't just about compliance—it's about maintaining trust and safeguarding your brand's reputation. So it's essential to foster a security-first mindset across the team. This means not just relying on IT, but actively integrating security into every stage of your marketing processes. By taking the right steps now, you can reduce risks, ensure compliance, and build long-lasting customer trust.

1. **Educate employees on cybersecurity risks:**

   Train marketing teams on common threats like phishing, social engineering, and malware attacks. Ensure they understand their role in protecting customer data and the company's security policies.

2. **Develop incident response plans for data breaches:**

   Create clear, step-by-step procedures for responding to a marketing data breach. Ensure all employees know how to report incidents and who to contact.

3. **Conduct regular security drills and penetration testing:**

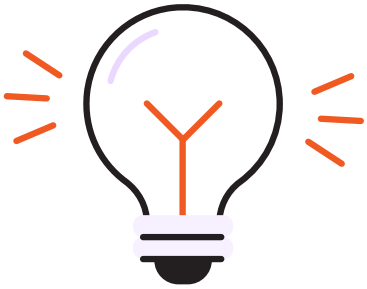
   Request the IT/Security team to simulate security breaches to test how well the marketing team responds and conduct penetration tests to identify and fix vulnerabilities.

4. **Partner with IT/Security teams for ongoing risk assessments:**

   Work closely with IT and security teams to assess marketing tools and processes for potential risks.

5. **Regularly update security measures to stay ahead of emerging threats:**

   Frequently update security protocols to address new vulnerabilities, adapt to evolving threats, and ensure compliance with the latest standards.



**Did you know?**

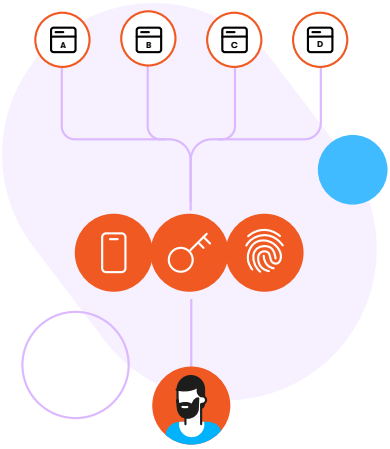
- 80% of organizations reported significant benefits through their privacy investments in building loyalty and trust. (Cisco)

- 80% of organizations report that security awareness training has lowered their vulnerability to phishing attacks. (Proofpoint)

# Xperience by Kentico: The secure choice for modern marketers.

When choosing a platform to protect customer data, marketers need more than just compliance—they need a modern, secure-by-design solution that makes security effortless so they can focus on their campaigns.

Xperience by Kentico provides a unified CMS with built-in digital marketing features, reducing the complexity of managing multiple disconnected tools and giving you full control over security across your content and marketing ecosystem.



## Comprehensive, built-in security

Security is embedded in every layer of Xperience by Kentico, ensuring that your data remains protected at all times. Customer data is encrypted at every stage, both at rest and in transit, providing maximum security. Single Sign-On (SSO) and Multi-Factor Authentication (MFA) via external identity providers offer secure access management.

You stay in control with granular access permissions: RBAC lets you assign user roles with specific permissions, Workspaces help organize content and limit team access, and Page ACLs let you control who can view or edit individual pages.


## Seamless integrations with security in mind

We know marketers need to connect to tools like CRMs and advanced analytics platforms. Xperience by Kentico offers secure API integrations using OAuth 2.0 (allows apps to access data without sharing passwords) and OpenID Connect (verifies user identities for secure logins and SSO), ensuring that third-party connections remain protected while allowing you to continue using your favorite marketing tools, worry-free.


## Built for compliance and peace of mind

Customer data is securely stored in a database that can be self-hosted on your infrastructure, giving you full control over security, access, and compliance, or managed by Kentico in our SaaS cloud environment, where we ensure enterprise-grade security, automatic updates, and compliance with industry standards.

Our SaaS platform is ISO 27001 and SOC 2 Type II certified, meeting the highest standards for security and compliance. Self-hosted customers have full control but can use Kentico's tools and best practices for a secure, compliant setup.

What's more, Xperience by Kentico is designed for GDPR and CCPA compliance, with built-in consent and privacy management tools to help you handle data requests, manage consent, and simplify regulatory reporting—whether you're self-hosting or using our SaaS service.

## Proactive security & fast recovery

Xperience by Kentico continuously monitors for risks, applying automated, zero-downtime security patches to keep your platform protected without disruption.

For SaaS customers, we handle security for you, with automatic backups, threat protection, and a secure infrastructure—so you stay protected without the hassle.

For self-hosted deployments, you have full control over security, with tools to protect your infrastructure and enforce best practices.

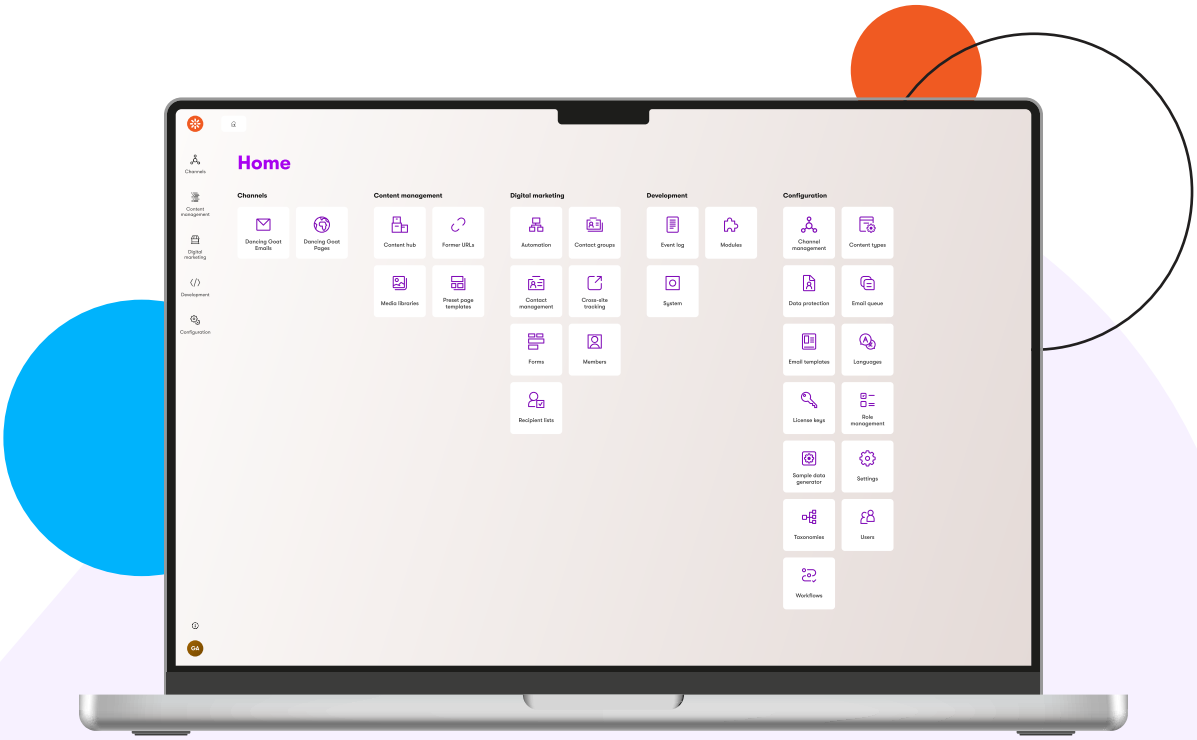
In the rare event of an issue, SaaS customers can trigger an instant restore via the Xperience Portal, minimizing downtime and keeping your business running smoothly.

## Industry-leading support and transparent communication

At Kentico, we provide industry-leading support with a dedicated team ready to assist whenever you need it. We ensure prompt responses to security issues, resolving bugs quickly to minimize any risk to your business. Our commitment to transparent security advisories keeps you informed about potential threats and proactive measures, so you always stay ahead of security challenges.

## Security without the complexity

Security shouldn't slow you down. Xperience by Kentico is designed to make security effortless—built-in protections, automated updates, and secure integrations mean you don't have to worry about complexity. Focus on creating great customer experiences, while we take care of keeping your data safe and compliant.



*“Security is at the core of everything we do at Kentico. We take a multi-layered approach—embedding security into our development lifecycle, running external penetration tests, and even leveraging a bug-bounty program to strengthen our defenses. Our commitment goes beyond just fixing vulnerabilities—we address them transparently and proactively, ensuring our customers always have a secure and reliable platform.”*

**Matěj Groman.**
Security Specialist, at Kentico

# Choose Xperience by Kentico SaaS for market-leading security.

| | | | |
|---|---|---|---|
| Built-in security | Data encryption (at rest & in transit) | Single Sign-On (SSO) & Multi-Factor Authentication (MFA) | Role-Based Access Control (RBAC) & granular permissions |
| Secure integrations (OAuth 2.0 & OpenID Connect) | GDPR & CCPA compliance tools | ISO 27001 & SOC 2 Type II certifications | Self-hosted or SaaS deployment options |
| Automated security patches & updates | Continuous threat monitoring & protection | Instant restore & fast disaster recovery | Secure API connections & authentication |
| Automatic backups | Industry-leading support & rapid issue resolution | Transparent security advisories & updates | Security-focused infrastructure & best practices |

# Securing your MarTech stack: A continuous commitment.

Securing your MarTech ecosystem isn't a one-time task—it's an ongoing effort that requires vigilance, best practices, and the right technology. With cyber threats evolving daily, businesses must proactively strengthen security across all touchpoints, from access controls and encryption to compliance and employee education.

# Key takeaways:

**Security must be proactive, not reactive:** Security is a continuous priority. Organizations that treat it as a one-time checkbox risk costly breaches, compliance failures, and operational disruptions.

**Education on security risks is key:** Awareness of phishing, social engineering, and data breaches helps prevent human errors that lead to security incidents.

**Standards like ISO 27001, SOC 2 Type II, and GDPR provide a security baseline:** However, true security requires ongoing best practices beyond meeting legal requirements.

**MarTech is a prime target for cyber threats:** With vast integrations and customer data, a single security lapse can lead to breaches, compliance failures, and reputational damage.

**Regular security updates and patching are critical:** Fragmented MarTech stacks, like composable solutions with multiple third-party integrations, can delay security patches, increasing exposure to threats.

**Minimizing third-party dependencies reduces risk:** A unified CMS with built-in marketing tools helps limit security vulnerabilities by reducing reliance on external integrations.

**Security is a shared responsibility:** Marketers, IT, and security teams must collaborate to assess risks, secure integrations, and follow best practices.

**Role-based access control & MFA are essential:** These access management tools reduce unauthorized access and improve data security.

**Xperience by Kentico simplifies security management:** With built-in security controls, compliance certifications, and a unified ecosystem, it helps businesses maintain a secure MarTech stack with less complexity.

With Xperience by Kentico, security is built-in—not an afterthought. Our secure, compliant, and unified CMS simplifies security management, helping you focus on marketing while we handle the risks.

**Ready to strengthen your MarTech security?**

Get in touch with our experts today to see how Xperience by Kentico can help you build a secure, resilient marketing technology ecosystem.

# About Kentico.

Reduce the complexity of your marketing technologies and take control of your content across your websites, microsites, emails, and other digital channels through a single solution. Empower your team to create personalized, engaging customer experiences while eliminating time-consuming tasks with a comprehensive content management system that is easy to learn and use.

Tailor content and delivery to individual preferences and develop consistent interactions across multiple digital touchpoints and reach your customers on their favorite channels—any time, anywhere. No need to worry about surprise expenses thanks to transparent, predictable pricing and low ownership costs. Kentico's platform consolidates all the tools you need for successful multichannel content management and digital marketing in a single solution. It offers a rich set of built-in capabilities to help your team achieve more with fewer processes and less technology. With transparent pricing and flexible licensing, you will improve productivity while accelerating business outcomes.

# Eager to learn more?

Talk to our experts! Schedule a free live online 1-on-1 demo of Kentico and let one of our experts walk you through the features and capabilities that will help you create amazing digital experiences.

**MEET OUR EXPERTS**


**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