QAD Security Whitepaper

QAD is dedicated to providing secure manufacturing and supply chain solutions, helping our customers thrive in a competitive, high-risk, and ever-changing world. We invest heavily in security and are committed to continual improvement. This whitepaper outlines our comprehensive approach to ensuring business continuity, data confidentiality, integrity, and availability.

Compliance

QAD adheres to rigorous industry standards and regulations to maintain the highest levels of security and compliance.

Certifications and Attestations

- **ISO 27001**: QAD is certified under the ISO 27001 standard, which specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). This certification demonstrates our commitment to managing and protecting company and customer information.
- **ISO 20000:** QAD is certified under the ISO 20000 standard, which specifies requirements for service providers to plan, establish, implement, operate, monitor, review, and improve Service Management System.
- **SOC 1 / SOC 2 Type II**: Our SOC 2 Type II report attests to the security, availability, and confidentiality of the systems we use to process user data. This annual audit provides an in-depth review of the operational effectiveness of our controls.
- **CSA Star**: QAD's participation in the Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) registry highlights our dedication to cloud security transparency.
- **TISAX** (Trusted Information Security Assessment Exchange): QAD maintains certifications in TISAX, specifically tailored for the automotive industry, ensuring secure and trusted data exchanges between manufacturers, suppliers, and service providers. This attestation applies to QAD Supplier Relationship Management

Data Collection

- QAD Products capture First and Last Names, usernames, and business email addresses, and general usage information. Some products also allow for phone number capture to provide SMS notifications.

Regulatory Compliance

QAD ensures compliance with global regulations to protect personal data and maintain customer trust. Our compliance practices align with industry standards such as NIST, which provides a framework for improving our security posture.

- **NIST** Framework: QAD follows the NIST Cybersecurity Framework to guide our security practices, including risk management, security controls, and incident response.
- **GDPR**: QAD complies with the General Data Protection Regulation (GDPR), ensuring that we protect individuals' privacy and personal data within the European Union.

Organizational Security

QAD's security program is governed by a risk-based approach, ensuring robust security practices across our products and operations.

Security Steering Committee

The Security Steering Committee at QAD sets the enterprise security strategy and oversees the execution of the security program. This committee ensures that all security initiatives align with our business objectives and regulatory requirements.

Risk Management

We conduct regular risk assessments to identify and mitigate potential security risks. Our risk management process includes:

- Identification: Recognizing potential threats and vulnerabilities.
- Assessment: Evaluating the impact and likelihood of identified risks.
- Mitigation: Implementing measures to reduce or eliminate risks.
- Monitoring: Continuously tracking the effectiveness of risk mitigation efforts.

Key Security Policies

Our comprehensive information security policies and standards govern all security aspects at QAD. Key policies include:

- **Acceptable Use Policy:** The Acceptable Use Policy defines the acceptable and prohibited uses of QAD systems and data to ensure all users adhere to security and ethical guidelines. This policy covers user responsibilities, data handling, and restrictions on unauthorized activities to protect QAD's digital assets. Compliance with this policy helps maintain a secure and efficient work environment.
- **Data Protection Policy:** The Data Protection Policy outlines QAD's measures to safeguard sensitive information from unauthorized access, alteration, and disclosure. This includes data encryption, access controls, and regular audits to ensure compliance with data protection regulations. The policy also defines procedures for handling data breaches and protecting personal data.
- **Access Control Policy:** The Access Control Policy establishes clear procedures for granting, modifying, and revoking access to QAD systems based on the principle of least privilege. This policy ensures that users have the appropriate level of access required for their roles, minimizing the risk of unauthorized access. Regular reviews and recertifications of access permissions help maintain the integrity and security of QAD systems.
- **Incident Response Policy:** The Incident Response Policy details QAD's comprehensive approach to detecting, responding to, and recovering from security incidents. This includes predefined procedures for incident identification, containment, eradication, and recovery to minimize impact. The policy also emphasizes regular training and incident response exercises to ensure readiness and continuous improvement.
- **Secure Software Development Lifecycle**: QAD's product security encompasses authentication, authorization, encryption, and network security requirements. Source code controls, static and dynamic code assessments, and threat modeling identify and mitigate security flaws. We also validate open-source and third-party software, conduct security testing, and review overall security practices to ensure robust protection.
- **Asset Management:** QAD has established a formal Asset Management policy to facilitate effective management, control, and maintenance of the assets/information to its operational environment by classifying assets as per the functionality and criticality. This policy helps to identify, classify, label, and handle Information Assets of QAD, and to apply protection mechanisms corresponding with the level of confidentiality and sensitivity.
- **Data Classification Policy**: The Data Classification Policy defines the framework for categorizing QAD's data based on its sensitivity and criticality. By systematically classifying data, QAD can effectively manage and safeguard its information assets, ensuring compliance with regulatory requirements and minimizing the risk of data breaches. Regular audits and reviews of data classification help maintain the accuracy and relevance of classifications.

Security Awareness and Training

- **Security Onboarding Training:** All new employees and contractors must undergo human-led training and video-based training and testing.
- **Annual Security Awareness Training**: All QAD employees undergo annual training to stay informed about the latest security threats and best practices.
- **Secure Development Training**: Developers receive annual training on secure coding practices and secure software development lifecycle (SDLC) methodologies.
- **Phishing Simulations**: Regular phishing simulations are conducted to test and improve employee awareness and response to phishing attacks.

Third-Party Risk Management

- Formal Vendor Assessment Process: Vendors undergo a formal assessment process to evaluate their security practices.
- Screening and Oversight: Continuous screening and oversight help identify and address potential risks.
- Potential risks are discussed with subprocessors and critical vendors during periodic reviews.

Infrastructure & Endpoint Security

QAD employs robust security measures to protect our infrastructure and endpoints.

Identity and Access Management

Our identity and access management (IAM) practices ensure that only authorized individuals can access necessary systems and data.

- **Least-Privilege Access**: Access is granted based on the principle of least privilege, ensuring users have only the permissions necessary for their roles.
- **Periodic Access Recertification**: Regular reviews of access permissions ensure that users' access remains appropriate over time.
- **Privileged Access Management**: Elevated privileges are tightly controlled and monitored.
- **Zero Trust Framework**: To deliver defense-in-depth, the principle of network segmentation and user segregation is followed at the application and service layers. All remote connectivity is through secure protocols.

Network Security

QAD's network security measures protect against unauthorized access and attacks.

- **Anomaly Detection**: We use advanced anomaly detection systems to identify unusual activity that may indicate a security threat.
- **Network Detection and Response (NDR)**: Our NDR systems monitor network traffic for signs of malicious activity and respond accordingly.
- **Endpoint Detection and Response (EDR)**: EDR solutions provide real-time monitoring and analysis of endpoint activity to detect and respond to threats.
- **Anti-DDoS** Protection: Anti-DDoS measures are in place to protect our web products from distributed denial-of-service attacks.

Data Protection

- **Encryption**: Data encryption at rest and in transit is available to protect against unauthorized access.
- **Data Classification**: Data is classified based on sensitivity and criticality, ensuring appropriate protection measures are applied.
- **Backups**: Regular data backups ensure data can be recovered during a data loss incident. Production environments are retained for 30 days. Backups are stored in a geographically separate site.

Endpoint Security

- **Mobile Device Management** (MDM): MDM software manages and secures mobile devices used by QAD employees.
- **Web Filtering**: Web filtering tools on workstations block access to malicious websites and content.
- **Vulnerability Scanning and Patching**: Regular scans identify vulnerabilities, and timely patches are applied to address them.

Physical Security

QAD's physical security is managed in partnership with our hosting providers, ensuring the protection of our global infrastructure.

Key Hosting Providers

Our hosting providers, including IBM, Alibaba, Flexential, and AWS, implement robust physical security measures to protect our data centers. Hosting solutions are selected by region and by product.

- Flexential
- IBM
- AWS

- Alibaba

Security Operations

QAD's security operations team and Crowdstrike's Falcon Complete team work around the clock to monitor and respond to security incidents.

Incident Response

Our incident response capabilities ensure a swift and effective response to security incidents. Information around events will be made available on the QAD Trust Center, with real-time information at status.rzsoftware.com and qad.statuspage.io

- **24x7x365 Monitoring**: Continuous monitoring teams detect, respond, and respond to security threats in real-time. QAD uses third party services to augment internal teams.
- **Incident Response Exercises**: Regular exercises test and improve our incident response plans.
- **Real-Time Alerts**: Security alerts are triaged and escalated as necessary to protect our environments and customers.

Threat Intelligence

QAD leverages a third-party service to enhance our threat intelligence capabilities. This service aids in the collection and monitoring of information available on the dark web and other marketplace areas, providing critical insights into potential threats. Additionally, it helps monitor for threats to our organization and industry as a whole, ensuring that we stay ahead of emerging security risks and maintain robust protection against cyber threats.

Security Logging

- **Event Logging:** Security events are logged and maintained for one year to support forensic analysis and compliance requirements.

Business Continuity and Disaster Recovery

Our business continuity and disaster recovery (BCDR) plans ensure we can maintain operations and recover quickly from disruptions.

- **Documented Plans**: BCDR plans are documented and communicated to relevant stakeholders.
- **Regular Testing**: Plans are tested regularly to ensure they remain effective and relevant.

Shared Responsibility Model

Security within QAD Cloud products is a shared responsibility between QAD and our customers. To securely operate in the QAD Cloud, customers must understand and fulfill their security and compliance responsibilities.

Customer Responsibilities

- **Data Protection**: Customers are responsible for protecting the data they control, including implementing strong password policies and access controls.
- **Configuration Management**: Customers must securely configure and manage their virtual hosts, containers, storage, file systems, and applications.
- **Endpoint Security**: Ensuring the security of devices that access QAD Cloud resources, including using up-to-date antivirus software and applying security patches.
- **Incident Reporting**: Promptly reporting any suspicious activity or potential vulnerabilities to QAD.
- **Security Training**: Ensuring that personnel accessing QAD Cloud resources undergo appropriate security awareness training and understand their role in maintaining security.
- **Automation and OT Networks**: The customer is responsible for securely connecting scanners, printers, PLCs, and other plant equipment to the cloud. Ensure a secure design when deciding to connect OT equipment to the cloud.

QAD Responsibilities

- QAD provides a secure network infrastructure, including platform security, virtual private networking, load balancing, DNS, and gateways.
- QAD and our customers share the responsibility of ensuring optimal configurations of network access controls.
- QAD is responsible for providing hardened, secure systems, protecting and securing the operating systems against attacks, patch management, and vulnerability mitigations and remediations.
- QAD provides identity lifecycle management, authentication, authorization, and attestation services.

Responsible Disclosure Program

QAD encourages the responsible reporting of vulnerabilities to improve the security of our products and services. Security researchers and others can report vulnerabilities to security@qad.com.

From all of us at QAD: ***Be Vigilant. Be Secure!***