magnolia

Advanced Security

Take the security of your custom Magnolia DX Cloud solution and your data to the next level

Magnolia DX Cloud Advanced Security Solutions

At Magnolia DXP, we incorporate a high standard of security practices into both our application and our cloud platform.

If you're a Magnolia DX Cloud customer operating a business with extensive security needs, our Advanced Security features help take the security of your custom solution and data to the level your business requires.
This brief describes the advanced features that you can select to bolster security across your website, data, and operations, as well as to enhance security testing and management of security-related information.
With a complete, end-to-end security solution, you gain peace of mind and can focus on your strategic business goals instead of operational concerns.

2 Magnolia DX Cloud Advanced Security Solutions
3 Advanced CDN Security
4 Fastly Managed Security Service
5 Advanced Data Security
6 Advanced Operational Security
7 Advanced Security Testing
8 Overview of Standard Security vs. Advanced Security
9 Compliance and Standards Alignment
10 Magnolia DX Cloud Advanced Security Packages at a glance
11 Next Steps



Advanced CDN Security

Using a content delivery network (CDN) solution helps ensure that your websites can deliver fast, personalized, and secure experiences to your customers globally.

If you're using Fastly, our default CDN on Magnolia DX Cloud, you can now bring more of its security features and benefits into your custom solution. These include:

Automated DDoS Mitigation and Protection with Advanced Edge Rate Limiting

Your Magnolia DX Cloud subscription already comes with distributed denial-of-service (DDoS) mitigation and protection for Layers 3, 4, and 7 delivered by Fastly. These block highly disruptive Layer 3 or 4 DDoS attacks, and inspect and block more complex Layer 7 attacks.
Advanced Security enables automated DDoS protection and advanced edge rate limiting as an additional security layer in front of our Fastly Next-Gen WAF (Web Application Firewall). With advanced edge rate limiting, you can limit the capacity of your website to serve the areas you expect your traffic to come from, while limiting or excluding access from other areas. As a result, you can ensure that your website is fully available for your regular visitors while remaining blocked for malicious traffic.

WAF Custom Rule Set

Your Magnolia DX Cloud subscription includes a ModSecurity Core Rule Set for your web application firewall. The rule set provides the most common rules that protect a website from malicious requests.
With Advanced Security, you have the possibility to customize your WAF Rule Set and implement your own logic for handling requests in the WAF. If your website includes some very specific applications, or if you have specific security weaknesses, you can create custom rules to overcome those potential security risks.

Advanced Bot Protection

Advanced Security detects and mitigates anomalous and velocity-based bot attacks based on request header and body anomalies, traffic source reputation, and other criteria. Volumetric bot-generated traffic is mitigated via advanced rate limiting to both detect and prevent automated behavior against your applications and APIs.

AI traffic Management

The rapid growth of AI technologies has led to an increase in automated crawlers that frequently scrape website content without permission, attribution, or compensation. OurAdvanced Security addresses this challenge by providing specialized tools to detect and manage these agents at the network edge through dedicated signals.

By identifying these bots, you gain total control over their access. You can implement custom rules to block, throttle, or redirect unauthorized scrapers, or conversely, prioritize and serve specialized content to beneficial AI agents, ensuring your digital assets are managed exactly on your terms.

Area of concern	Feature	Base Subscription	Advanced Security
Advanced CDN Security	DDoS Mitigation and Protection	Layer 3, 4 & 7	Automated DDoS Protection on Layer 3, 4 & 7 + advanced rate limiting
	WAF Rules	Default Rule Set	Custom Rule Set
	Bot Protection Service	Excluded	Included
	Bot Management	Excluded	Included
	AI Traffic Management	Excluded	Included



Fastly Managed Security Service

For even more peace of mind, you can opt for a fully managed security service from Fastly. Especially in the case of a large-scale attack, Fastly's experience in handling such attacks from the first signs to reaction can make all the difference in successfully fighting such security threats.

24/7 proactive monitoring enables you to focus on your core business and reduce risk. You can rest assured knowing that Fastly's security experts continuously monitor for threats and take proactive actions to mitigate attacks.
You also get access to comprehensive reporting, which provides actionable, tracked insights that continuously improve your security posture.

	Response Security Service	Managed Security Service
24/7/365 attack support, 15-minute response SLA	✓	✓
Direct security phone line and chat channel	✓	✓
Configuration assistance	✓	✓
Access to a security expert	✓	✓
24/7/365 proactive monitoring with threat hunting		✓
Post-event reports		✓
Monthly security reports and reviews		✓
Readiness drills		✓



Advanced Data Security

As data is moving more and more across multi-cloud, distributed cloud, or even hybrid cloud environments, immediate measures must be taken to mitigate cloud data security challenges.

Encryption, intrusion monitoring, and vulnerability scanning are proactive measures to help retain control over your data and reduce data security risks. Our Advanced Security features enhance the security of your data through:

Encryption Key Storage

All data at rest in Magnolia DX Cloud is encrypted by default with AES-256 using keys held in a FIPS 140-2 validated KMS, managed by either the underlying cloud provider or by Magnolia. This applies to persistent disks, file shares, and object storage.

With Advanced Security, you can step up to Customer-Managed Encryption Keys (CMK / BYOK). Your organization retains full authority over the key lifecycle - generation, rotation, revocation, and destruction. Magnolia services request your keys to encrypt and decrypt data on demand, and you can revoke Magnolia's access at any time, including emergency crypto-shredding scenarios.

This model supports key-sovereignty obligations commonly required under DORA, ISO/IEC 27001 Annex A.8.24 (Use of cryptography), and GDPR Art. 32.

Active Threat Monitoring

Advanced Security implements Intruder Detection System (IDS) and Intruder Prevention System (IPS) services that automatically detect and even actively suppress occurring anomalies on the cluster on demand. The platform has all the required tools to address outbreaks, perform forensic analysis, and prevent similar threat patterns from becoming active in the future.

Vulnerability Scanning

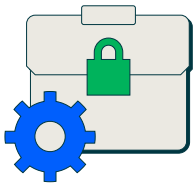
Magnolia DX Cloud runs an integrated GitLab security pipeline that scans every commit and every promoted build across four complementary dimensions before code reaches production:

Scan type	What it catches
SAST	Code-level vulnerabilities (OWASP Top 10, CWE Top 25) using Semgrep-based analyzers
Container Scanning	Vulnerable OS packages and libraries in container images, against NVD and OS-vendor advisory databases
IaC Scanning	Misconfigurations in Kubernetes manifests, Helm charts, and Terraform
Secret Detection	Hardcoded credentials, API tokens, and private keys, using pattern and entropy detection

Findings are CVSS-scored, deduplicated, and surfaced to developers directly in the merge request. High and Critical findings can be configured to block promotion to production. A Software Bill of Materials (SBOM) in CycloneDX format is generated for every production image, supporting NIS2 supply-chain transparency and US Executive Order 14028 SBOM requirements.

Scans run both at build time (shift-left) and against running clusters (runtime), so dormant or newly-disclosed CVEs in already-deployed code are flagged continuously.

Area of concern	Feature	Base Subscription	Advanced Security
Advanced Data Security	Encryption Key Storage	Key owned by cloud vendor or Magnolia	Key owned by customer
	Active Threat Monitoring	Excluded	Included
	Vulnerability Scanning	Docker image scanning	Isolated pipeline environment



Advanced Operational Security

To improve threat detection and prevention within organizations' operations, Advanced Security offers a set of features that increase protection of sensitive information across asset management tools, public-facing websites, and cluster communications.

Malware Detection

With Magnolia DX Cloud Advanced Security, uploads of assets or zip files to the Magnolia DAM are scanned and checked for malware. This feature will be extended to cover assets stored in connected DAM systems as well. If malware is detected, you receive instant feedback.

This capability provides an extra layer of protection in case an employee's computer is hacked and helps prevent damage from intentional malicious behavior.

Web Defacement Protection

Advanced Security offers web defacement protection that monitors public-facing websites 24/7 to detect possible website defacements or hacks.

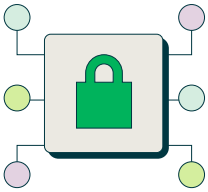
The solution will monitor your site (for example, your top-most visited pages), take snapshots of suspicious changes, and it even allows you to revert to a previous version if your public-facing website underwent an attack. You are notified via email if an attack occurs or if your website changes.

Secure Cluster Communication Traffic

In addition to securing every outgoing service communication, Magnolia DX Cloud Advanced Security can leverage existing concepts to secure and encrypt communication inside the clusters. This capability uses a service mesh to encrypt network traffic and API communication by using mTLS by default, even if this is not considered in the application itself or in a development state (pod to pod).

With this feature, you maximize the security of your clusters, so that if any system within an environment is hacked, the other pieces of the environment are not affected.

Security Aspect	Feature	Standard Security	Advanced Security
Malware and Web Defacement Protection	Malware Detection	Excluded	Included with signature-based malware scanning
	Web Defacement Protection	Excluded	Included
	Secure Cluster Communication Traffic	Excluded	Included



Advanced Security Testing

To provide the most secure environment for our customers, Magnolia DX Cloud regularly undergoes security testing, including but not limited to penetration testing conducted by Compass Security Group, an independent third-party security vendor.

With Advanced Security, you can also opt in for a 3rd Party Penetration Test of your own dedicated infrastructure.

3rd Party Penetration Test

During the penetration test, we analyze your exposed infrastructure and search for vulnerabilities and possible direct attack vectors by first scanning your system and services, and then manually testing each of them. The identified attack vectors will be exploited and proven out to identify and measure risks associated with the exploitation of the target's attack surface. We then provide a detailed report with suggestions to improve or fix possible vulnerabilities detected.

The penetration tests are performed in partnership with our longtime and highly trusted security partner, Compass Security Group.

What's tested: platform vs. your customizations

The Magnolia DX Cloud platform itself is independently penetration-tested annually by Compass Security Group as part of every Magnolia DX Cloud subscription - Standard and Advanced. An executive summary of the most recent platform test is available to all customers under NDA.

The Advanced Security pen test is complementary and focuses on your dedicated environment and the extensions you build on top of the platform, which fall outside the scope of the platform-wide assessment. Typical scope includes:

- Custom-developed templates, components, and front-end code
- Customer-built REST or GraphQL APIs and third-party integrations
- Additional pods, services, or workloads deployed alongside the standard Magnolia stack
- Network paths and east-west traffic introduced above the baseline platform topology
- Custom authentication, SSO, and authorization flows configured for your tenant

The engagement combines automated reconnaissance with manual exploitation against your specific attack surface, delivered as a CVSS-scored report with prioritized remediation guidance. Scope, timing, and rules of engagement are agreed during a kickoff workshop.

Security Aspect	Feature	Standard Security	Advanced Security
Security Testing	3rd Party Penetration Test	Optional	Included

Overview *of* Standard Security vs. Advanced Security

Advanced Security brings a wealth of additional features on top of what's included in the Standard Security subscription. A quick overview of the advanced security capabilities is reflected in the table below.

Security aspect	Feature	Standard Security	Advanced Security
CDN Security	DDoS Mitigation and Protection	Layer 3, 4 & 7	Layer 3, 4 & 7 + advanced edge rate limiting
	WAF	Default Rule Set	Custom Rule Set
	Bot Protection Service	Excluded	Included
	Bot Management	Excluded	Included
	AI Traffic Management	Excluded	Included
Data Security	Encryption Key Storage	Key owned by cloud vendor or Magnolia DXP	Key owned by customer
	Active Threat Monitoring	Excluded	Included
	Vulnerability Scanning	Docker image scanning	Isolated pipeline environment
Operational Security	Malware Detection	Excluded	Included with Signature-based malware scanning
	Web Defacement Protection	Excluded	Included
	Encrypted in-cluster communication	Excluded	Included
Security Testing	3rd Party Penetration Test	Optional	Included

Compliance *and* Standards Alignment

Magnolia DX Cloud operates under a continuously audited control framework. The Standard and Advanced Security capabilities described in this brief map to the controls most commonly cited in customer security assessments.

Standard	Status
ISO/IEC 27001:2022	Certified - Information security management system
ISO/IEC 42001:2023	Certified - Artificial intelligence management system
SOC 2 Type II	Attested - Security, Availability, and Confidentiality Trust Services Criteria
ENS High (Esquema Nacional de Seguridad)	Compliant - Spanish public-sector framework
Independent platform penetration testing	Annual, by Compass Security Group

EU regulatory frameworks Magnolia DX Cloud is designed to support

- **GDPR** - EU/EEA data residency options, signed DPA, sub-processor transparency, and Art. 32 technical and organizational measures
- **NIS2** - Operational resilience and incident-reporting capabilities for essential and important entities, supported by mandatory immutable audit logging and 24/7 monitoring (included in Standard Security)
- **DORA** - ICT risk management, ICT-related incident classification and reporting, and third-party risk evidence for financial entities; Magnolia provides the audit artifacts, SLAs, and exit-management commitments required of critical ICT third-party service providers

Customer compliance enablement (non-certifying)

While Magnolia DX Cloud does not itself hold PCI-DSS or HIPAA certification, the Advanced Security controls - customer-managed keys, in-cluster mTLS, immutable audit logging, IDS/IPS, vulnerability scanning, and managed WAF - are designed to support customers operating workloads subject to:

- **PCI-DSS v4.0** for payment-adjacent flows where Magnolia is not in the cardholder data environment
- **HIPAA Security Rule** for ePHI handling, under a customer-specific risk assessment
- **FedRAMP-aligned** and government-sector deployment patterns, including controls comparable to those required by the Singapore Government IM8 / MTCS frameworks

A detailed control-mapping appendix (Advanced Security feature → ISO/IEC 27001 Annex A / NIST SP 800-53 Rev. 5 / CIS Controls v8) is available on request under NDA.

Magnolia DX Cloud Advanced Security Packages *at a glance*

You can opt for the full Magnolia DX Cloud Advanced Security Package or select individual packages, depending on your security needs.

Advanced CDN Security	DDoS mitigation & protection	Bot protection service
	DDoS observer dashboard	AI Traffic Management
	WAF custom rule set	Advanced edge rate limiting

Fastly Managed Security Service	24/7/365 Security Service	24/7/365 proactive monitoring with threat hunting
	24/7/365 attack support with 15-minute response SLA	Post-event reports
	Direct security phone line and chat channel	Monthly security reports and reviews
	Access to security expert	Readiness drills

Advanced Data Security	Encryption key storage	Active threat monitoring
	Vulnerability scanning	Additional resources (node)

Advanced Operational Security	Malware detection	Secure cluster communication traffic
	Web Defacement Protection	

Advanced Security Testing	3rd Party Penetration Test	Kickoff & scoping
	Conducting a pen test	Pen test report

Get started with Magnolia DX Cloud

Navigating the wide range of digital experience technologies available today can be difficult. Even after exploring different solution types, deployment options, editorial experiences, development approaches, and delivery methods, you need to carefully weigh the benefits and drawbacks of each choice for your marketing and technology teams.

Magnolia DX Cloud helps you capitalize on the best technologies for your business while overcoming key limitations. You gain a truly composable, modular platform with essential building blocks for creating a robust DXP, plus the flexibility for change. By handling the heavy lifting of hosting and maintenance, Magnolia DX Cloud provides a worry-less infrastructure that allows your team to focus on innovation.
Importantly, we are committed to your success. Instead of remaining invisible to a large DXP vendor or attempting to build a DXP all on your own, you can work closely with our digital experience architects to help you realize your ideal business outcomes.



Lukas Reck
Product Manager
Magnolia DX Cloud

Ready to learn more?

Book a demo with us