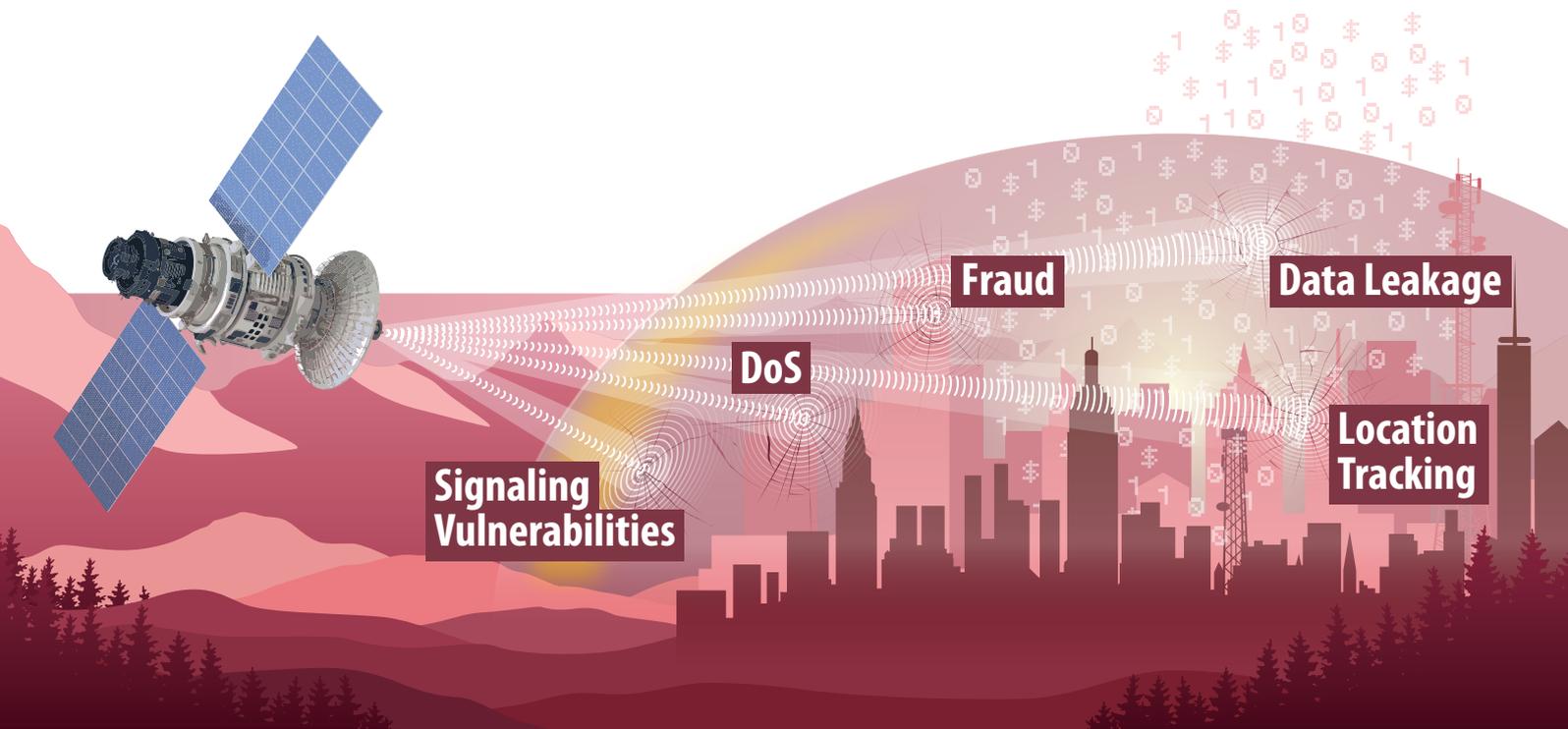


## PT TELECOM SECURITY ASSESSMENT™

### PROACTIVE SECURITY ASSESSMENT OF TELECOM CORE NETWORK



#### RESULTS AND DELIVERABLES

- + Full list of critical signaling vulnerabilities and validated attack scenarios
- + In-depth report with immediate and accurate assessment results
- + Expert guidance on remediation from acclaimed security pros
- + Ability to establish regular security checks and change management control
- + Monitoring of signaling security with [PT Telecom Attack Discovery](#) free trial



Associate  
Member

Used even more widely than the Internet, signaling networks link individuals, businesses, and smart IoT devices into a solid mobile ecosystem. This ecosystem depends on telecom operators to maintain reliable and protected communication.

However, fundamental flaws in signaling protocols—SS7, Diameter, and GTP—and configuration errors in network equipment leave the door open to severe security threats: privacy violation, subscriber location tracking, fraud, operation disruption, and more. In addition, the convergence of traditional and new technologies brings new vulnerabilities and attack vectors.

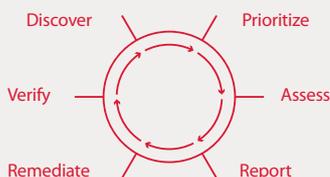
Many carriers might prefer a one-size-fits-all solution to protect their networks, but the reality is that existing infrastructure and protocols cannot be fixed overnight. The most practical approach is to start with a detailed security assessment, followed by continuous signaling monitoring for attacks. With the risk of failure clear, telecom operators should rely on a security partner with recognized real-world experience in signaling security.

Leading mobile operators around the globe trust telecom security assessment from Positive Technologies to enhance visibility of telecom infrastructure, manage security risks, and gain total control of their core network.

#### STOP BEING AN EASY TARGET, PREVENT ATTACKS BEFORE THEY START

PT Telecom Security Assessment is a flagship service that provides unbiased evaluation of the current signaling network protection level. It helps to discover critical vulnerabilities before they strike and make sure that current security measures are getting the job done. PT Telecom Security Assessment is an essential step to building an effective signaling vulnerability management process and shielding your core network and subscribers from cyberattacks.

## VULNERABILITY MANAGEMENT LIFECYCLE



## EXTENSIVE SCOPE, ACTIONABLE RESULTS

PT Telecom Security Assessment includes the following:

- + Simulation of attacks
- + Assessment of potential impact
- + Analysis of possible fraud
- + Forensic investigation

## RELATED REPORTS BY POSITIVE TECHNOLOGIES

The latest research by Positive Technologies shows that next-generation 4G and 5G networks built on the [Diameter protocol](#) have the same flaws as their [SS7-based](#) predecessors:

	SS7	Diameter
Call and SMS Interception	+	+
Location Tracking	+	+
Fraud	+	+
DoS	+	+

## PT TELECOM SECURITY ASSESSMENT BENEFITS

### Build Effective Signaling Vulnerability Management Process

Enhance visibility of signaling network vulnerabilities that threaten your core network and subscribers, and get expert guidance on remediation. By improving your knowledge of signaling infrastructure, telecom threats, and adversaries' action patterns, you can develop an effective vulnerability management process and reduce security incident risks to acceptable levels.

### Protect Subscribers and Core Network

PT Telecom Security Assessment helps to identify possible vectors of attack against the core network and subscribers. Such attacks could result in compromise of privacy, fraud, and degradation or even disruption of services. The goal is to discover critical flaws and vulnerabilities, as well as provide actionable recommendations, in order to stop attacks before they start.

### Stop Privacy Violations

Secure customers' trust and strengthen ongoing engagement by protecting their personal data from existing and emerging threats. Manage critical signaling vulnerabilities and get ahead of hacker attacks. Prevent malicious attempts to track subscribers' location, intercept private communications, redirect traffic, or access email and social network accounts.

### Reduce Fraud Risks

Flaws in signaling networks allow fraudsters to bypass billing systems, transfer money using forged USSD requests, steal funds with mobile banking, and hack digital wallets. In each case, revenue is lost and reputation jeopardized. Safeguard your business by timely detecting critical vulnerabilities that can cause financial losses.

### Maintain Network Availability

DoS attacks strike telecom operators harder than any other sector. Denial of service degrades network capacity, disrupts customer services, and pushes subscribers to find alternative providers. [Our research](#) shows that attempts to cause disruption have very high success rates. Reduce exposure to DoS attacks by discovering exploitable flaws and receiving remediation advice, which enables an effective response.

### Build Secure IoT Ecosystem

Attacks will proliferate as the threat surface widens to encompass connected homes, vehicles, and other smart devices in the Internet of Things. As the role of the IoT grows in daily life and critical infrastructure, corporations and governments will demand greater stability in the telecom networks that connect them. Businesses will choose carriers who take IoT security seriously.

### Stay Compliant

Strengthen your cybersecurity capabilities. PT Telecom Security Assessment empowers operators to take proactive measures and fix signaling vulnerabilities before they attract the attention of regulators. Assess your compliance level and follow GSMA and other authorities' recommendations to meet regulatory standards.



Primary Security Threats for SS7 Cellular Networks, 2016



Next-generation networks, next-level cybersecurity problems, 2017

## About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at [ptsecurity.com](http://ptsecurity.com).

© 2018 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.