STROZ FRIEDBERG
A LevelBlue Company

SERVICE BRIEF

Product Security Testing

Cyber Solutions

Enhance Your Security Posture with Comprehensive Product Security Assessments

As technology advances, security threats also increase across hardware, firmware, applications, cloud, and network services. A fragmented approach to product security can create vulnerabilities that attackers may exploit. Stroz Friedberg's Full Stack Product Security Testing offers comprehensive security assessments to identify risks throughout the entire product stack—from silicon to software, and all the way to the networks these devices connect to inhabit.

Our security testing approach is designed to help organizations secure their entire product ecosystem, leveraging proven methodologies and deep technical experience. Our assessment offerings include:

Hardware Security Assessments

- Schematic and PCB analysis to identify potential security flaws
- Debug port identification and exploitation risk analysis
- Side-channel and fault injection attack testing
- Secure element and cryptographic implementation validation

Firmware Security Reviews

- Firmware extraction and reverse engineering
- Static and dynamic analysis for vulnerabilities
- Bootloader and chain of trust validation
- Secure update mechanism and rollback protection review

Application and API Security Assessments

- Static code review and dynamic security testing of applications and APIs
- Comprehensive static/dynamic review of authentication and authorization logic
- Verifying internal or service-to-service endpoints are not exposed unintentionally
- Injection testing with a priority on low privileged or unauthenticated user perspectives

Network Security Assessments

- Evaluation of network architecture and segmentation
- Endpoint security testing for workstations and internal services
- Detection of misconfigured access controls and privilege escalation risks
- Internal penetration testing to identify lateral movement pathways

Cloud Security Assessments

- Review of cloud environments in AWS, GCP, and Azure
- Identify exposed cloud storage, misconfigured, or overly permissive IAM roles
- Analyze network security groups and firewall rules to validate segmentation
- Perform dynamic testing to explore paths that are hidden from a pure configuration review

Stroz Friedberg's Product Security Testing Approach

We offer multiple tiers of security testing, from basic security validation to comprehensive penetration testing. Our flexible engagement models enable organizations to customize assessments to meet their specific product security needs. Our Full Stack Product Security Testing follows a structured process to deliver actionable insights and help secure product architectures efficiently:

01 Engagement Kickoff – Understanding the Product and Defining Scope

Stroz Friedberg meets with the client to define the security testing scope, identify key attack surfaces, and align objectives with product risks.

By defining these risks early, Stroz Friedberg can help ensure testing methodology is focused, efficient, and tailored to real-world threats.

Example: The product is a medical device that wirelessly transmits real-time patient data, making firmware security, communication protocols, and physical attack points key concerns. Stroz Friedberg collaborates with the client's engineering team to understand how an attacker might attempt to bypass authentication, manipulate firmware, or intercept wireless signals

02 Threat Modeling – Identifying Attack Vectors Based on Product Architecture

Stroz Friedberg performs a condensed threat modeling exercise to help identify security gaps based on the product's architecture and intended use functionality.

This structured approach helps ensure testing focuses on the most exploitable and high-impact security risks, reducing the chance of real-world breaches. It provides input to guide testing priorities and simulate attacker behavior.

Example: The product uses Wi-Fi, Zigbee, and Bluetooth, which creates multiple attack opportunities, such as wireless spoofing, device impersonation, and API hijacking. Stroz Friedberg collaborates with the client's development team to outline realistic attack scenarios, like exploiting weak authentication methods to remotely control connected devices.

03 Security Testing and Exploitation – Uncovering Real-World Vulnerabilities

Stroz Friedberg performs hands-on security testing across hardware, firmware, network, and applications, identifying real-world vulnerabilities that attackers could exploit.

By providing proof-of-concept attacks, Stroz Friedberg helps ensure the client understands the severity of each issue and the immediate need for remediation.

Example: The product undergoes testing, revealing a UART debug interface that grants unauthorized root access. Further firmware analysis uncovers hardcoded API keys and weak encryption protecting the backend cloud interface. Stroz Friedberg demonstrates how these vulnerabilities could be exploited to steal customer data, manipulate transactions, or install malicious firmware.

04 Reporting, Risk Prioritization, and Validation – Fixing and Securing the Product

Stroz Friedberg provides a comprehensive report, prioritizing security findings according to their exploitability and potential impact on the product.

Stroz Friedberg then provides detailed and actionable strategic recommendations, along with proof-of-concept exploits to help with remediation. Once security improvements are in place, the client can implement the remediations and proceed without these critical security flaws, further strengthening the tested product.

Example: An IoT sensor network is found to be vulnerable to unauthorized firmware installation, which allows attackers to manipulate sensor readings or disrupt operations. Stroz Friedberg provides detailed strategic and actionable recommendations to implement firmware signing, disable debug interfaces, and strengthen encryption.

STROZ FRIEDBERG
A LevelBlue Company

About Stroz Friedberg

Stroz Friedberg, a LevelBlue company, delivers intelligence-driven digital risk management with expert-led services designed for adaptive resilience.

With over 25 years of leading the resolution of the most complex, high-stakes digital risk issues, we manage the entire digital risk lifecycle – from cyber threats and insider risks to IP theft and regulatory compliance. Our approach combines managed security services with expert analysis and strategy, supported by threat intelligence gathered from thousands of engagements across various industries.

We translate complex technical and legal risks into actionable strategies, helping CISOs and legal teams turn digital risks into board-ready insights. Our comprehensive services include managed cyber defense, digital forensics and incident response, trade secret protection, expert witness support, threat intelligence, security strategy and governance, attack path mapping and testing, and resilience engineering.

Operating as one trusted partner, we align technical precision with business priorities to protect critical assets, adapt to evolving threats, and maximize ROI through proven outcomes. Through LevelBlue's portfolio, these specialized services integrate seamlessly with 24/7 managed security operations and AI-driven threat detection for comprehensive digital risk protection.

Cybersecurity. Simplified.

levelblue.com/strozfriedberg