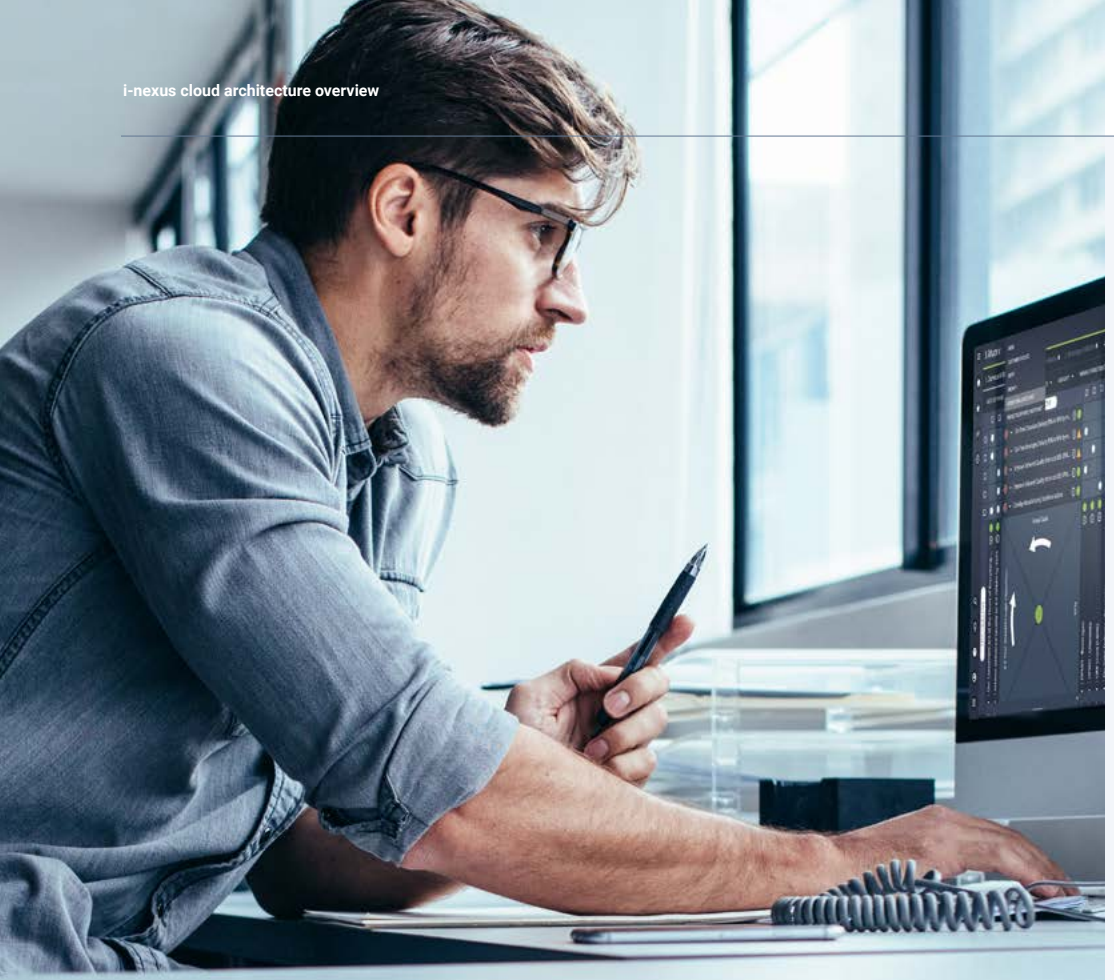
i-nexus cloud architecture overview



Contents

Confidentiality, availability, and integrity of data is paramount...

This guide explore the technical specifications of i-nexus, from new releases and testing, to security, General Data Protection Regulation compliance, and the hosting environment.

As part of this, business leaders must rest assured that, when using i-nexus, they are benefitting from best-in-class data protection, up-to-date testing and compliance.

Through knowing that these systems are working in the background, you can focus on what is important - achieving more of your goals with less effort.

Company

All members of the Executive Team and Directors are directly responsible for implementing and continually improving the security of their business areas and the adherence of their teams. Each team member understands their role and responsibility in regards to i-nexus security policies.

ISO 27001

A crucial element of i-nexus' information security and our customers' peace-of-mind is our adherence to the ISO27001 international standard in best practice for an Information Security Management System (ISMS). This is a mark of our organizational excellence in applying security best practices, as our timeline shows:

- We successfully implemented in 2014 and current certification is ISO/IEC 27001:2022
- We have maintained our certification since this point with multiple recertifications
- This highlights our ongoing commitment to information security and protecting our customers' data

Scope

The scope of the information security systems is as follows:

- Covering the remote working staff in the UK
- All internal information systems that allow the ongoing delivery of day-to-day processes
- All aspects of interaction of these with our externally hosted solution available to customers via our service provider Amazon Web Services (AWS).
- Our software development systems to include locally and remotely based team members
- Security of our customers' data
- Protection of personal data both of our staff, customers and other partners
- Ensuring our suppliers that impact on our ability to satisfy the above are appropriately monitored and controlled
- Compliance with all appropriate legislation, regulations and contractual obligations applicable to the above

Objectives

The following covers the objectives of the i-nexus Information Security System:

- Develop and maintain a suite of security policies
- Establish regulatory compliance and best practice alignment to ensure the confidentiality, availability and integrity of all forms of business and personal data as applicable. This is to include but is not limited to:
  - Establish a systematic approach to risk assessment
  - Establish a suitable business continuity plan
  - Record, review, investigate and implement corrective action where necessary for all reported security incidents
  - Incorporate the appropriate level of monitoring, review and continuous improvement
- Ensure there is a level of commitment to security at all levels and that an Executive level sponsorship for security is established
- Ensure security roles and responsibilities are defined
- Deliver regular security awareness and education to all staff
- Review information security matters arising at each board meeting

Hosting environment

AWS hosted

i-nexus is hosted on an AWS (Amazon Web Services) infrastructure following the AWS Well-Architected Framework, Red Hat Architecture and both Red Hat Server and Networking security principles. The five pillars of the Framework (operational excellence, security, reliability, performance efficiency, and cost optimization) underpin the high performance and resilience of our platform; providing a consistent service, quality, stability and scalability.

Multi-region

i-nexus currently maintains AWS environments in multiple regions in Europe and North America. However, depending on customer requirements, we can utilise any AWS region globally.

Secure private cloud

Each one of our environments are built using separate Amazon VPC (Virtual Private Cloud) to ensure full secure separation. Every VPC is segmented into five separate zones (Presentation, Application, Data, Data processing and DMZ) with specific network access rules restricting traffic between zones. This means that all back-end systems, such as databases and application servers, are in private-facing subnets with no Internet access and no direct access to the servers.

i-nexus' servers are built using the latest generation AWS EC2 hardware specification and the latest version of the Linux operating system, that has been specifically hardened for our application.

i-nexus' network architecture

i-nexus adopts a multi-tier network architecture. This means that our main network is split into distinct segments with separate security groups and access control lists to protect traffic between each segment.

Each layer of our architecture in more detail:

1. Presentation layer. An externally-facing zone containing our web proxy servers and web application firewall. This security group has external internet access, but this is restricted to only allow HTTP & HTTPS traffic on ports 80 & 443.
2. Application layer. An internal layer containing our application servers and a private network segment, with no external access.
3. Data layer. An internal layer only, for our encrypted database servers and the encrypted document store. Access to this zone is strictly controlled via access control lists on the firewall. This ensures that all customer data is stored on machines that have no direct access to the internet. **(See Diagram 1 for our shared cloud network layout)**
4. DMZ. This zone hosts our file transfer services and no server in this zone can initiate a connection to any other security group.
5. Data processing. This is our large data zone to support future data analytics capabilities

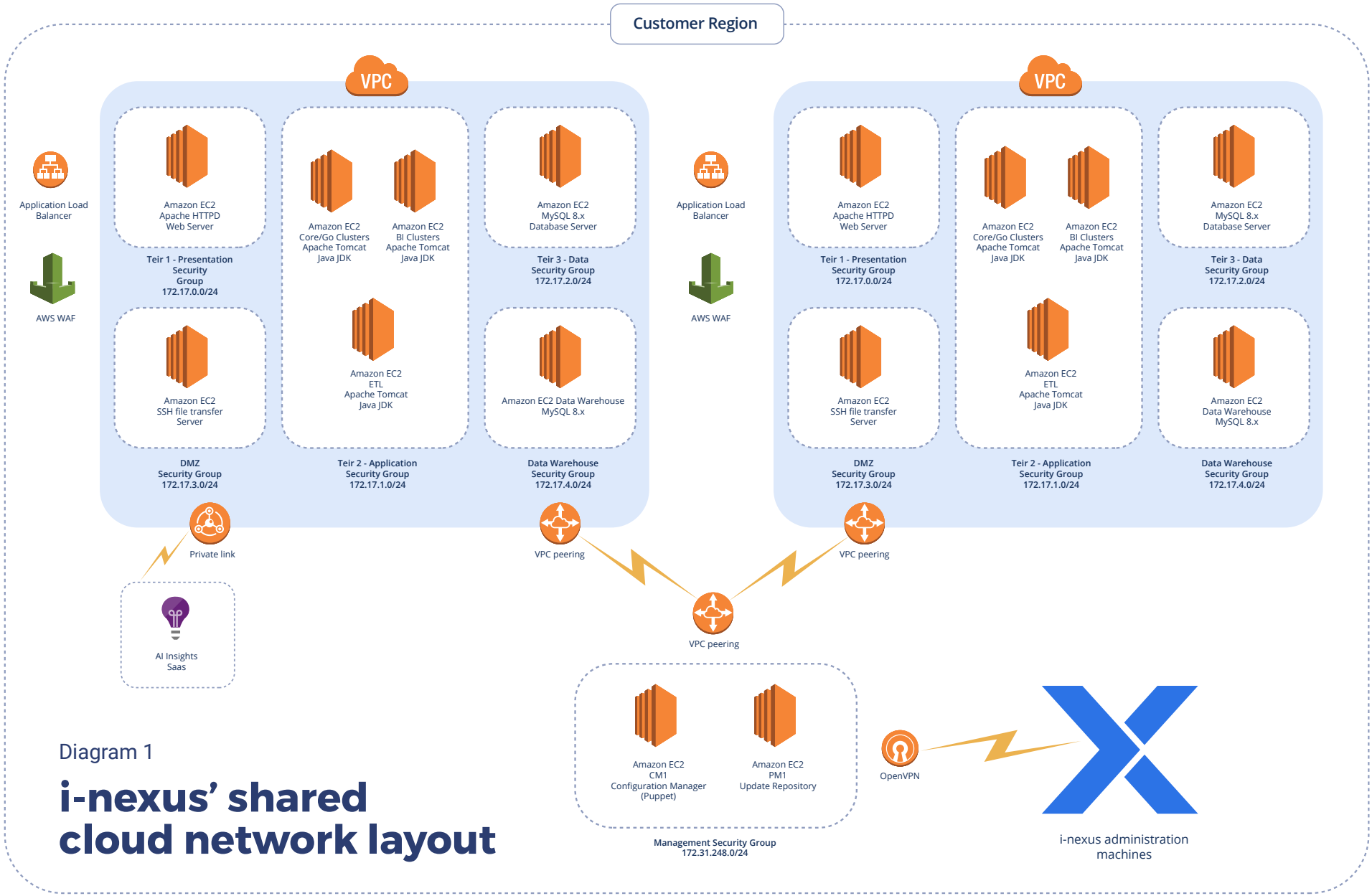


Diagram 1

i-nexus' shared cloud network layout

Management VPC

i-nexus has implemented a Management VPC that allows us to maintain no Internet access within our secure private cloud, whilst ensuring that our cloud servers remain fully up-to-date. The Management VPC contains i-nexus' Puppet configuration management servers and update repositories.

The management VPC is only accessible via a secure client to site VPN from i-nexus configured laptops/ desktops.

Administrative access to the AWS server infrastructure is via a hardened jump server in i-nexus' AWS Management VPC hosted in London. The Management VPC connects to each one of our cloud environments using secure site-to-site peering.

VPC automated provisioning

Each one of our VPCs is automatically deployed using a combination of AWS CloudFormation templates, Puppet & Pulp.

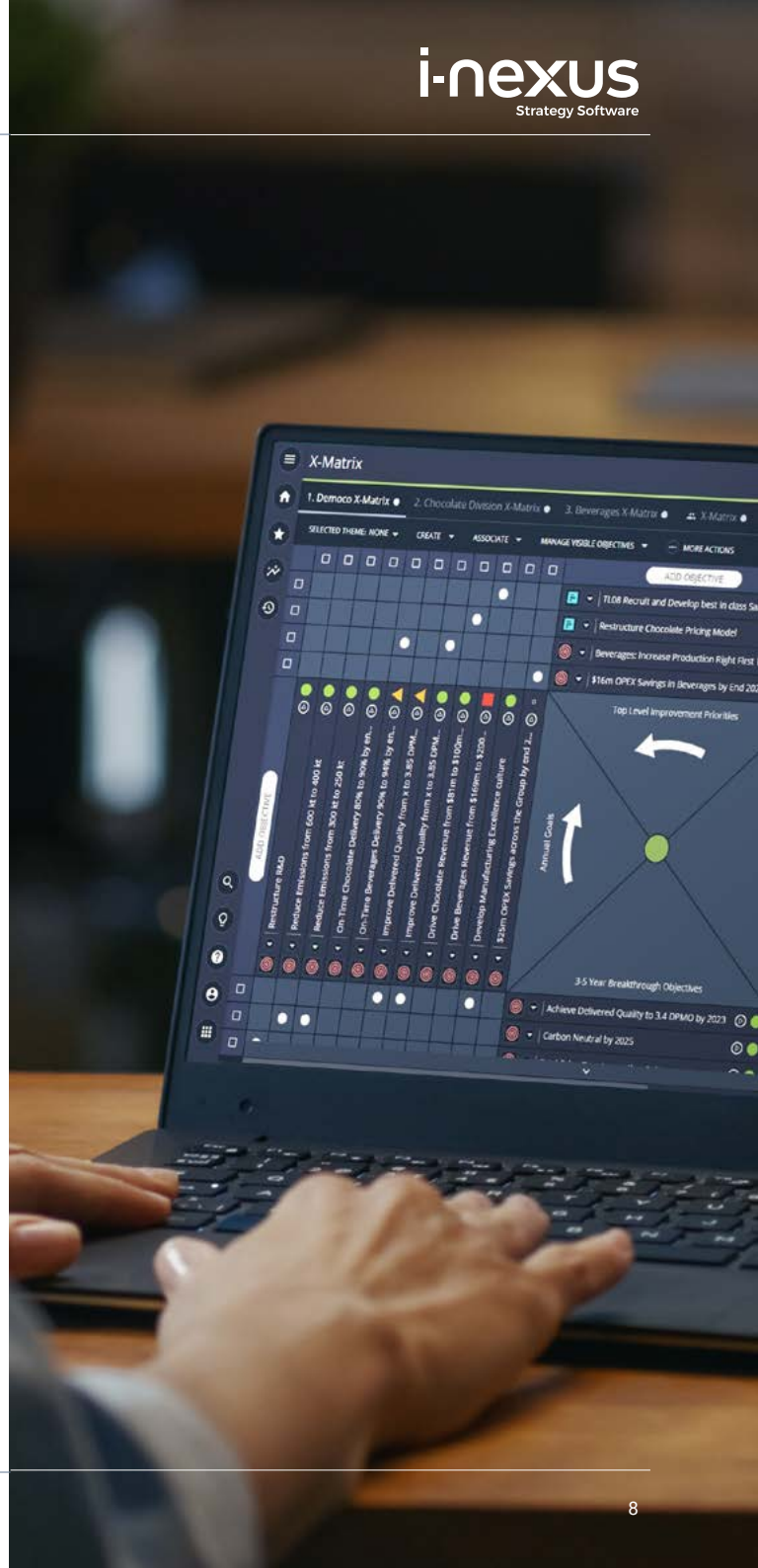
AWS templates allow us to provision the basic AWS VPC infrastructure using pre-hardened i-nexus Amazon machine images. With all non-essential services, ports and accounts disabled, maximum web security guaranteed and continuously monitored for any changes to the infrastructure.

Once the basic infrastructure has been provisioned via AWS CloudFormation, the servers automatically connect to i-nexus' central Puppet configuration management servers. Here, the security configuration is completed and any required services for effective operation are installed.

Finally, Pulp is our central repository server used to distribute updates to i-nexus' closed infrastructure.

AWS identify and access management

To further secure the system, all accounts with access to the AWS Management Console must have multi-factor authentication.



Cloud and application architecture

Customer requirements

To ensure that your organization can fully use and benefit from the features of the i-nexus software, customers must ensure:

- An appropriate web browser is used - typically Microsoft Edge, Mozilla Firefox or Google Chrome.
- The web browser is the current official release

SaaS

SaaS service

Shared service

In the standard shared SaaS model, the same physical architecture is used to deliver i-nexus securely to multiple customers. Each customer system runs in its own separate web application and has its own independent database, however, it is running on a platform of shared high-power hardware.

This way, each customer system remains logically distinct and secure, yet benefits from the economies of scale from shared hardware. i-nexus is not a multitenant system architecture, as each customer has their own instance of the software and separate database. Indeed, different customers can run different versions of the i-nexus software simultaneously on the same infrastructure.

Dedicated service

In some circumstances, customers may be unable to deploy on such shared infrastructure, for example, due to internal IT security rules or policies. In such cases, we can provide a separate and dedicated VPC within a specific AWS region without any part of it being shared with another customer.

Dedicated customers are assigned their own AWS VPC and all infrastructure within it. This allows customers to gain all the benefits of a SaaS deployment whilst still adhering to IT security rules and requirements.

Our dedicated environments can be tailored to suit individual customer requirements.

Database and data separation

Each customer instance is provisioned with its own separate database. i-nexus does not have any shared database schemas across our SaaS infrastructure.

Multiple domains

We maintain separate VPC infrastructures for each one of our Development, Test and Production environments. Furthermore, our AWS Development environment is completely closed with no access to or from the Internet.

Data encryption

All our instances in AWS have been built with security in mind. Because of this, i-nexus uses full disk encryption on every provisioned disk, a security baseline based on least privilege and access. All machines have external Internet access specifically blocked, with server access available only via a jump server in our management VLAN, and all databases have table space encryption applied to them.

Customer data in i-nexus is stored encrypted with each data store (Database, Documents & Backups) using a different set of access keys/ passwords. Data at rest is encrypted using AES256.

User Passwords stored in the database are stored as SHA256 hashes.

Backups are encrypted via AES256 linked to the originating machine.

New encryption keys are created on a monthly basis and an automation process ensures that this new key is replicated to all servers for use in all processes that generate data at rest or back-ups.

Data security

Data protection and GDPR

i-nexus is a Data Processor, i.e. it processes data on behalf of its customers - the Data Controller.

As such we will:

- Only act on the Controller's documented instructions
- Impose confidentiality obligations on all personnel who process the relevant data
- Ensure the security of the personal data that we process
- Abide by the rules regarding appointment of sub-processors
- Implement measures to assist the Controller in complying with the rights of data subjects
- Assist the Controller in obtaining approval from DPAs where required
- At the Controller's election, either return or destroy the personal data at the end of the relationship (except as required by EU or Member State law), and
- Provide the Controller with all information necessary to demonstrate compliance with the GDPR.

As a Processor there are a number of core requirements, we will review 2 specifically:

1. We must ensure that any personal data that we process are kept confidential.

We achieve this in a number of ways including that all persons authorized to process the personal data are under an appropriate obligation of confidentiality and more generally a suite of security, intrusion detection and vulnerability tests.

Penetration testing

Once a year, i-nexus conducts a full external penetration test with a third-party testing company to ensure that our systems are fully secured, up-to-date and free of vulnerabilities.

Any problems found are quickly rectified before the third-party company issues our certificate of compliance. Current certificates are available upon request.

Anti-virus AV scanning

i-nexus uses ESET Anti-Virus scanners on all servers with the latest virus updates synchronized daily.

Intrusion detection

i-nexus uses AWS WAF, a web application firewall that helps protect our customer's web application from common web exploits. This ensures the security and availability of applications and prevents consumption of excessive resources. AWS WAF gives control over which traffic to allow or block through customizable web security rules.

In addition to custom WAF rules we purchase a 3rd party set of managed rules. These provide rulesets that are regularly updated to include the latest threat alerts by using Cyber Threat Intelligence. The rulesets are designed to mitigate and minimize vulnerabilities, including all those on OWASP Top 10 Web Application Threats list and many managed rules targeting common vulnerabilities such as code injection techniques (SQLi, NoSQLi, OScommandi, etc), XSS, directory traversal and known exploits involving web-applications using technologies such as Apache Struts2/ Apache Tomcat/Oracle WebLogic/WordPress/Drupal/ Joomla! and Malicious Bots rulesets.

2. We must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

In addition to those measures identified above this is ensured by:

- Encryption of the personal data
- On-going reviews of security measures, and
- Redundancy and back-up facilities.

Accreditation to ISO 27001 provides further evidence that we meet these obligations.

Application identify and access management

i-nexus supports Single Sign On or Multi-Factor Authentication. Using Single Sign On, users gain the convenience of signing in once through one account, with security ensured through centralized user account management. Through SAML 2.0, web-based, cross-domain Single Sign On is enabled for i-nexus and supported on both Shared and Dedicated infrastructure.

Performance

Monitoring

All key system resources are monitoring using a combination of different monitoring systems. CPU, memory, Storage, database connections are monitored using Nagios.

Instana is used for application performance monitoring. Website uptime monitoring is carried out using new-relic.

i-nexus monitors over 4000 different data points on our infrastructure. This ensures that system performance continues to scale in-line with user number increases and each new software release.

Scalability and elasticity

i-nexus software is load and performance tested as part of every regression testing cycle to understand the impact of changes on performance between builds. This is an essential part of our software development process.

Every day, i-nexus is accessed by thousands of users contributing to over 100,000 projects. We stress-test and prove our security and reliability to ensure all customers can remain on-track via the system, even at the busiest times of the year.

Reliability

i-nexus has proven to be a highly available system and unscheduled downtime is a rare occurrence. In the unlikely event that it does occur, there are policies and procedures in place to ensure the outage is kept to a minimum.

We aim for, and maintain, an excellent uptime record for our SaaS application which exceeds the industry standard of 99.99%.

Continuity

To ensure the reliability and consistency of customer data, we operate a 3 stage backup process with automated data integrity testing:

Backup integrity testing

Twice a week, a full restore of the night's back-up is performed to check for any issues and ensure that, in the event of a disaster, fully-restorable customer data is always available.

Disaster recovery

For each of our cloud environments we host a mirror of that environment in the same geographical location but in a different availability zone. In the event of a disaster, our customers can be quickly migrated over to this mirror environment to minimise downtime.

Stage 1

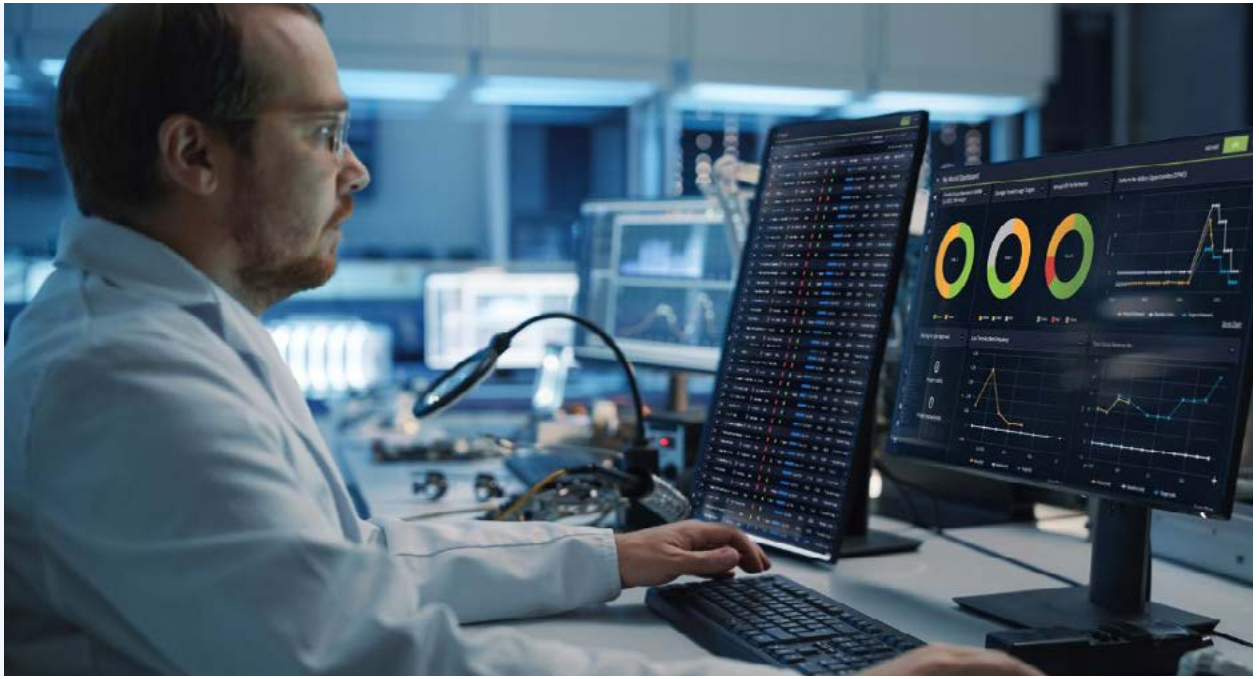
Master to multiple slave database real-time replication. If we lose one of our master database servers, one of our slaves will replace it with no loss of your data to the client.

Stage 2

Daily replication on one slave is paused so a backup can be taken. A full back-up of each individual system is taken, encrypted and stored locally on the server for 7 days.

Stage 3

Nightly full backups of the storage area are made to a secondary location. These are then replicated to multiple data centres in the same availability region.



Integration

i-nexus uses Jitterbit Harmony as its chosen ELT integration.

Jitterbit connects to over 1,000 end points for enterprise applications and databases, including:

- CRMs
- ERPs
- Financial platforms

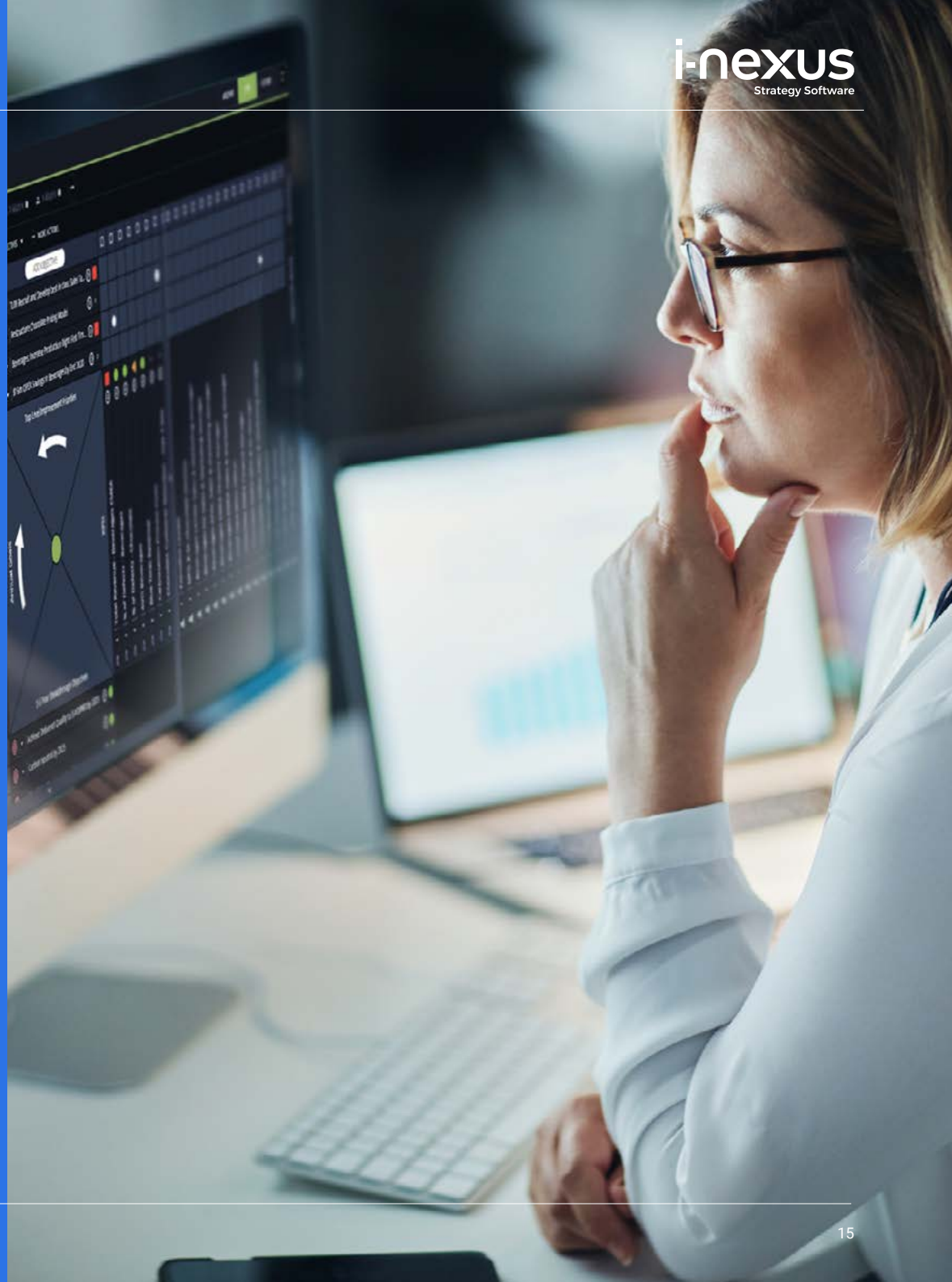
Jitterbit Harmony ensures quick, scalable and secure integrations with i-nexus and your other systems.

Customer support

As part of i-nexus' new customer on-boarding, all customers receive a Service Level Agreement detailing the support and services provided by i-nexus.

i-nexus customers benefit from an expert customer support team with detailed experience in the i-nexus system itself, as well as strategy execution best practice and processes.

As part of our ongoing customer support, all customers will receive advance notification of any scheduled maintenance events which are performed out of standard work hours.



Release management

Quality control and testing

All of i-nexus' software releases undertake strict quality control, using the following process:

1. All code is peer-reviewed before being included in the product. The peer-review includes an assessment of the testing undertaken by the developer as well as the code quality.
2. Developer tests are written at the lowest appropriate level. These are automated where possible.
3. Testing is then carried out by a test specialist at a functional level, to ensure that all new functionality meets the acceptance criteria for the business requirement.
4. Once this has been successfully completed, it is merged into the next release branch and rolled-out when a new release or software update is planned.

Release testing

Before anything is made available to i-nexus customers on our SaaS infrastructure, it undergoes a regression test. This consists of various user flows to test all the areas of the product typically experienced by end-users.

The Development Team identifies any areas of the product that may have been negatively impacted by a new change, for further exploratory testing and rectification.

The team also carries out regular 'regression weeks' where the following additional automated tests are undertaken:

- **Page transition test:** Establishes the loading time for different pages in the product.
- **Load test:** Establishes the response time of the product when multiple users log-in and perform different actions.
- **Financial Navigator performance test:** Establishes the current performance of the Financial Navigator using different custom views to measure loading time.
- **Bowling Chart performance test:** Measures the loading time of the Bowling Chart and certain actions like expanding and collapsing nodes.
- **Tree view performance test:** Creates, deletes, and edits projects from the 'My Projects' tree view.

The results of each test are compared by a test specialist against previously recorded results.

Again, any negative change in performance is investigated further and remediation work carried out as necessary. If such work is required, the automated tests are done again on completion, along with selected user flows in the changed area. This maintains the high quality of the i-nexus platform and user experience.

Pre-deployment testing

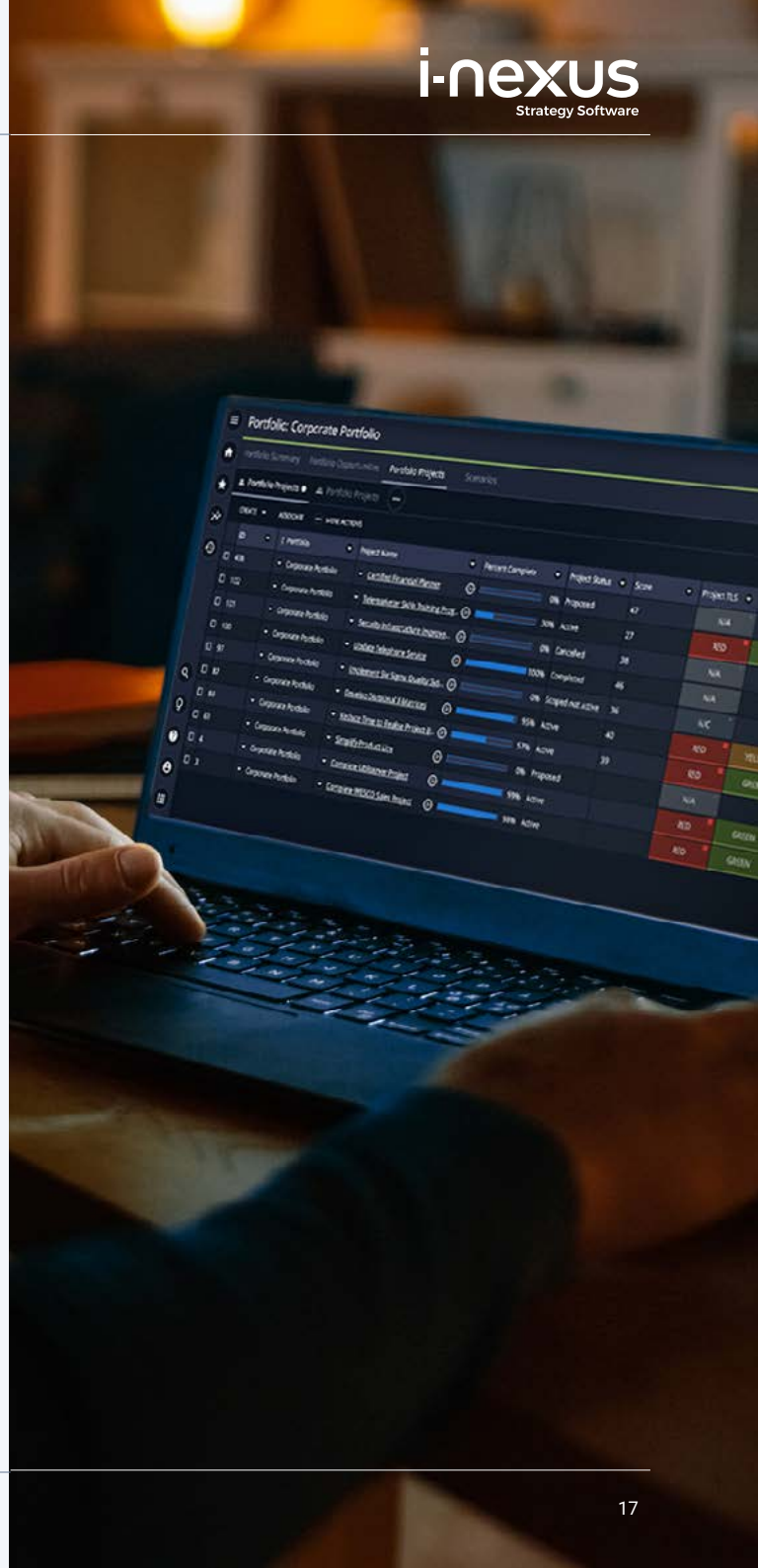
During each regression cycle, a pre-deployment test is carried out to establish that backup copies of live customer data can be updated to the new build without any issues. This test is carried out by the Technical Services department which is external to the Development Team. The Development Team do not have direct access to customer data or domains.

Any issues uncovered are reported to the Development Team, resolved, and the pre-deployment test is carried out again to ensure they are fixed.

Once all tests have been completed in in the regression cycle, a pre-release sanity test is performed by the Senior Test Specialist. This is a final check that all critical product functionality is available. After this final step, the build number to be deployed is supplied to the Cloud Operations Manager.

Release frequency

i-nexus uses an agile methodology to build and scale its software rapidly and readily respond to customer needs. Each release contains functional product enhancements, fixes for identified defects, and security and performance improvements. It is made available to our SaaS environment every six weeks, with eight SaaS releases, on average, per year.



SaaS release process

i-nexus provides all customers with a controlled release of all software to our SaaS environment.

The process is as follows:

1. SaaS upgrades are scheduled on weekends to ensure maximum availability during the working week.
2. The i-nexus SaaS upgrade/downtime window is between Friday 10:00 pm - Sunday 4:00 pm GMT/BST, however, domain downtime is generally less. This window allows for the deployment of any larger product releases. If a full outage time is needed, all customers will be advised well in advance.
3. The release date is scheduled to ensure on-call staff are available from Customer Services, Development and Cloud Operations Teams for full support coverage should any issues occur.
4. Customer Expert Users are notified by email of the next scheduled SaaS release date.
5. i-nexus supplies a detailed Software Release Bulletin and a set of release notes containing a full list of defect fixes in the build, prior to release deployment.
6. Domain downtime notifications are posted onto the affected domains before the upgrade.
7. Customers with test domains may request a staged release process to ensure that internal testing has been completed prior to the live domain upgrade.
8. Upgrades commence following the completion of nightly database back-ups for data security.
9. Technical Services confirm the release has been deployed successfully and advise Customer Services. i-nexus Customer Service conduct post-release sanity testing on upgraded domains and follow a thorough scripted testing process to confirm domains are available and core functionality is working as expected.

Should any urgent issues be located during the final release process the Release Manager will take responsibility to ensure the on-call team swiftly resolve them.

Customer-specific smoke testing

i-nexus can undertake customer-specific post-release testing to ensure custom configuration or bespoke functionality is working as expected following the release deployment. A customer testing script can be produced and provided as a formal i-nexus sign-off document for each release.

Customers who would like this are advised to discuss their additional upgrade testing requirements with Sales or their dedicated Account Manager.

Next steps

The security, quality, performance and robustness of the i-nexus platform is of utmost importance to everyone at i-nexus.

This guide has set out to comprehensively cover i-nexus' Information Security, product release and data protection policies. However, it doesn't have all the answers.

Our team are on-hand to answer any further questions you may have regarding Information Security, customer requirements or any other aspect of this guide.

No matter how big or small, we'll answer every question.

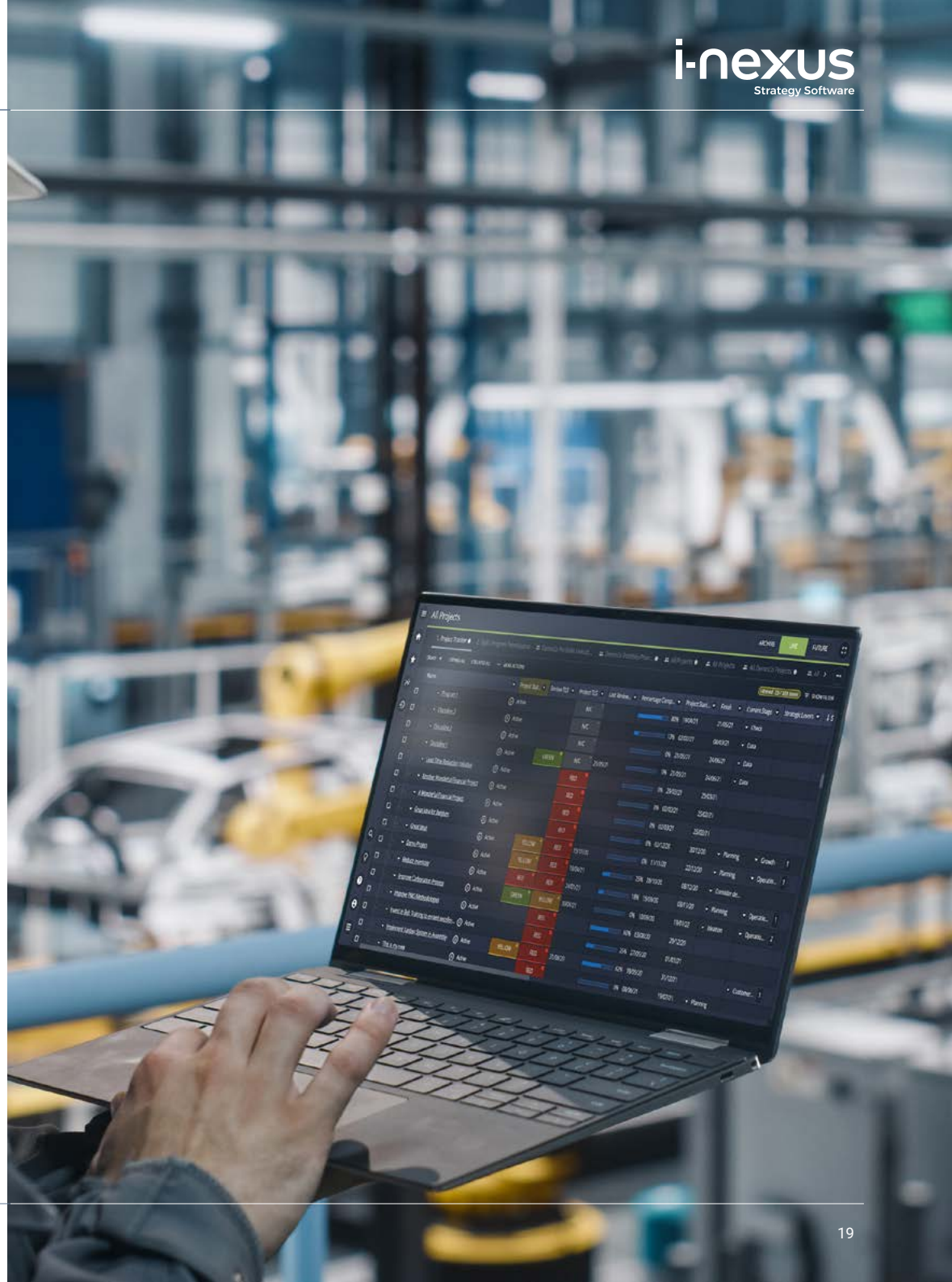
How to reach us

To get in touch with any questions, reach out to the team via the below channels:

Email: info@i-nexus.com

Web: www.i-nexus.com/contact-us

Phone: UK: +44 (0)845 607 0061 | USA: +1 855 615 1589



Trusted by global organizations

> We needed saving from spreadsheet hell. i-nexus transformed our Hoshin Kanri method, replacing spreadsheets with a digital solution. Better still, i-nexus has enabled us to take the next evolutionary step beyond KPI reporting and towards building a stronger countermeasure culture.

UNIVERSAL ROBOTS

Mogens Saigal, Senior Director, Universal Robots A/S

Discover the better way to achieve your goals
Watch i-nexus in action by visiting i-nexus.com today

UK: +44 (0)845 607 0061
USA: +1 855 615 1589
info@i-nexus.com