ALLIED ESM

HALO OFFICIAL PARTNER

Under the Hood

How Halo Is Built.

A technical overview of the Halo platform architecture.

Hosting · Data · Application · Integration · Security

Built for the Modern Enterprise

Four layers. One platform. Zero compromise.

Halo is built on a deliberate, modern technology stack. Where legacy platforms carry the weight of two decades of architectural decisions, the Halo SaaS platform was purpose-built approximately six years ago — designed from the ground up for speed, scalability, and open integration. In SaaS terms, six years is a meaningful differentiator. It means Halo was architected with cloud-native thinking from day one, not retrofitted onto infrastructure built when on-premise was still the norm.

The result is a platform that is lightweight, fast to navigate, and genuinely extensible without the professional services overhead that older platforms demand. This document walks through the four architectural layers that underpin every Halo deployment.

1

AWS Global Hosting

Halo runs on Amazon Web Services across seven active hosting regions spanning North America, Europe, the Middle East, Africa, and Asia-Pacific. Every deployment benefits from enterprise-grade redundancy, geographic data residency control, and a formal 99.95% uptime commitment backed by automatic failover.

2

Microsoft SQL Server

All platform data is stored in Microsoft SQL Server — a battle-tested relational database with a proven enterprise track record for reliability, transactional integrity, and compliance-grade auditability. Every change is tracked and tamper-evident by design.

3

React Application Framework

The Halo user interface is built on React — the modern, component-based JavaScript framework trusted by the world's most demanding digital products. The result is a fast, responsive interface with no full-page reloads and consistent rendering at scale.

4

API-First Integration Architecture

Every screen and data object in Halo is API-driven. This underpins 250+ native integrations and enables connectivity to virtually any third-party system with an open REST API — all within a low-code / no-code configuration model that requires no custom development.

The Hosting Layer

Global infrastructure. Enterprise-grade reliability.

Every Halo instance is hosted on Amazon Web Services across seven active regions: London (UK), Frankfurt (EU), North Virginia (US), Canada Central, Cape Town (South Africa), Sydney (Australia), and Bahrain (Middle East). Customers select the region that aligns with their data residency requirements at onboarding — EU customer data is hosted exclusively in the London or Frankfurt regions and never leaves the EU, including backups. UK-only hosting, US-only hosting, and other regional configurations are all supported.

Each region operates a multi-Availability Zone (AZ) model: a minimum of three physically separate data centres, each with independent power, cooling, and network connectivity. Halo's database infrastructure runs a production-replica cluster model across these AZs, with a file-share witness providing automatic failover should any node become unhealthy. At the application layer, Halo follows a blue-green deployment model, eliminating scheduled downtime during updates. The combined result is zero-downtime failover for both node-level and full availability zone failures.

All application and database infrastructure is held within a private subnet, accessible only via a public NAT gateway. Access is restricted to Halo infrastructure engineers and high-privilege administrators; all other access requires formal approval and is automatically revoked after a defined period. The platform is backed by a formal Business Continuity and Disaster Recovery plan, with a Recovery Time Objective of 4 hours and Recovery Point Objective of 1 hour for large-scale incidents.

7	99.95%	1 Hour
Hosting Regions	**Uptime Target**	**Recovery Point**
London · Frankfurt · N. Virginia · Sydney · Canada · Cape Town · Bahrain	Formal 99.90% SLA with auto-generated service credits if breached	RPO of 1hr, RTO of 4hrs — backed by formal BC/DR plan

The Data Layer

Proven reliability. Enterprise-grade security.

Halo stores all platform data in Microsoft SQL Server — a relational database with decades of enterprise deployment history across financial services, healthcare, government, and global manufacturing. Its maturity is a genuine asset: proven reliability, a large ecosystem of tooling and compliance support across every major regulatory framework.

High-Availability Architecture

Deployed across production-replica database clusters spanning multiple AWS Availability Zones. A file-share witness enables automatic failover with zero downtime should any node become unhealthy.

Full Audit Trail

Every change in Halo — tickets, configuration updates, agent actions, and admin changes — is logged in a tamper-evident record stored directly in the SQL Server database. Supports ISO 27001, SOC 2, GDPR, and ISO/IEC 20000 compliance.

Multi-Layer Encryption

AES-256 encryption at rest for all databases and backups. X.509 certificates protect sensitive field-level data. TLS 1.2+ with HSTS enforced in transit. Only Halo application servers can read encrypted values.

Automated Backup Policy

Transactional backups every hour (3-day retention), daily backups (2 weeks), and monthly backups (60 days). All encrypted, stored within the same regional boundary as primary data, and tested monthly for integrity.

Read-only database access is available for customers requiring direct Power BI connectivity — enabling live operational dashboards and custom reporting without any data export.

The Application Layer

Built on React. Fast, modern, and built to scale.

The Halo user interface is built on React — the open-source JavaScript framework originally developed by Meta, now the most widely adopted frontend framework in enterprise software development. React powers a significant share of the world's most demanding web applications, from large-scale SaaS platforms to financial trading systems and global e-commerce. Its presence in the Halo stack is a deliberate architectural choice, not a default.

React's component-based model means the Halo UI is assembled from discrete, independently rendered elements. Changes to one part of the screen do not trigger full-page reloads — only the components that need to update do so. The practical result is a platform that feels fast and responsive at scale, even during high-volume agent activity. React's virtual DOM and concurrent rendering capabilities ensure the interface remains interactive during intensive operations.

Halo's microservices — including automations and chat — are handled outside of the standard application infrastructure, each with their own load balancer and auto-scaling group. This means high-demand features operate independently of the core platform, improving processing speeds and the overall resilience of the service.

The Integration Layer

Every screen and data object in Halo is API-driven. This is a foundational design decision — not a bolt-on integration layer — and it shapes what Halo can connect to, how quickly, and with how little friction.

Halo ships with over 250 native, purpose-built integrations spanning ITSM toolchains, monitoring and observability platforms, identity providers, collaboration tools, and business applications. These are bidirectional integrations that push and pull data, trigger automations, and appear natively within Halo workflows.

Beyond the native library, any external system that exposes a REST API can be connected through Halo's configuration model — no custom development required. This low-code integration capability means organisations with bespoke internal applications, legacy systems, or specialist tooling are not blocked. They configure, connect, and go.

Security & Compliance

Independently audited. Continuously monitored.

Halo Service Solutions holds a comprehensive set of independently audited security certifications, covering information security management, data privacy, payment security, and cloud security assurance. All certifications are maintained as live, audited commitments — not self-declarations.

Certification	Scope & Significance
ISO/IEC 27001:2022	ISMS certified by UKAS-accredited body BAB (cert. HALO[2143826]). Covers risk management, access controls, physical security, incident response, business continuity, and supplier management.
SOC 2 Type 2	Independent operational audit covering Security, Availability, and Confidentiality Trust Services Criteria over a defined period. Reports available under NDA on request.
PCI DSS — Level 1	Payment Card Industry Data Security Standard at the highest service provider tier. Demonstrates rigorous controls over cardholder data environments.
Cyber Essentials (UK Gov)	UK Government-backed certification confirming five key technical controls: boundary firewalls, secure configuration, access control, malware protection, and patch management.
CSA STAR Level 1	Cloud Security Alliance registry demonstrating transparency and adherence to cloud security best practices.
GDPR (EU & UK)	Full GDPR compliance. Data Processing Agreement (DPA) available. EU data hosted exclusively in EU regions. Standard Contractual Clauses (SCCs) in place for international transfers where applicable.
HIPAA	HIPAA compliance for US healthcare customers. Business Associate Agreement (BAA) available on request.

Continuous Monitoring & Intrusion Detection

Halo operates a layered monitoring and intrusion detection stack across the entire hosted environment: 5-minute health checks on all instances, database-level performance tracking, and per-instance API analysis via Azure Application Insights. At the security layer, AWS CloudTrail logs all API activity; AWS GuardDuty monitors for anomalous account-level traffic; AWS Security Hub enforces benchmark compliance; and AWS CloudWatch triggers

automated alerts for threshold breaches. All security data is centralised via AWS Security Lake. Annual penetration testing by a specialist third party covers application-level attack vectors, with findings triaged and actioned.

Performance at Scale

Tested under load. Documented. Transparent.

Halo has published formal stress testing results for a standard, unoptimised single instance. The figures below represent the point at which performance degradation first becomes detectable — they are baselines, not hard limits. Every threshold has a clear, documented optimisation path, and Halo's active development roadmap targets improvements across all four dimensions.

7M+

Unarchived Tickets

Standard baseline before optimisation is recommended

1,500

Concurrent Agents

Simultaneous active users on a standard instance

1.5M

Configuration Items

Fully supported on a standard single instance

Dimension	Standard Instance Baseline	Optimisation Available
Ticket Volume	7 million unarchived records	Automated archiving + database indexing
Configuration Items	1.5 million CIs	Data indexing and query caching
Concurrent Agents	1,500 simultaneous users	Load balancing for high-concurrency environments
External API Calls	200 calls per minute (client-built integrations)	API batching and integration-level optimisation

Testing was conducted without any platform-level or infrastructure optimisations applied, establishing a genuine worst-case baseline. Halo's engineering team is available to discuss architecture and scaling requirements directly for organisations operating at the enterprise end of the scale.

Ready to Explore Halo?

Allied ESM — your technical Halo partner.

Allied ESM is an authorised Halo partner specialising in platform evaluation, architecture design, and enterprise deployment. Whether you are assessing Halo against an existing platform or planning a first implementation, we can provide hands-on technical guidance at every stage.

- Platform demonstrations and technical deep-dives
- Architecture review and integration planning
- Migration assessment and deployment support
- Ongoing managed service and performance optimisation

Get in Touch

info@alliedesm.com | alliedesm.com