

Quest Supply Chain Risk Management

Air Gap Architecture for Microsoft Platform Management



The Microsoft Platform Management line of products earns a high level of trust from its customers as it performs critical administrative, auditing and security tasks directly within the customer’s environment. Therefore, in addition to our general efforts around Supply Chain management, Quest goes beyond the ordinary to also address the concern of insider threats head on.

This white paper describes the Air Gap architecture as it is used for the Microsoft Platform Management line of products.¹

PROTECTION AGAINST INSIDER THREAT ACTORS

The Quest® Platform Management product line applies an architectural Supply Chain Security approach to product development, assembly and validation that eliminates most insider and outsider threats by design and further fortifies the existing Quest Supply Chain Security controls against the remaining potential attack vectors.

PHYSICALLY SEGREGATED AND PHYSICALLY SECURED ASSEMBLY ENVIRONMENT

The Air Gap environment is physically separated from the Quest network, located in a secure facility within Quest, and has dedicated additional physical access controls for the few team members who are allowed to work in the environment.

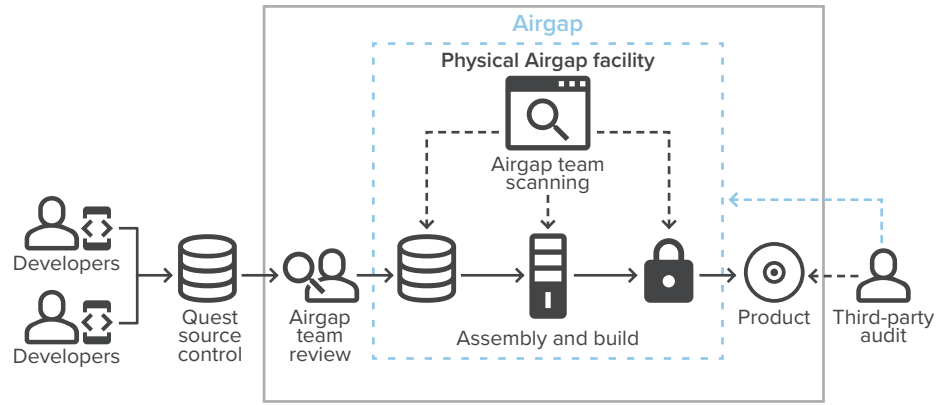
For the purpose of Supply Chain and Assembly Security, Quest adds an additional, much stricter, network security standard on top of its general corporate controls and standards. The physical separation makes it impossible to penetrate with means short of physical force.

DEDICATED TEAM

The Air Gap team is structured to reduce insider risk. It does so by:

- Ensuring that reporting chain and accountability are independent from product development teams

¹ Please contact your sales representative for details about applicable products



Physical separation with an air gap.

The physical separation makes it impossible to penetrate with means short of physical force.

- Requiring background checks and validation of citizenship
- Reducing risk surface by small team scope
- Preventing any remote access to Air Gap Environment

SEPARATION OF DUTIES

Product Development and Product Build and Assembly duties are entirely separate. The Air Gap team performs, at a minimum, the following separated duties in an independent fashion:

- **Source code level review** and inspection is performed independently by the Air Gap team with a mix of manual and automated reviews. This enables detection on the transparent source code level of any malicious and security critical contribution.
- **Independent audit of security SLDC procedures** ensures that there is an additional control instance to guarantee all Quest security SLDC procedures have been followed by the development teams.
- **End-to-end chain of custody** and signature validation ensures fidelity of all incorporated third-party supplier components and also ensures a correct and complete inventory that is maintained and detected independently within the Air Gap Secure Build facility.
- **Secure code signing** with a dedicated, physical Quest signing certificate ensures that only the Air Gap team

has the ability to sign the complete product. Checksums are produced where applicable. This enables customers to validate authenticity after product delivery and prevents any insiders or outsiders from tampering with the completed product in the final delivery phase.

This internal separation of duties addressed many of the recent cybersecurity concerns and incidents that can be observed in the news media and various government publications.

ATTRIBUTABILITY AND FORENSICS

A physically separated environment and separation of duties result in complete attributability of contributions to and modifications of the final products. This serves as a preventive measure, a deterrent and a forensic capability, significantly increasing the stakes for a malicious actor to be caught during or after the action.

THREAT MITIGATION CONTROLS

The Quest Platform Management line of products applies all of Quest’s standard threat mitigation controls.

Outsider and Insider attempts to tamper with or bypass these controls are mitigated by deployment in the Air Gap environment which utilizes physical separation and separation of duties as outlined above.

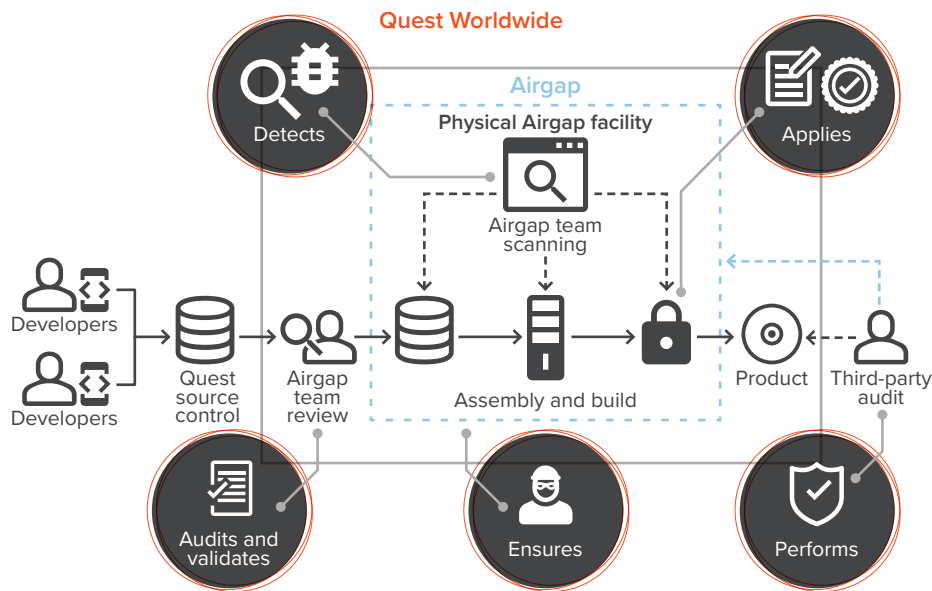
Security control	Description
Security training	2.5 hours of assigned Security Training required for developers, managers, and directors
Secure development lifecycle	Follows and internally audits a best practice secure development lifecycle
Third-party software	Bundled 3rd party software is checked for vulnerabilities via standard process before application release
Vulnerability scanning	All software is scanned for vulnerabilities by utilizing an industry standard SAST/DAST product
Penetration testing	Products undergo third party penetration testing annually
Malware scanning	All products are scanned for malware before release with two independent industry standard anti-malware scanners
Code signing	Software distributed to customers is cryptographically signed using Quest's official signing key which validates authenticity
Software integrity	Checksums for software installers are published for customers to ensure integrity of distributed software
Insider threat mitigation	Air gapped architecture severely constraints and deters insider threats
Integrated internal audit	Air gapped architecture ensures a continuous internal audit of all practices via separation of duty and physical separation of environments
Physical separation	An air gapped secure assembly facility limits access to physical actors
Validating chain of custody	Ensures fidelity of supplied components

CONCLUSION

The Quest Platform Management product line employs a wide set of threat mitigation controls and in addition prevents

malicious circumvention of these controls by malicious outside and inside actors, hereby reacting to the developing threats faced by the supply chain in today's complex security landscape.

All state of the art security controls are used with complete separation of duties.



Security controls with complete separation of duties..

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.

© 2023 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners.

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.