Fortinet Secure Product Development Lifecycle

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.

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:

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify potential risks to the supply chain</td>
<td>Build controls to help protect the supply chain from risks</td>
<td>Detect issues early, giving more time and options to respond</td>
<td>Respond as quickly as possible to mitigate the vulnerability or threat</td>
<td>Recover with minimal impact to customers</td>
</tr>
</tbody>
</table>

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.