Fortinet’s Commitment to Product Security and Integrity

The Fortinet Approach

Secure product design lifecycle covers every stage, from design through end of life.

Security is baked into the product from first conception.

Strong product scrutiny at all stages of the product development lifecycle, internal and external.

Rapid remediation with a transparent incident response plan.

Operating as a partnership with our customers, transparently sharing information and feedback.

Collaborating with the industry to develop and implement stronger standards for the benefit of all our customers.

Our Commitment

Our top priority is to protect customers with robust security at all stages of the product lifecycle and continuously improve our policies and processes with the security of our customers in mind

As a leading cybersecurity vendor, Fortinet’s mission is to secure people, devices, and data everywhere. More than 730,000 customers trust Fortinet solutions, which are among the most deployed, most patented, and most validated in the industry. Fortinet secures some of the world’s most critical national infrastructure and recognizes the importance of robust supply chain security for our customers. We remain committed to implementing a comprehensive approach to protecting the security and integrity of our products throughout the product design, development, manufacturing, delivery, and support processes.

Fortinet Secure Product Development Lifecycle Policy (SPDLC)

Our Secure Product Development Lifecycle Policy, which is based secure-by-design and secure-by-default principles, helps ensure that security is designed into each product from inception, covering every stage of the product lifecycle all the way through to end of life. These efforts include:

- Developing our own network and content processors, and system-on-a-chip (SOC) application-specific integrated circuits (ASICs) in-house.
- Conducting R&D primarily in the U.S. and Canada.
- Operating a Trusted Supplier Program with rigorous selection and qualification of manufacturing partners, adhering to NIST SP 800-161.
- Aligning with secure development best practices (including NIST SP 800-53, 800-161, and 800-218, EO 14028, and UK Telecom Security Act).
- Implementing technical measures to prevent malware and/or rogue components that could compromise functionality.
- Employing threat modeling helps ensure security is baked into products from the start and using defense-in-depth to help mitigate risks.
- Employing robust security testing of our products, including leveraging tools and techniques such as static application security testing (SAST) and software composition analysis built into our build processes, dynamic application security testing (DAST), vulnerability scanning, and fuzzing prior to each release, as well as penetration testing and manual code audits by our dedicated security engineers.
- Performing independent third-party penetration testing at regular intervals.
- Validating our products through third-party product quality standards, including NIST FIPS 140-2 and NIAP Common Criteria NDcPP / EAL4+.

Fortinet’s Vulnerability Disclosure Policy

Fortinet’s product development processes introduce robust product security scrutiny at all stages of the product development lifecycle, internal and external. The Fortinet Product Security Incident Response Team (PSIRT) is responsible for maintaining security standards for Fortinet products and operates one of the industry’s most robust PSIRT programs. Fortinet’s culture of proactive, transparent, and responsible vulnerability disclosure follows best practices endorsed by government entities, such as CISA in the United States. It is one of the many ways we demonstrate our commitment to protecting our customers.

~80%

of Fortinet vulnerabilities discovered in 2023 were identified internally through our rigorous auditing process.

Our customers can feel assured knowing that ~80% of Fortinet vulnerabilities discovered in 2023 were identified internally through our rigorous auditing process. This proactive approach enables fixes to be developed and implemented before malicious exploitation can occur.

Fortinet works with Fortinet customers, independent security researchers, consultants, industry organizations, and other vendors to accomplish our PSIRT mission. Findings obtained through these exercises are responded to appropriately, and all remediated issues, whether internally or externally discovered, are transparently and responsibly published for our customers, including through a Monthly Vulnerability Advisory published on the second Tuesday of each month.

By disclosing vulnerabilities proactively and transparently, we provide customers with the information they need to protect their assets effectively. Safeguarding our customers is our top priority, and Fortinet empowers our customers to make informed, risk-based decisions about their security.

Responsible, Radical Transparency

Fortinet understands that customers have a heightened awareness of security when selecting suppliers and have a choice in who and what they trust to deploy on their networks. Fortinet operates a responsible and transparent PSIRT program to provide the information customers need to make risk-based decisions, including:

- Publicly available PSIRT Policy and Advisories, including all internally discovered issues
- A broad range of independent certifications, including FIPS 140-2/3, CC EAL4+, CC NDcPP, and SOC2
- Adherence to the Presidential Executive Order on Improving the Nation’s Cybersecurity, including producing a Software Bill of Materials (SBOM)

For information on third-party product certifications, see Fortinet Security and Trust.

Mitigating Controls

Fortinet recognizes that upgrading immediately is not always an option and, whenever possible, provides compensating controls for our customers, which may include:

Virtual Patching
Automatic virtual patching of device external-facing interfaces controlled by Fortinet to allow immediate risk mitigation while offering a controlled upgrade process

Automatic Upgrade
Upgrade by default policy setting for low-end systems to ensure upgrade to the latest patch release

Workarounds
Configurational changes to mitigate against potential risks

Hardware and File System Integrity Checking
Hardware chain of trust in the BIOS and FortiSP5 ASIC for secure boot functionality