

Secure Product Development Lifecycle



Approach

- The Fortinet Secure Development Lifecycle covers every stage of the product lifecycle, from design through end of life
- Security is baked into the product from inception
- Fortinet has strong product scrutiny at all stages of the product development lifecycle, internal and external
- When issues inevitably occur, Fortinet remediates rapidly with a transparent incident response plan
- Fortinet operates in partnership with our customers and regional CERT teams, sharing information and feedback
- Fortinet works with industry to develop and implement stronger standards for the benefit of all our customers

Protecting customers with supply chain security at all stages of the product lifecycle

Our Commitment

Fortinet recognizes that supply chain security is an increasingly important dimension of cybersecurity and enterprise risk management. Fortinet is committed to implementing a comprehensive approach to protecting the security and integrity of its products throughout the product design, development, manufacturing, delivery, and support processes.

Supply Chain Breadth

Fortinet focuses on risk management and security of Fortinet products and services from the inception of an idea through to its commercial realization and use, including:

- Product design and development
- Component and material sourcing
- Manufacturing and assembly
- Product delivery
- Technical services and support

Highlights

Fortinet Supply Chain Process



Fortinet manages a coordinated program across our engineering, manufacturing, technical services teams, together with our suppliers and channel partners, to ensure the security of our supply chain.



- Fortinet develops its own Network Processors (NP), Content Processors (CP), and System-on-Chip (SoC) Application Specific Integrated Circuits (ASICs) technology in house

- R&D conducted primarily in the US and Canada



- Fortinet operates a Trusted Supplier Program with a rigorous selection and qualification of manufacturing partners, adhering to NIST 800-161

- Implement technical measures to prevent malware and rogue components that could compromise functionality

- Technical support provided from dedicated Fortinet regional centers

- Application of secure development best practices (including NIST 800-53, NIST 800-160, NIST 800-218, US EO 14028, UK TSB)



- Regular patch release cycles and a notification service to support and encourage customers to apply security patches



The Fortinet Supply Chain Risk Management program covers security risk management for the entire breadth of the supply chain and implements five key steps for managing supply chain risks:



Identify: Identify potential risks to the supply chain

Protect: Build controls to help protect the supply chain from risks

Detect: Detect issues early, giving more time and options to respond

Respond: Respond as quickly as possible to mitigate the vulnerability or threat

Recover: Recover with minimal impact to customers

Transparency

Fortinet understands that customers have a heightened awareness regarding security when selecting suppliers and have a choice in who they trust to deploy on their networks. Fortinet operates a transparency program to provide all of the information customers need to make a security-driven decision including:

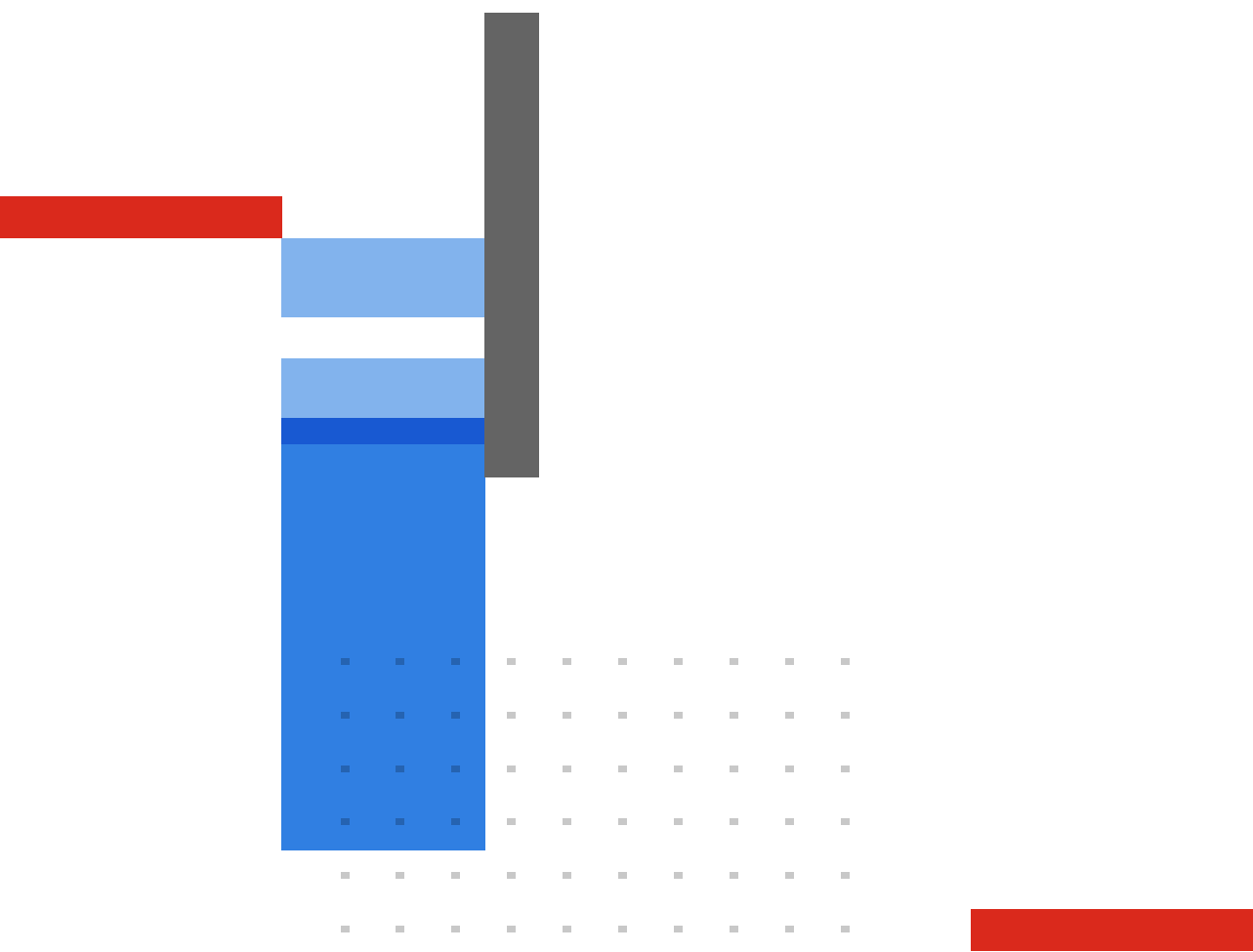
- Publicly available [PSIRT Policy](#) and [Advisories](#) including all internally discovered issues
- Broad range of independent certifications including FIPS 140-2, CC EAL4+ and NDcPP, SOC2
- Adherence to US [Presidential Executive Order on Improving the Nation's Cybersecurity](#) with production of Software Bill of Materials

For more information on third party product certifications see [here](#).

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.