GAN Technical Platform Guide for McDonalds

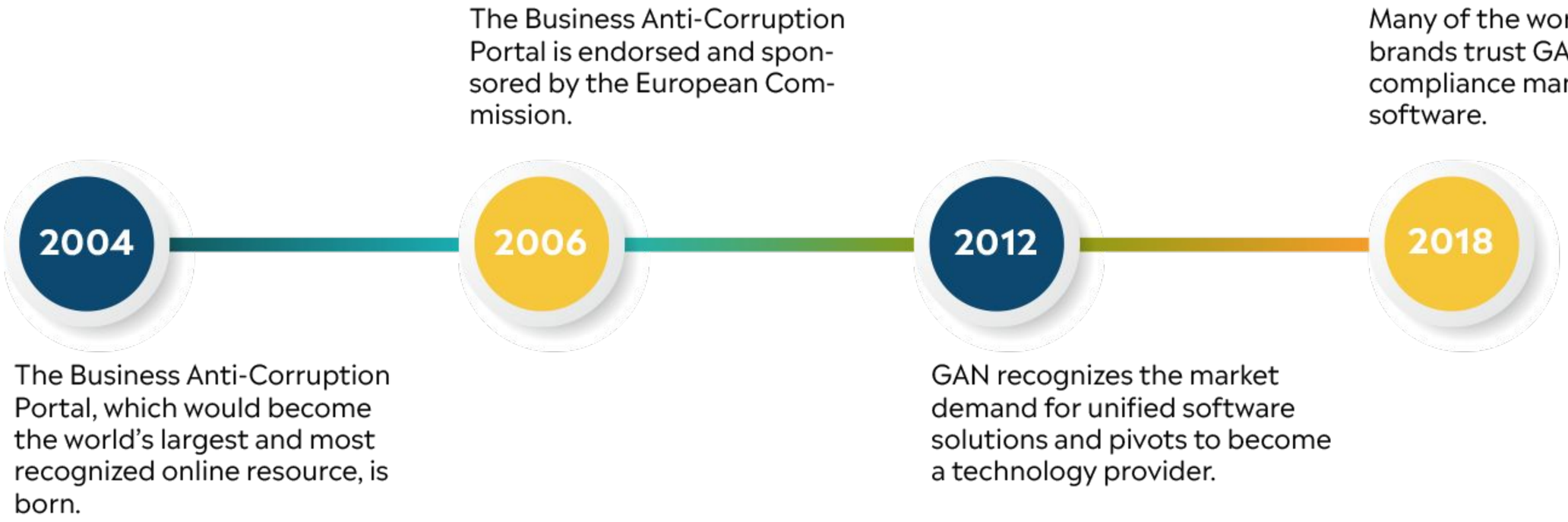
Platform, Security & Technology Overview

Version: 1.15, June 15, 2021

Confidential Information

Who We Are

The GAN Integrity Story

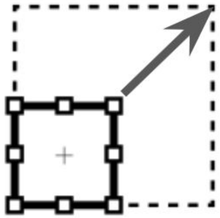


GAN INTEGRITY

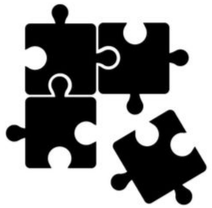
GAN Platform: Product Focus

Danish Design DNA

Compliance Expertise



Scalability



Modularity

Agile

Security

Engineering: Practices

Processes

- SDLC with Agile principles with roadmap, backlog and sprint planning
- Key gate points during SDLC: Fitness for Development, Security Review, Fitness for Launch
- Structured Maintenance, Incident and Bug Processes
- Defined SLA metrics
- 24x7 Tech Operations with uptime KPI tracking

Secure Development Practices

- Engineers trained in secure engineering practices (OWASP TOP 10) and frameworks
- Code reviews ny Tech Leads before code is deployed to production
- Regular penetration tests done by 3rd party
- Trained security staff in DevOps Team
- Sensitive information is never sent or stored in plain text
- Security frameworks to handle headers, cookies, encryption and manipulation of requests (e.g. XSS & injection prevention)

24x7 Tech Operations

- Global platform require 24x7 operation
- 24x7 Tech Operation Team and Global Support Team

Global Support Team: Practices

Processes

- Global support team - 24x7 coverage ”follow-the-sun” team layout
- Handling maintenance, incident and bug management process to ensure 1) Timely client communication, 2) Critical client needs are heard
- Less than 8 hours support ticket response time
- Ticket scope is not only technical support issues, but also user support, UI guidance and content questions

State-of-the-art Tool Set

- Zendesk external facing ticket system - integrated with internal facing Jira ticketing system
- Client self-service - eg. FAQ and support articles

Hosting Overview

GAN Platform is fully hosted on **Amazon Web Services (AWS)** in the EU.

- GAN platform hosted in EU-WEST-1 Region (Ireland)
- Multiple Availability Zones (AZ’s) utilised (separate data centers)
- Replication across AZ’s (to ensure low error tolerance and high availability)
- Frankfurt region (EU-CENTRAL-1) and Ireland region (EU-WEST-1) used as backup locations

Availability & Disaster Recovery

Worst case disaster impact

- RTO (Recovery Time Objective): 3h 45 min (to satisfy SLA 99.5%)
- RPO (Recovery Point Objective): 24 hours

Most likely scenario: Element in tech stack fails partly

- Replication lag < 1 minutes (data loss)
- Rebalancing and regaining production performance (1-5 hours to restore)

Data retention:

- Daily + monthly backup
- Backup saved for 30 days

Documented plan and procedures for gaining control after a disaster

Access Controls

Employees at GAN use

- Strong password - Always personal credentials
- Private keys (SSH) for access to key systems
- MFA for all 3rd party services
- Mandatory passwords vaults

Access Management

- Only employees with explicit needs get data access
- Access levels are revised event based and periodic
- On- and off-boarding process for employees entering/leaving GAN
- Regular periodic internal security audits and access reviews for all critical systems
- Always change default vendor passwords
- Technical services (AWS, Google, Sendgrid, ..):
  - SSO/MFA for admin access
  - Secret API key for app2app communication

Physical Office Security

- GAN has main offices in Copenhagen and New York
- GAN offices are installed with security system and access chip with pin-code
- GAN has clean desk policy; customer data, source code, PII or credentials etc. must be locked away or stored on company hardware protected by personal credentials

Security Processes

Monitoring

- Transactions to API's and VPC is logged with Cloudtrail.
- Captures income/outgoing traffic to/from our VPC
- Monitoring of system health and performance done by system and application metrics systems.
- Tools: CloudWatch, LogStash ELK, Kibana, New Relic, Bugsnag

Encryption

- In motion:
  - Strong protocol (TLS 1.2)
  - Strong key exchange (ECDHE_RSA with P-256)
  - Strong cipher (AES_128_GCM)
- At rest:
  - AES-256 algorithm (Postgres and S3)
  - AWS encrypted disks
- Encryption keys are managed using AWS KMS
- All filesystems encrypted with asymmetric keys

Security Testing

- Regular penetration tests by 3rd party Cobalt Labs in San Francisco
- Scope is vulnerability assessment and penetration testing
- Assessed against OWASP
- Mandatory security reviews as part of SDLC

Certification

- We are preparing for ISO27001 certification and have an active audit contract with DNV GL

Log Files and retention

- Application events including user access: Indefinitely (during client lifetime)
- APM/monitoring logs: 30 Days
- Error logs: 30 Days
- No network flow logs
- Logs related to DNS: 4 hours (CloudFlare)

Data Privacy & GDPR

- GDPR compliance program in place ranging from assigning of responsibilities to compliance monitoring and training.
- Appointed Data Protection Officer (DPO).
- Participant in the US-EU/US-Swiss Privacy Shield.
- Data processing agreements:
  - In place with all third parties (sub-processors) that process personal data on behalf of our customers.
  - New sub-processors must conclude a data processing agreement that clearly states and delineates their authority to process such personal data.
  - Sub-processors are prohibited from selling or using the personal data for their own purposes.
- GAN has classified the types of personal data we process via our services in our data processing agreements with our customers, ensuring there is a clear and well-documented record of the personal data being processed in our capacity as a data processor.
- Employee actions:
  - All employees complete privacy and information security training upon annually.
  - New employees are required to complete this training as part of their employee onboarding process.

Service Level: Maintenance Process

Maintenance Needed → Send Notification → Maintenance Open → Maintenance Closed

Engineering
Will give 1 week lead time for **scheduled maintenance** and customer notification will go out 5 days in advance. **Urgent maintenance** will give 30 minutes notice and customer notification will be sent immediately

Support
Selects customer segment to notify, confirms maintenance details, creates messaging content, selects what dates to send

Marketing
Templates message, pulls customer segment, and sends notification

Engineering
Will update support on maintenance status

Support
Will field any questions/issues through tickets and revert to engineering if necessary

Customer update
Support will update the customer that the issue has been resolved.

Service Level: Categories and Response Times

Service Management	Response Time	Comments
P1 Incident Response to Customer (Critical)	1 hour during primary coverage hours	Function of all or a substantial part of a Service has failed, critically degrading Customer's operational performance. No practicable workaround.
P2 Incident Response to Customer (Moderate)	24 hours during primary coverage hours	The reported fault does not materially affect Customer's Services or a workaround exists that does not substantially inconvenience Customer on an ongoing basis.
Data Breach Incident Response to Customer	Without undue delay and no later than 72 hours	Personal data breaches have to be reported to affected customers, who themselves have an obligation to notify data subjects and authorities if the GDPR applies. The "without undue delay" standard requires GAN to notify the customer as soon as possible once GAN has discovered and concluded a personal data breach has occured. This typically means no less than 72 hours, as that is the maximum time limit the GDPR applies to our customers, and it is a common timeline agreed in contracts. GAN Legal Team need to be involved.
Change Management	Information Time & Channels	Details about scheduled maintenance, releases, and changes will be announced via e-mail to the customer contact. A precondition for this is a properly configured technical contact with the GAN Global Support Team
Scheduled/Planned maintenance	Immediately 5 days in advance 4 weeks in advance	• In case of a necessary hotfix & precautionary measures to avoid service downtimes • Scheduled maintenance window • In case of any structural changes of e.g. API structures which require changes/adaptations on customer side

Service Level: KPI and categories to be measured

Term	Definition	Comments
KPI	Monthly average of system downtime; measured in full service down time and partial service downtime	• Full service downtime: Whole product is not available • Partial service downtime; eg. a data vendor is not available or a specific function is not working • In calculating the downtime is announced maintenance not included • Our SLA required uptime KPI is 99.5% • 1 month = 43.200 minutes so if we are down more than 216 minutes in a month are we below our uptime KPI
KPI Categories	Uptime/downtime are measured with certain categories	• Products measured: DD, G&H, Case, COI, Campaigns, User Management – and overall • Each single vendor: AWS, RDC, Control Risks, Traliant, PSA, Exago, Hotlines (MAP, Expolink, Whistle Blower Security) – and overall • What we measure: Incidents & Maintenance
KPI Reporting	Monthly and yearly	KPI calculation and reporting of: • Uptime % of above products – and overall • Uptime % of all single vendors – and overall • Monthly and yearly reporting

GAN INTEGRITY

ganintegrity.com

info@ganintegrity.com

@gan_integrity