SaaS Security and Compliance Whitepaper

Table of Contents

Introduction

As the world's seventh largest pure-play software company we are committed to provide state-of-the-art application designs, security products, and cloud platform facilities.

The standard way that security, privacy, reliability, availability, integrity, scalability, and recoverability of the solution are represented is through compliance, like requirements and implementation guides, compliance profiles have a list of “controls”, we compare our SaaS solution including its technology and operations against these controls.

The checklist covers everything from technology design and deployment to the day-to-day operational aspects of policies and procedures.
As mentioned, these checklists are provided by industry and standards organizations such as CSA and NIST. These two are more focused on technology. There are other profiles more focused on operations. A popular one comes from the International Standards Organization (ISO), called ISO 27001.

Nowadays, when enterprises want to understand a SaaS offering’s assurances around security, privacy, reliability, availability, integrity, scalability, and recoverability, they will ask for an “attestation” or “certification” to one or more of the above compliance profiles.

This paper sets out the Micro Focus directions on compliance and explains our technical and operations approach in many important areas of security, privacy, reliability, availability, integrity, scalability, and recoverability.

Data Handling

Micro Focus employs a multi-tier, multi-datacenter data-ingestion pipeline to process data securely. The Micro Focus ingestion pipeline includes network devices that can process data from multiple inputs.
Our customers choose what information to store/process within the application, all client's data is labeled and treated as confidential.

The data does not leave our application and never leaves the cloud; it is only accessed through the application by a properly credentialed and entitled user. Data as it is stored in our system is always stored in a cryptographically encrypted form, as will be explained below.

Public Cloud Platform

Most of Micro Focus SaaS applications runs on Amazon Web Services (AWS). Cloud security is one of AWS' highest priorities. As an AWS customer, we and therefore our enterprise customers benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.
The AWS infrastructure puts strong safeguards in place to help protect customer privacy.
All data is stored in highly secure AWS data centers, AWS manages dozens of compliance programs in its infrastructure, this means that all of the datacenter related portions of our compliance profiles have already been completed, it allows us to maintain the highest standard of security.
Finally, the AWS security design is such that security scales with our AWS cloud usage. No matter the size of our business, the AWS infrastructure is designed to keep data safe.
One of the key features of AWS is that it enables us to implement business continuity with replication between applications and data across multiple data centers in the same region using availability zones.
While doing so, we also retain a complete control and ownership over the region in which our data is physically located, making it easy to meet regional compliance and data residency.
requirements.

AWS provides several security capabilities and services to increase privacy and control network access, these include:

- Network firewalls built into Amazon VPC and web application firewall capabilities in AWS WAF let us create private networks and control access to instances and applications
- Encryption in transit with TLS across all services

Availability is of paramount importance in the cloud. AWS customers benefit from AWS services and technologies built from the ground up to provide better resilience in the face of DDoS attacks. We use a combination of AWS services to implement a defensive in-depth strategy and thwart attacks. AWS offers a range of tools to allow us to move fast while still ensuring that our cloud resources comply with organizational standards and best practices.
AWS services include:

- **Trusted Advisor** - focuses on networks, storage, and user access.
- Deployments for vulnerabilities or deviations from best practices including impacted networks, OS, and attached storage
- Deployment tools to manage the creation and decommissioning of AWS resources according to organization standards
- Inventory and configuration management tools, including **AWS Config**, that identify AWS resources and then track and manage changes to those resources over time
- Template definition and management tools, including **AWS CloudFormation**, to create standard, pre-configured environments and Terraform for deployment

AWS provides tools and features that enable us to see exactly what's happening in our AWS environment, this includes:

- Deep visibility into API calls through **AWS CloudTrail**, including who, what, and from where calls were made
- Alert notifications through **Amazon CloudWatch** when specific events occur, or thresholds are exceeded

Compliance

Hosting our SaaS infrastructure on AWS creates a shared responsibility model between Micro Focus and AWS. This shared model reduces our operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.
Because the AWS cloud infrastructure comes with so many built-in security features, we can simply focus on the security of our guest operating system (including updates and security patches), our application software as well as configuration of the AWS-provided security features such as firewalls and configuration monitors.

ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

We are ISO 27001:2013 certified
ISO 27001:2013 demonstrates implementation and maintenance for the highest security standards controls, assuring secure delivery of Micro Focus software products and SaaS operations.

We are ISO 27034-1 certified

ISO 27034-1 application security standard, demonstrates proactive integration of security as part of Micro Focus software development lifecycle.

Security and Risk Management

We have just reviewed in detail the Micro Focus compliance programs, these programs use standardized compliance profiles because these are the ways which the industry has developed to express assurances around software-based services.
These compliance profiles require a certain amount of formality and rigor around how we work, how we develop and deploy our solutions, and how we operationally run our service.
Behind this formality, we have taken specific actions in the delivery of our services to fulfill these requirements.
The following sections describe, in “non-formal terms,” some of the actions we’ve taken to ensure the following:

- Our systems are designed with security capabilities. They will withstand security attacks of several forms, from denial of service to vulnerability exploits to malware.
- We build them with professional, documented processes. Important decisions are made carefully and are documented. Mistakes can be easily detected and reversed.
- We respect our customers' data in our stewardship of it as well as in their privacy. In no case will we lose their hard-earned work.
- Our systems will be highly available, so they can count on using them when they need them. If there are unforeseen problems such as hardware or network failures, our platform will respond and take actions to continue working.
- Our people are of the highest integrity; everyone knows their job and knows how to expedite processes through the company as needed to deliver our services.
- We regularly monitor and test our systems against attacks and poor performance and to make sure preventative mechanisms are working.

Secure Software Design Lifecycle

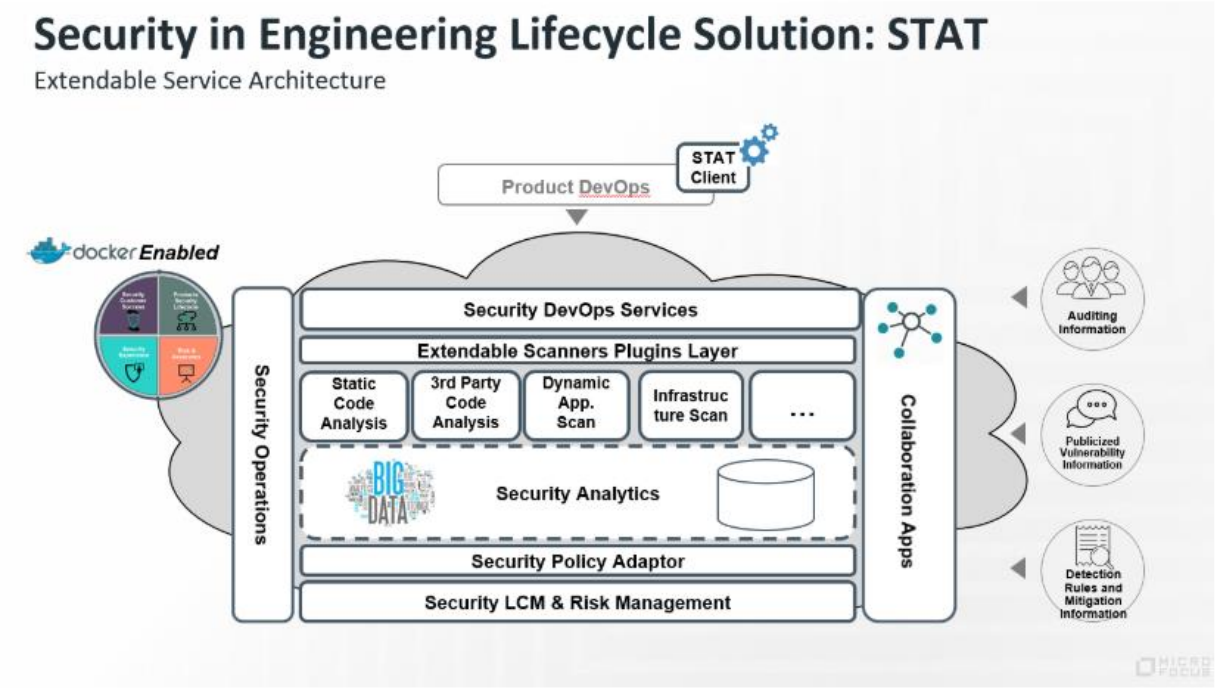
The Security Development Lifecycle (SDL) is a security assurance process that is focused on software development. As a company-wide initiative and a mandatory policy, we “design in” security from the start. At Micro Focus, the SDL is based on three core concepts—education, continuous process improvement, and accountability.

Micro Focus conduct penetration tests for its applications, the assessment findings are being remediate according to our SDLC program SLA’s, critical findings are mitigated immediately, and a patch is being released.

In addition, Micro Focus conduct automatic scans with internal platform called STAT.

STAT is an Automatic Security Testing platform for Agile and DEVOPS, used daily to automatically scan source code and apps, and intercept new vulnerabilities in a near-real-time manner.

The following tools are part of these scans: Webinspect, OWASP Dependency, Checker, CoreOS Clair, Fortify and Nessus.



Access Management

Access control to resources is a core security measure and as such must be controlled and enforced by policy. The purpose of this countermeasure is to prevent excessive admin rights, and to limit the number of administrators whose access was approved by management.
Account owners holds the root access key and that has a security impact that we take under consideration:

- Changes to accounts are monitored and reviewed
- The number of accounts is minimal and constantly reviewed to detect orphan accounts
- The average time to disable account upon termination

We use VSM as our cloud management tool, which helps in managing access to accounts and delegate permissions, in a way that account owners able to manage all access.

- Account admin delegation is being monitored and alert whenever user grant with admin access.
- Any request for account admin delegation is being approved by our SaaS security officer.

Continuing Accounts, we create multiple AWS accounts for our organizations separate accounts, for example, production resources and backup resources. This separation allows us to cleanly separate different types of resources and provide excellent security benefits.

AWS Identity and Access Management (IAM) is a web service that helps us securely control access to AWS resources for our users.
We use IAM to control who can use our AWS resources (authentication), what resources they can use and in what ways (authorization).
We use IAM to create additional users and assign permissions to these users following the least privilege principle.

User Access Review Procedure

Micro Focus conduct periodic access reviews for access management **to** ensure that necessary personnel have access to essential systems and unauthorized employees (or miscreants) don't.
The process include**s** the following points:

- Manager Reviews of Employee Profiles
- Review Employee Termination Procedures
- Automate Reviews and Compliance
- Review Administrative Groups Members
- Review Profiles with Password Never Expire

Penetration and Vulnerability Testing

A penetration test (or pen test) is a set of procedures designed to bypass the security controls of a system in order to test that system's resistance to attacks. Our products categorized by a criticality level, SaaS products considered high criticality and every major release is being tested. Operational penetration test is performed annually as the infrastructure is rarely changed.
Vulnerability scans are conducted monthly against our internet facing assets and the findings being remediated according to our patch management program.
Our NOC team monitor the remediation process and that patching SLA's are met.
Emergency updates will be performed as soon as possible after ensuring patch stability. These updates should only be applied if they fix an existing problem that the server is experiencing.
Critical updates are applied during off hours within seven days' time frame after ensuring patch stability and an emergency CAB.
Non-critical updates on non-critical systems will be performed on regular scheduled maintenance windows within a two months period.

AWS Trusted Advisor

AWS Trusted Advisor is an application that draws upon best practices learned from AWS' aggregated operational history of serving hundreds of thousands of AWS customers. Trusted Advisor inspects our AWS environment and makes recommendations for saving money, improving system performance, or closing security gaps.
Trusted Advisor checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports or to a resource.
Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks and loss of data), the ports with highest risk are flagged red, and those with less risk are flagged yellow.
Ports flagged green are typically used by applications that require unrestricted access, such as HTTP and SMTP.
Trusted Advisor also checks for our use of AWS IAM, the root account and warns if MFA is not enabled.
For Amazon S3, Trusted Advisor checks buckets that have open access permissions, Bucket permissions that grant upload/delete access to everyone creates potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket.
This check examines explicit bucket permissions, but it does not examine associated bucket policies that might override the bucket permissions.

Trusted Advisor also checks the password policy for our account and warns when a password policy is not enabled or if password content requirements have not been enabled.

Data Encryption

SaaS security involves several different controls, including identity management (and federation), internal security settings, role management, incident response, service outage planning and auditing.
In this section we will focus on techniques for protecting sensitive data stored within our SaaS applications.
Micro Focus consist on the following stages:

- Define approved cryptography

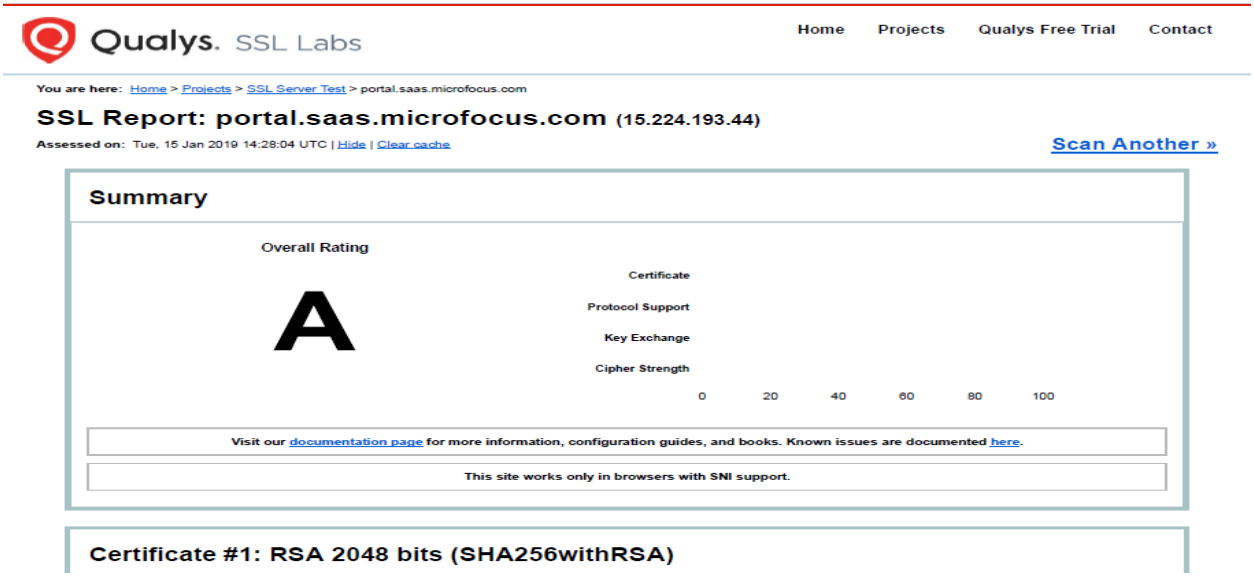
- Define encryption architecture and insecure protocols guidelines
- Data in transit encryption
- Data at rest encryption

Whenever the use of cryptography is required by subsequent sections of Micro Focus policy or by customer contract, only approved cryptography may be used. Some network protocols are inherently more insecure than others.
These include any services which do the following things:

- Pass Usernames and Passwords Over a Network Unencrypted — Many older protocols, such as Telnet and FTP, do not encrypt the authentication session and should be avoided.
- Pass Sensitive Data Over a Network Unencrypted — Many protocols pass data over the network unencrypted. These protocols include Telnet, FTP, HTTP, and SMTP. Many network file systems, such as NFS and SMB, also pass information over the network unencrypted.
- Remote memory dump services, like netdump, pass the contents of memory over the network unencrypted. Memory dumps can contain passwords or, even worse, database entries and other sensitive information.

Data in Transit Encryption

Micro Focus use TLS1.2 for data in transit encryption (browsers).



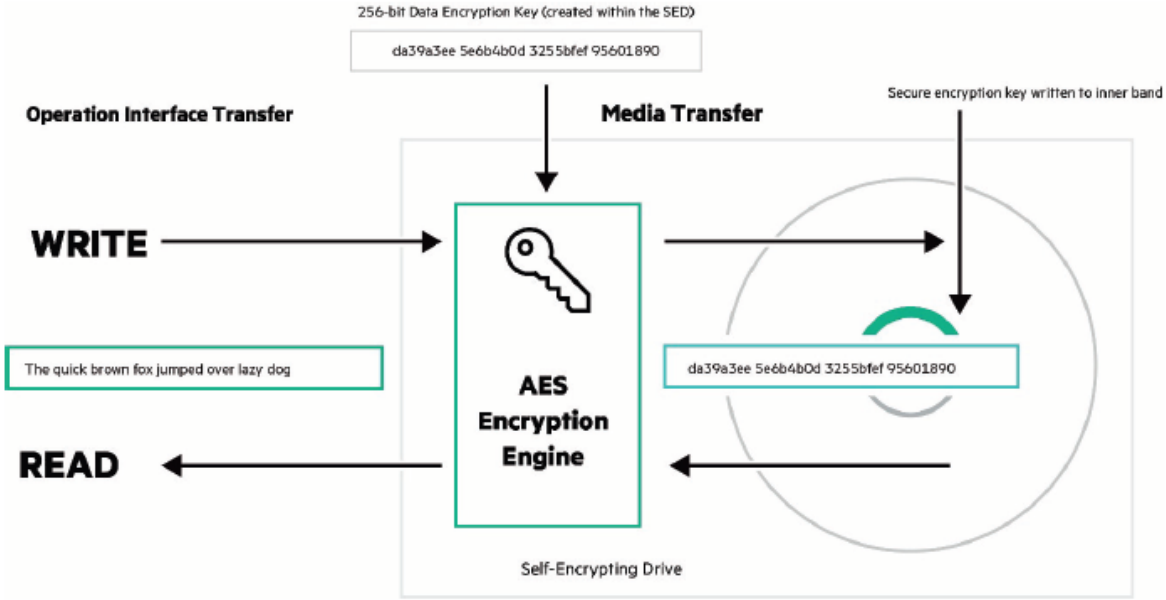
Data at Rest Encryption

Micro Focus uses HPE 3PAR devices for storage, all data written to each FIPS 140-2 disk uses Full Data Encryption.
All data encryption is handled at the drive level and no external software or hardware is needed to encrypt data.
The benefits from FDE are as follows:

- Government Standard based encryption—industry wide standard
- Uses AES-256
- Dedicated engine for full speed encryption contained on every drive
- Encryption key is unique and protected on the media
- Encryption key itself is encrypted and stored on the media

Self-Encrypting Disk (SED)

On SED drives, data is always encrypted on the storage medium, no license is necessary. Enabling encryption on the array protects the SED drives from any malicious intent by locking the disks to the array in which encryption is enabled. The same array encryption-locking key is used for all disks within the same encrypted storage array.
Government Standard based encryption—industry wide standard



Data at Rest Encryption (AWS)

AWS server-side encryption encrypts data on our behalf “after” the API call is received by the service, leveraging AWS KMS. We do not have to worry about managing and rotating the keys as AWS automatically manages them for us.
Amazon S3 or EBS supports server-side encryption (SSE) of user data.
Server-side encryption is transparent to us. Our database uses EBS storage so all database storage is encrypted in this way.
AWS generates a unique encryption key for each object, and then encrypts the object using AES-256.
The encryption key is then encrypted itself using AES-256-with a master key that is stored in a secure location.
The master key is rotated on a regular basis.

Logging and Monitoring

Logging and monitoring are key components in security and operational best practices as well as requirements for industry and regulatory compliance. Understanding the changes made to our resources is a critical component of IT governance and security. It is equally important to prevent changes and unauthorized access to the log data.
AWS CloudTrail is a web service that records AWS API calls made on our account and delivers log files to an Amazon S3 bucket that we specify, It records important information about each API call, including the name of the API, the identity of the caller, the time of the API call, the request parameters and the response elements returned by the AWS service.
This information helps us to track changes made to our AWS resources and to troubleshoot operational issues.
Near-real-time alerts to misconfigurations of logs detailing API calls or resource changes is critically important for effective IT governance and adherence to internal and external compliance requirements.
Even from an operational perspective, it is imperative that logging is configured properly to give us the ability to oversee the activities of our users and resources.
We are using our own product, ArcSight SIEM system for log management, these systems are being monitored by our Security Operation Center team.

Incident Management

Developing an incident-response strategy for our cloud-based environment is different from developing one for traditional, on-premise environments.
When using the AWS cloud, we have a wealth of information in the form of logs and metrics that can be very helpful when responding to a security incident.
If some of our virtual machines get compromised in the AWS cloud, we could simply modify the security group attached to that instance to isolate the problem.
We can take this one step further by creating a new subnet, once we have isolated the issue, we can further investigate to identify the threat source, vulnerabilities in our configuration, and potential risks.
Our incident response strategy includes the following phases: anticipate, deter, detect, respond, and recover.
Micro Focus has defined incident response and notification processes to meet contractual requirements and applicable regulations.
Once an incident has been detected and the CSM was notified, the SOC team provides an update to CSM every 12 hours, or as soon as new information is available, until the incident has been resolved.
A brief root cause analysis will be sent to the customer within five business days of resolution.
This program is being audit annually as part of the ISO27001 certification.

Protecting the Perimeter

Micro Focus offers its customers cloud access to its products as a service, this service is available both from our own datacenters and AWS cloud.
For our datacenters we are using network architecture which have a fail-safe topology, load balancing and segregation between production environment to the labs by a FW.
For AWS deployment we are using network architecture which consist on separate VPCs for management and other services.
We are using the following controls for perimeter defense:

- IPS to prevent attacks on the network
- Periodically vulnerabilities scan.
- FWs performing deep packet inspection, TCP session state and anti-spoofing
- Managed dedicated active directory with strict group policy

- Patch management process is in place to ensure all components are up to date
- In transit and at rest encryption for client data
- TLS version 1.2
- Malware detection agent is installed on all servers and workstations
- Backups for both data and configurations
- SOC team monitors incidents and keep track on service availability

The Intrusion prevention system is enabled on our SaaS perimeter to detect and block brute force and spoofing attacks.
System configurations consist on the followings:

- The effectiveness of this system is being tested annually based on attack history
- IPS is being updated constantly for new attacks signatures

Business Continuity & Disaster Recovery

Business Continuity (BC) ensures an organization's critical business functions continue to operate or recover quickly in case of an incident, it may also be referred to as High Availability (HA).
Because Micro Focus is a global organization and we have multiple datacenters around the globe, our BCP relay on data and configuration backup to a remote location.
Our operational teams follow a program that test and validate these backups.

Conclusions

This paper has covered in extensive detail Micro Focus's commitment to compliance as well as our technical approach to security.
For more information regarding Micro Focus cloud security contact the Customer Success Team and I will be happy to join to a meeting.
Sincerely,
Snir Karat
Product Operations Security Officer