Quest® Supply Chain Risk Management

Strategy mitigates risk.

Quest® and One Identity know the value of providing secure and trustworthy products to the marketplace. Our extensive history of designing products that help customers mitigate and prevent insider threats in complex network environments was born out of an engineering focus on quality and security. Through our strategies, standards and practices, we implement a secure software development lifecycle and a comprehensive information security management framework that combine to provide secure products across a wide spectrum of diverse product offerings.

EXECUTIVE SUMMARY

Quest and One Identity are well known for delivering robust solutions to the marketplace. The delivery mechanism is aided by a mature supply chain security infrastructure. To manage the potential of product compromise, we leverage proactive security measures designed to identify and eliminate the likelihood of supply chain risks.

Our strategy is based on the following fundamental principles:

- Secure product delivery requires an intense focus on confidentiality, integrity and availability of data.
- Unintentional vulnerabilities that provide opportunities for exploitation must be eliminated in the design process.
- All supply chain components must be tested and proven genuine, and to not contain any unwanted functionality.

Supply chain security at Quest and One Identity focuses on minimizing risks to customers by taking preventative steps to reduce the likelihood that our products contain vulnerabilities, hidden malicious code or backdoors inserted by threat actors. We know that as your supplier, we are a key part of your supply chain. And we know that both our teams and our design processes are key to eliminating risk in that supply chain.

We strive to ensure that all of our employees and contractors act with integrity in developing our products. We recognize that our ability to manage both our teams and our processes promises the most effective security outcomes for our products and for your business.

As your supplier, we are a key part of your supply chain. And we know that both our teams and our design processes are key to eliminating risk in that supply chain.

SECURITY ENVIRONMENT PHILOSOPHY

The Quest supply chain security model is based on the premise that risks exist at all points in the supply chain. These risks are most evident where third-party suppliers have access (direct or indirect) to software code. To combat this spectrum of risks, we employ continuous security assessments throughout the development process. Wherever third-party suppliers need access to our developing products, we limit the number of vendors and the access those vendors are allowed.

All new suppliers go through an extensive vendor trustworthiness assessment. Security requirements are baked into our process early on, starting with the inclusion of security provisions in supplier contracts.

We have established baseline standards for data protection, privacy and security within our supply chain. All suppliers must meet those standards to qualify to do business with us.

DEVELOPMENT PROCESS AND ENVIRONMENT

At Quest and One Identity, we understand that the development process must focus on building products in trustworthy locations. Then, we develop solutions to an exacting standard with a practice that includes the following:

- The build environment is protected by security controls designed to prevent unauthorized access.
- Source code, regardless of origin, is inspected for evidence of misconfiguration and unauthorized modifications.
- Our software architecture guarantees a deterministic software build, preventing interference with the accepted and reviewed source code.

Figure 1 illustrates a standard Quest development process.

THREAT MITIGATION

Quest and One Identity have implemented controls to mitigate risks in the product development lifecycle. We manage our product development portfolio by performing a pulse check on each process with the assistance of the following assessments:

- Supplier capabilities assessments ensure suppliers have processes in place that promote good security development and management practices.
- Product security assessments identify susceptibility to critical security compromise and mitigation requirements.
- Product logistics programs control access to the product in each step in the supply chain.

INSIDER THREAT PREVENTION

Quest and One Identity have strictly limited access to sensitive areas of the

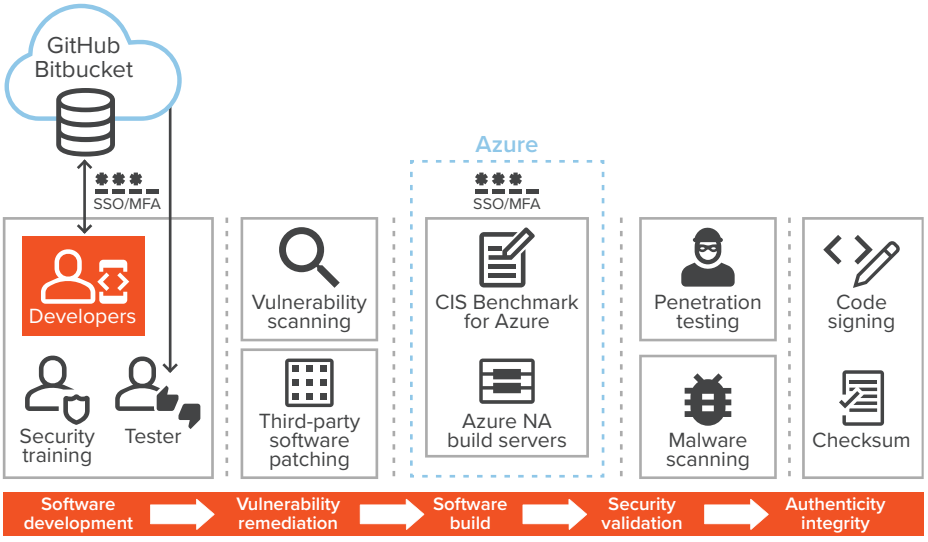

Figure 1. A standard Quest development process.

Quest

Security control	Description
Security training	Assigned security training is required for developers, managers and directors
Secure development lifecycle	A best-practice secure development lifecycle is followed
Third-party software	Bundled third-party software is checked for vulnerabilities via a standard process before application release
Vulnerability scanning	All software is scanned for vulnerabilities by utilizing an industry-standard SAST/DAST product
Penetration testing (Third party)	Products undergo third-party penetration testing annually
Malware scanning	All products are scanned for malware before release with independent, industry-standard, anti-malware scanners
Code signing	Software distributed to customers is cryptographically signed using Quest's official signing key that validates authenticity
Software integrity	Checksums for software installers are published for customers to ensure the integrity of distributed software

Figure 2. Quest security controls.

business (e.g., product development) to authorized personnel only, and then we only authorize the minimum level of access required for the performance of their validated assigned roles and duties. This restricted access is then strictly monitored, and sharing of access codes or passwords is absolutely forbidden. In this way, we substantially reduce the risk of infiltration by a potential rogue insider.

These controls are replicated throughout all supply chain elements, with limitations on people and organizations designed to protect the integrity of organizational processes, communications channels and systems covering the comprehensive supply chain. Then, in addition to all of this, we also apply further controls:

- Risk assessments identify weak spots and restrict information to only trusted individuals and technologies.
- Off-boarding procedures quickly terminate exiting employees and suppliers from the access list.
- Background checks are required to inspect the history of individuals and the reputations of supplier organizations.

CONCLUSION

The mitigation of risk within the supply chain is a priority for Quest and One Identity. The level of security we apply to create and protect our solutions has become a differentiating factor for many customers.

As a team, we understand that supply chain risks can be introduced at any point in the supply chain and may be inherited by each subsequent acquirer. Therefore, we have designed a supply chain risk management strategy that begins as early as possible in the product development lifecycle.

Quest and One Identity fully integrate supply chain security into the secure development lifecycle. We strive to meet the needs of our discerning customer base. The goal is to provide assurance at the level required to guarantee our products operate as intended — free from vulnerabilities, delivered with the expected quality and delivered uncompromised.

FOR MORE INFORMATION

We have additional product line supply chain security information with details on specific products. For more information, please contact your Quest or One Identity account manager.

Information about Quest and One Identity products can be found at quest.com/solutions/.

Our contact details are available at quest.com/company/contact-us.aspx.

Our goal is to deliver products that operate as intended — free from vulnerabilities, delivered with the expected quality and delivered uncompromised.

ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.