White Paper

Security

Micro Focus Supply Chain Security

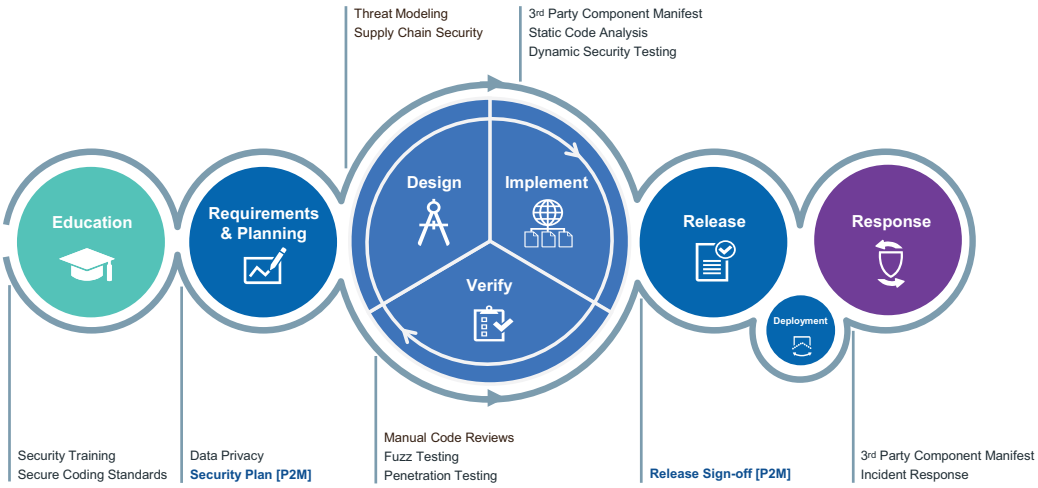
MICRO FOCUS

Micro Focus observes a "zero trust" philosophy in assessing and managing risk associated with the software systems we develop.

Overview

Micro Focus takes seriously our responsibility to provide solutions that satisfy the business requirements of our customers while also maintaining a level of security consistent with the deployment environment and information protection needs. Accordingly, Micro Focus observes a "zero trust" philosophy in assessing and managing risk associated with the software systems we develop. Beginning with "secure by design," our priority is to practice the best possible security hygiene through all phases of our software supply chain.

In this document, we outline our approach to supply chain risk management and the dual goals of maintaining resilience against cyberthreats and ensuring confidence in the security, integrity, and reliability of our software. Security and trust are achieved by adopting industry best practices and applying them to our products and business processes. This approach is reflected in our Secure Development Lifecycle (SDL) framework. The SDL is a governance element that supports secure, end to end product development and shipment, with support from fundamental control structures, such as Product to Market (P2M).



The Micro Focus SDL includes 13 security practices with a multi-level maturity structure similar to the Capability Maturity Model Integration (CMMI), the OWASP Software Assurance Maturity Model (SAMM), and the Building Security In Maturity Model (BSIMM). The P2M is our gating mechanism; at each gate, security sign-off is required before a product can advance through the development cycle and ultimately be released to manufacturing (on-premises products) or production (SaaS).

These process-focused controls are augmented by a corporate policy designed to ensure that the infrastructure (the environments in which our software is designed, built, tested, and deployed) minimizes supply chain risk exposure. Our adoption of industry best practices—upon which Micro Focus policies,

standards, processes, and guidelines are built—is also influenced by publications such as NIST SP 800-53, NIST 800-171, NIST Cybersecurity Framework (CSF), the Defense Federal Acquisition Regulation Supplement (DFARS), and others. Additionally, several Micro Focus product groups and solutions meet ISO standards 15408, 27001, and 27034.

See **www.microfocus.com/en-us/about/product-security** for details about the ISO standards for which we have achieved certification.

What follows is not an explicit enumeration of SDL security practices, P2M requirements, and risk management controls for our supply chain. Instead, it is a comprehensive overview of our zero-trust approach to managing our software supply chain.

Our Software Factory approach simplifies and optimizes the DevOps toolchain, which includes leveraging Micro Focus solutions. In doing so, we can more effectively reduce and manage supply chain risk while improving product quality and security.

Suppliers

Micro Focus conducts vendor risk assessments to understand the strengths and weaknesses of our suppliers. Contracts with vendors for third-party components or outsourced development require adherence to Micro Focus corporate standards for ethics and security design.

Our maturity model for third-party-supplied code expects security to be at the same or higher level than internally-developed code.

We further manage risk in this area by reducing the number of suppliers to the minimum necessary level. Our Software Factory approach simplifies and optimizes the DevOps toolchain, which includes leveraging Micro Focus solutions. In doing so, we can more effectively reduce and manage supply chain risk while improving product quality and security. See **www.microfocus.com/en-us/digital-transformation/our-perspective/software-factory** for more information about our Software Factory journey.

Third-Party Components

The need for third-party components is determined by engineering and product management. Vetted and approved components are downloaded over a secure channel from a trusted source. They are security tested and then stored in a secure, access-controlled repository for subsequent reuse in building Micro Focus software.

An internally-developed component and license management system manages license obligations and monitors the National Vulnerability Database for published CVEs that could impact in-use components. Third-party components are subject to software composition analysis as outlined in the Micro Focus SDL.

Build environments are hardened using corporate IT standards and include regular patching and antivirus. Only approved tools are available for use in the build toolchain.

Artifact Repository

Binary components are stored in an access-controlled repository and backed up in compliance with BC/DR policy. Authorized individuals authenticate using their unique corporate identity. Shared accounts are prohibited, and access is traceable to an individual's corporate identity and logged for audit purposes. Artifact repository environments are subject to corporate IT policy governing the use of endpoint security.

Source Repository

Source code is stored in an access-controlled repository and backed up in compliance with BC/DR policy. Authorized individuals authenticate using their unique corporate identity. Shared accounts are not allowed, and source access is limited to a "need-to-know" basis, with non-team member access authorized on a case-by-case basis. Access is traceable to an individual's corporate identity and logged for audit purposes.

Source repository environments are subject to corporate IT policy governing the use of endpoint security. Source code is scanned for malware as part of the check-in process.

Development Environment

Development environments (laptop, desktop, labs) are network-segmented and subject to corporate IT policy governing endpoint security. Asset management controls preclude the joining of any device to the network without end user authentication or device pre-registration.

Build Environment

Build environments are hardened using corporate IT standards and include regular patching and antivirus. Only approved tools are available for use in the build toolchain. Source and third-party components are pulled into the build environment from authorized source and artifact repositories.

Built solutions are pushed over secure channels to our code-signing service, which completes an additional malware scan before code-signing.

Access to build environments is restricted to the individuals responsible for configuring, troubleshooting, and maintaining the integrity of the build process.

Access to build environments is traceable to an individual's corporate identity and logged for audit purposes.

Testing and Staging Environments

Access to Micro Focus testing, staging, and production environments is restricted and traceable.

Testing and staging environments are restricted to the individuals charged with configuring, troubleshooting, and maintaining the environment for which they have responsibility. Access to these environments is traceable to an individual's corporate identity and logged for audit purposes.

Software Integrity and Availability

Product installers are signed using an approved signing process.

Product installers and associated components for on-premises solutions, and released for general availability, are hosted in a secure environment. Downloading occurs over a secure channel, and file hashes are available to assist in detecting file tampering.

Production Environment

SaaS and other IT production environments are maintained and controlled to ensure maximum system availability and security to meet or exceed Service Level Agreement obligations. No changes to any production system are authorized unless reviewed and approved by the Micro Focus Enterprise Change Advisory Board (CAB). The Micro Focus approach to managing risk in these environments is guided by these four principles:

- **Accountability:** Security and operation events should be traceable to their source. This may be applied at a number of different levels, such as the network source of a connection or the named account of support personnel.
- **Auditability:** Activities undertaken within the environment should be recorded and stored in secure locations to ensure that events are available for audits or incident investigation.
- **Least Privilege:** Access given to an operator within Micro Focus production environments, whether software or human, shall be limited to the permissions necessary for them to fulfill their role.
- **Segregation of Duty:** No one individual should be in place to complete key processes related to the security and protection of customer information.

Security Operations Center staff monitor production environments for performance degradation and suspected security events. Technical solutions include Micro Focus ArcSight SIEM.

On an as-needed basis, Micro Focus provides customers with evidence of System and Organization Controls (SOC) 2 compliance ("SOC2 Report").

The Micro Focus Network Security Management Standard establishes the minimum standards that contribute to the integrity and security of our supply chain. All network-connected assets are subject to vulnerability scanning, penetration testing, and patching on a scheduled or event-driven basis.

Infrastructure

Secure, available network resources are a cornerstone of geographically separated organizations and are a major component of the Micro Focus software supply chain.

The Micro Focus Network Security Management Standard establishes the minimum standards that contribute to the integrity and security of our supply chain. This standard includes requirements for network segmentation, security and access controls, and audits.

Asset Inventory and Management is governed by corporate IT policy. All network-connected assets are subject to vulnerability scanning, penetration testing, and patching on a scheduled or event-driven basis.

Infrastructure vulnerability scanning is conducted regularly, following corporate policy and under Micro Focus Cyber Security supervision. Vulnerability remediation is subject to a rigid schedule according to risk severity.

Data Privacy

At the Micro Focus Privacy Executive Committee's direction, we have developed a privacy framework to ensure compliance with applicable privacy regulations and laws. The basis for the privacy framework is a set of technical requirements translated from the articles of the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The requirements are applied to any Micro Focus software solution whose end users have legal rights associated with their data.

Micro Focus is also self-assessed at Level 1 of the Cybersecurity Maturity Model Certification (CMMC), and plans are being developed to achieve CMMC Levels 2 and 3 in support of our DOD customers.

See **www.microfocus.com/about/legal/#your_privacy** for access to the Micro Focus Privacy Policy.

Summary

A clean supply chain is critical to developing reliable software solutions that meet or exceed customer and market expectations for security, integrity, and reliability. Our comprehensive, multi-layered approach enables us to respond quickly to customer requirements while still controlling risks associated with today's cyberthreats.

Micro Focus is committed to formal supply chain security based on best practices. We have mature processes in place to manage code development and delivery. Our practices for inbound supply chain security, development process security, and release security provide assurance that we are managing security risk with appropriate diligence and focus.

We look forward to working with you on delivering secure, world-class products for your business.

Contact us at:
www.microfocus.com

Like what you read? Share it.