Automating Peace of Mind

Automation Anywhere Enterprise A2019 Combines Security and Scalability with Productivity and Cost Savings

You see the value of Robotic Process Automation (RPA) in increasing productivity and lowering operating costs. And you understand why Automation Anywhere Enterprise A2019 is the path to efficiency, standardization, and cost reductions. As the industry's first purely web-based, cloud-native, intelligent RPA platform, it provides a highly intuitive, consumer-like interface for all users—whether technically savvy or professionally trained. Users can build powerful bots at all levels, instantly. Quick to implement, scalable on-demand across the world's best-known cloud platforms, and capable of working at capacity non-stop, it harnesses the power of a Digital Workforce. It lets you automate processes such as invoicing, logistics, customer interaction, and much more.

At the same time, you want to manage all your automation work and resources in one centralized location on the cloud. But questions remain:

1. Will my company's data and processes be private and protected from other companies' data while in the cloud?
2. How is my data protected from external threats? From insider actions?
3. How can we maintain compliance with important regulations?
4. Underlying everything, will Enterprise A2019 be robust and available all the time, bringing the speed and accuracy my users expect?

The good news? Our cloud-based offering brings all the security and capabilities you need, with the added benefits of a cloud-based solution.

ENTERPRISE A2019 OVERVIEW

Automation Anywhere Enterprise A2019 enables your people to automate business processes on their own, in real-time, without changing any parts of existing processes. Business users build bots using our cloud-hosted bot creation capabilities; they can deploy and run Bot Runner nodes on their infrastructure through a secure, encrypted channel. A cloud-hosted Control Room makes it easy to monitor and manage bots.

PRIVACY AND CONFIDENTIALITY PROTECTIONS

Enterprise A2019 was built with a data-privacy-first approach. Three important safeguards support this approach:

1. Multi-tenant architecture with granular role-based access control (RBAC) capabilities
2. Latest encryption standards for data in motion and data at rest
3. Strong authentication and authorization

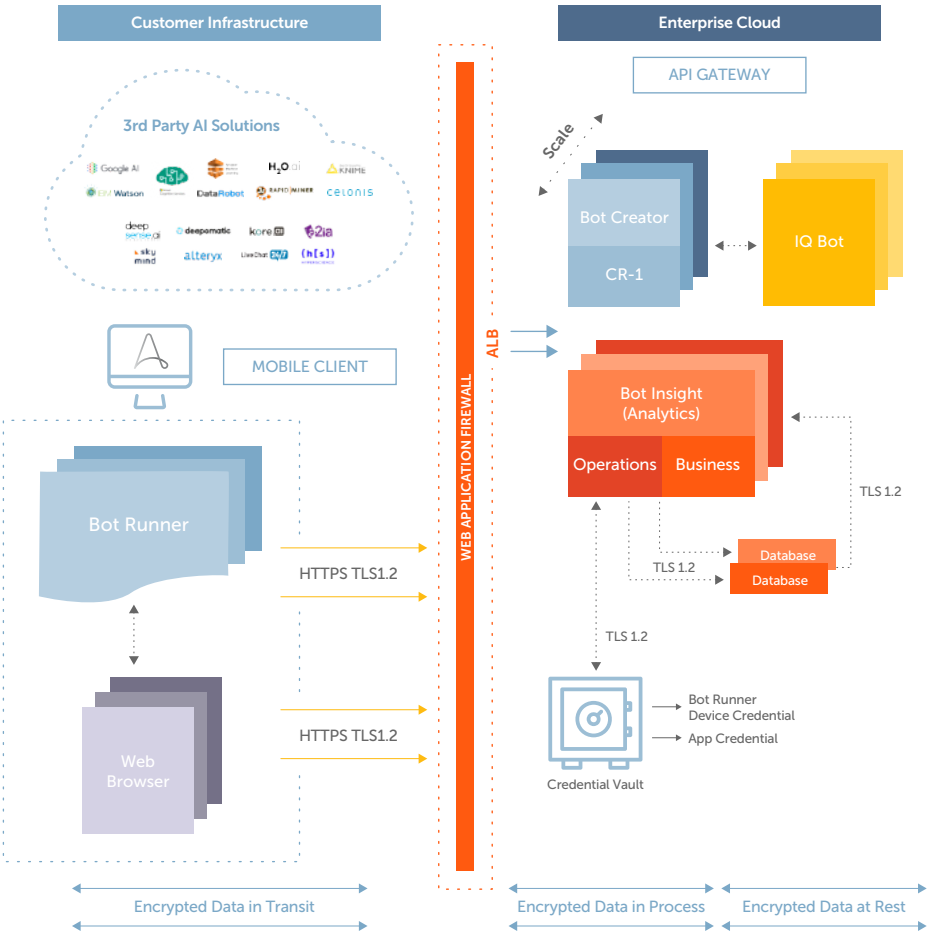


Illustration 1: Authentication Automation Enterprise A2019 Secure Deployment

Our multi-tenant architecture separates your processes and data from other tenants. You'll receive a unique tenant ID, generated when you become a tenant, which gets stored in a protected database. Tenants can only access their data and Control Room—no one else's. All Control Room instances, IQ Bot instances, and datastores are inside a private network on private subnets with no direct access to the internet. The data and processes of each customer are kept separate from and untouchable by any other tenant on the cloud infrastructure. Each tenant has a unique URL, and tenant user credentials are encrypted and stored in a secure vault. Additional runtime protections include bots operating in stealth mode, distributed credential protection, time limits, and more.

To protect the data that is moving to and from the cloud, we encrypt traffic with HTTPS and SSL/TLS 1.2. For added protection, the connection into the cloud-hosted Control Room is initiated by the Bot Runners/agents.

Data at rest (including local credentials, uploaded documents, and select runtime data used by bots) is encrypted using AES 256. This means that data, whether in motion or at rest, is encrypted using industry-standard encryption techniques.

A third key element is strict authentication and authorization control enforcement. On the customer side, the RPA system administrator defines individual users' authorization to access specific resources and to perform particular actions through role-based access control (RBAC).

Enterprise A2019 provides the industry's most comprehensive bank-grade security and governance, with the ability to enforce fine-grained RBAC at scale. Authentication mechanisms include native Active Directory integration using Kerberos and LDAP, as well as single sign-on (SSO) using SAML 2.0. A2019 can also be integrated with multi-factor authentication systems.

A user attempting to access a resource is first authenticated. On the authentication side, we maintain proper controls for requesting, approving, revoking, and revalidating cloud operations staff's access to the cloud infrastructure. Only employees with a clear business need can have access, and all requests are approved based on individual role-based access, which is reviewed regularly to validate the continued business need.

CLOUD SECURITY AND THREAT DEFENSE

To protect Enterprise A2019 from external threats or insider actions, we have taken several security measures as well as implemented segregation of duties.

The entire infrastructure is front-ended by a web application firewall (WAF), and continuous vulnerability scans are completed frequently. Protection against known and unknown external threats is done by antivirus software, anti-malware solutions, and other controls to ensure that malicious software does not gain unauthorized access to customer content. We also use threat intelligence for intrusion detection, with IDS/IPS systems, anomaly detection, DNS log and network flow log inspection, and attack prevention capabilities. This protection is augmented with 24/7 monitoring for DDoS attacks and the OWASP Top 10 threats. Penetration testing is carried out by a third-party security testing organization at least every three months.

Enterprise A2019 prevents fraud and manual errors through strict separation of duties. Customers can use the role creation wizard to define which users have access to individual tasks or broad sets of functionalities such as Control Room, IQ Bot objects, and functions, including user management, bot schedules, and audit logs. This helps ensure that only specific individuals can take potentially impactful actions. In addition, strict control over requests for access, approvals, revocations, or revalidations to our cloud infrastructure is maintained. The need for access is reevaluated periodically to ensure that all requests are validated.

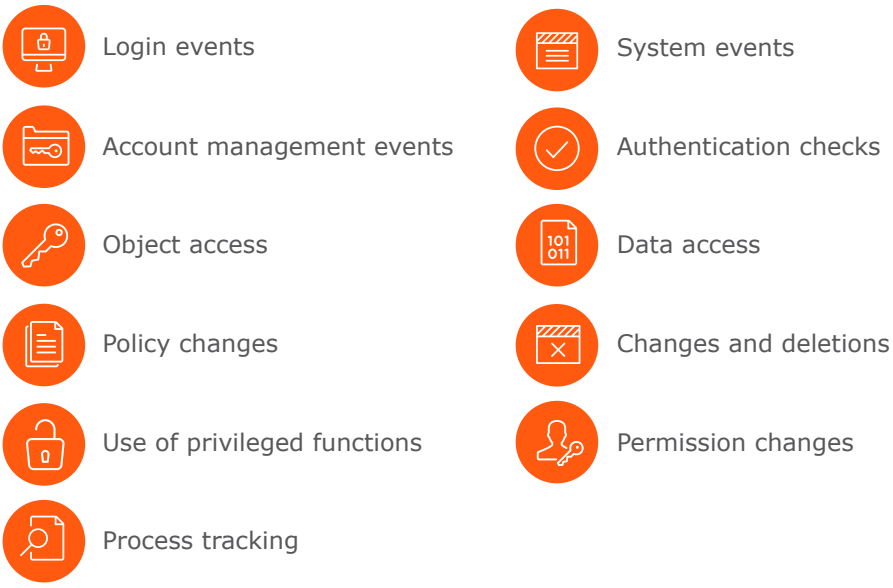
REGULATORY COMPLIANCE

Automation Anywhere is the first RPA vendor to achieve SOC 2 Type 1 compliance. Enterprise A2019 supports the FISMA moderate controls that are required for the major compliance frameworks such as PCI-DSS, SOX, and HIPAA. Enterprise A2019 is in the process of being ISO 27001 certified. Automation Anywhere participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. The platform is also Veracode Verified Continuous certified, which is the highest level of the Veracode Verified program and builds on the security processes embedded in the software development lifecycle.

Enterprise A2019 employs a robust logging system that forms the basis for compliance and provides full audit capabilities. User actions are audited within the platform to provide records of all access and actions taken by operations personnel. This includes successful and unsuccessful login events, object access, process tracking, and detailed information related to web applications.

All logs for individual tenant organizations are stored in an encrypted NoSQL data store. Access to the audit records is restricted through RBAC to enforce the principles of least privilege and separation of duties. Importantly, auditing is automated for all privileged and non-privileged roles, which ensures conformance to best practices as defined in NIST AC-6. Enterprise A2019 automates the offloading of audit records to a SIEM, eliminating much of the labor-intensive work normally associated with a regulatory compliance audit.

Enterprise A2019 Logs Events and Actions:



AVAILABILITY AND SCALABILITY

Cloud applications need to run on a robust, compliant, safe, and available platform. Constant, consistent availability calls for a solid foundation and robust processes. Enterprise A2019 provides full-fledged high availability (HA) and disaster recovery (DR), not just at the server level but down to the bot level and across multiple locations in the event of an interruption. For high availability, Enterprise A2019 delivers RPA as a service by leveraging the public cloud, with the cloud infrastructure deployed across multiple availability zones. Customers can be confident in performance and business continuity.

In terms of disaster recovery, emergency and contingency plans are in place for the cloud infrastructure where systems that process customer content are hosted. Production data centers have been designed with high availability in mind, based on the resiliency of the network and compute infrastructure. Backups, redundant storage, and data recovery procedures are designed to reconstruct customer content in its original or last-replicated state.

CLOUD BRINGS ADDITIONAL BENEFITS

Enterprise A2019 delivers all the expected benefits of RPA: increased productivity, decreased operating costs, more efficiency, and standardization. Yet, being cloud-based brings additional benefits of speed, cost savings, ease of use, and scalability.

With a cloud infrastructure, there is no need to wait for the rollout of new functionality. Enhancements to any aspect of the solution are available immediately, with no action required on the part of the customer.

Costs are dramatically lower since there is no hardware to purchase, configure, maintain, or manage.

The solution is easy to deploy because it is ready to provision immediately, and it supports software and bot development lifecycle management with policies centrally enforced by administrators. When changes are needed to user access rights, schedules, or policies, they can be implemented at once without requiring professional services teams or unwanted delays.

Scalability is another significant benefit of the cloud infrastructure. It can handle unexpected surges in workload demand. Enterprise A2109 can support even the most dramatic changes in automation workloads without missing a beat.

WHY MOVE TO ENTERPRISE A2019 NOW?

Enterprise A2019 can provide a powerful, intuitive way of empowering your workforce. Open and integrated, intelligent and connected, it lets you operate with enterprise-grade security and auditability. At Automation Anywhere, we have gone to great lengths to ensure that our solution meets all the requirements of cloud security:

Credential and key management

Encryption of data in transit and at rest

Logging and auditing

Data management and secure storage

Privileged access

Security/privacy/ legal review

Regulated data security controls

Our mission is to enable companies to operate with peace of mind, unprecedented productivity, and efficiency by automating any part of the enterprise that can be automated. With Enterprise A2019, there's no need to worry about your data and processes being kept private and protected from other companies' data in the cloud. Rest assured that they are protected from external threats and insider actions. Compliance is no longer an issue, with comprehensive logging. This robust, available, high-performance platform brings you the speed and accuracy your users expect, without worries about cloud security.

For more information, go to https://www.automationanywhere.com/solutions/rpa-security

Automation Anywhere www.automationanywhere.com

North America: 1-888-484-3535 x1 | International: 1-408-834-7676 x1

@AutomationAnywh www.linkedin.com/company/automation-anywhere sales@automationanywhere.com