SecurityGen

Telecom Security. Transcending Generations.

ACE: ARTIFICIAL CYBERSECURITY EXPERT

Breach and Attack Simulation Platform

Solution Overview Datasheet

www.secgen.com

Telecom networks have witnessed a rapid digital transformation in recent times. In addition to the introduction of Virtualization, Cloud, Artificial Intelligence, Internet of Things, and disaggregation, efforts are underway to implement 5G networks while ensuring continued compatibility with 2G, 3G, and even 4G/LTE networks. This convergence is proving to be a serious security challenge for telecom operators, as preventive protection alone is not enough anymore in this hyper-connected environment.

A Quick View Of The Underlying Security Challenges

Using signalling firewalls for border protection is no longer sufficient

Lack of effective security monitoring of interconnect networks (IDS)

Infrequent assessments create inefficiencies in telecom systems that need assured security

Identifying vulnerabilities not enough when defining priority of remediation

Increased regulations and compliance measures as 5G gets implemented

Operators vulnerable as they are only as secure as their legacy networks

Adding more woes to these operational challenges is the fact that telecom security experts are expensive and difficult to find.

Countering these challenges, operators need to conduct regular assessments to ensure that their defense and security systems are performing optimally 24x7.

Typically, telecom security teams perform assessments to test the strength of organizational defenses. These assessments are usually conducted through role-plays where the penetration testing team takes on the role of malicious attackers, while the defending team tries to identify issues and secure network breaches. Based on the outcome of these assessments, reports are created on possible weaknesses in the security of core assets and overall networks.

Unfortunately, network owners are unable to conduct these security assessments as regularly and consistently as needed, given the fact that they are resource-intensive and require very specific skill-sets. This makes them a very expensive proposition, one that network owners implement only occasionally. Consequently, the gap between scheduled assessments currently ranges from a few weeks to a few months. This leaves network owners extremely vulnerable to security threats, which if not detected on time, can wreck widespread damages.

The Solution:
Artificial Cybersecurity Expert - The ACE Platform

Backed by our team's comprehensive experience in the evaluation and testing of signalling and IP networks and to address the challenge of sporadic network security assessments, SecurityGen has developed the ACE platform - Artificial Cybersecurity Expert.

ACE is the first of its kind breach and attack simulation platform for telecom cybersecurity. We have designed ACE, not only to perform critical functions like any cybersecurity expert team but also to do so in a continuous, more efficient, and completely automated manner.

Understanding Breach And Attack Simulation (BAS)

Breach and attack simulation (BAS) is gaining momentum at a time when complexity and inter-dependence in an increasingly digital world is growing. Vulnerabilities, if undetected, can have grave consequences.

These simulations identify threats in signalling networks by mimicking actual attack scenarios and techniques used by malicious perpetrators.

It enables continuous testing for cyber security posture and helps avoid business interruptions caused by threats like leakage of subscriber data, fraud, call and traffic interception.

The inbuilt AI module enables ACE to constantly learn, enhance performance and incorporate actual, real-life scenarios and attack vectors from the field. With ACE being available 24x7, SOC/NOC teams can now continuously keep a keen watch on the security posture without incurring additional expenses.

ACE has been designed on a proactive security model that helps strengthen the security posture by constant inspectionand preventing security breaches. Insights offered by the ACE platform helps operators gauge network and subscriber safety any time during the day or night.

ACE - The Customer Benefits

- Fast time to start
- Continuous security
- Validation for timely response
- Staffing savings with zero ongoing maintenance costs
- World-leading expertise & telecom threat intelligence
- 24x7 availability
- Non-stop GSMA compliance

How The Platform Works

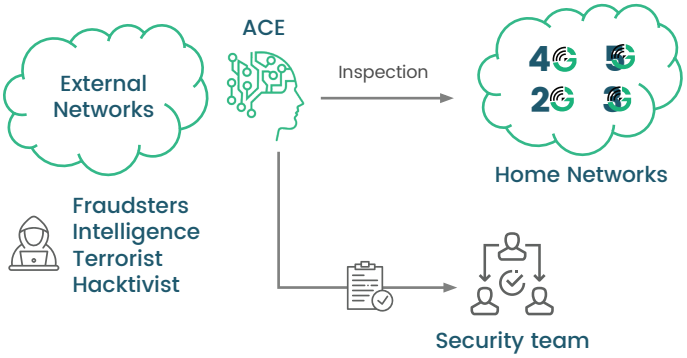
ACE with SaaS licensing delivers rapid set-up support, zero maintenance costs, and 24x7 availability. ACE provides critical services for signalling network security and GSMA compliance tests, in addition to a complete 365 signalling assessment that covers everything from 5G networks to legacy platforms like HTTP/2, Diameter, SS7, and GTP.

ACE security benefits can be availed by -

- Choosing service options and schedules
- Signing a contract and providing test subscriber data
- Receiving first results via the contact e-mail

As soon as the security inspection is completed, a comprehensive report with detailed results is made available for review. This report includes technical specifics, business impact, and recommendations for a secure response.

You can avail the ACE security service expertise by simply signing the agreement without spending time and effort in installation. In the SaaS-based model, ACE connects directly from the cloud to the customer's core network and performs inspections of the outer perimeter of the customer's core network via IPX connectivity. It can accurately identify vulnerabilities present in the network which adversaries could exploit. The good news is that this set-up does not require any reconfiguration of customer networks. Besides, ACE can be deployed as a Managed Service Provider. It will offer the same advantages as a SaaS model with the only difference that all the actual work can be performed by the experts of SecurityGen, and the customer receives the ready-made reports with minimal efforts.

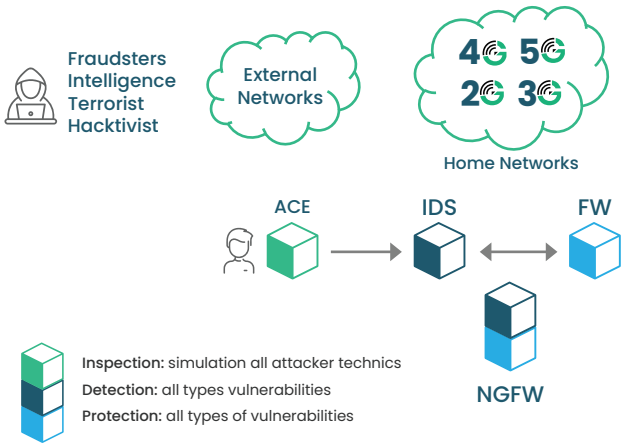


Enhanced Security
Combining Inspection With Detection & Protection Modules

ACE, the breach and attack simulation platform, logically integrates into cybersecurity model composed of the IDP platform". This synergy of ACE and te Next-Generation Signalling Protection Platform (NGFW) imparts enhanced security coverage by combining the inspect module with the Detect and Protect one.

This merging of regular security checks from ACE and NGFW traffic analysis enables operators to quickly identify blind spots and misconfigurations that could impact core network security levels.

ACE continuously reports the results of security assessments that help to cross-validate and check if signalling protection is ready and up-to-date. ACE offers a proactive security edge to signalling levels that boosts and enhances overall security posture.



ACE: The Use Cases

Ensures safe configuration - before production and after upgrades

Evaluates and makes sure that adequate security countermeasures are in place and provides valuable information in case network security levels are lowered.

Checks your border security measures effectiveness

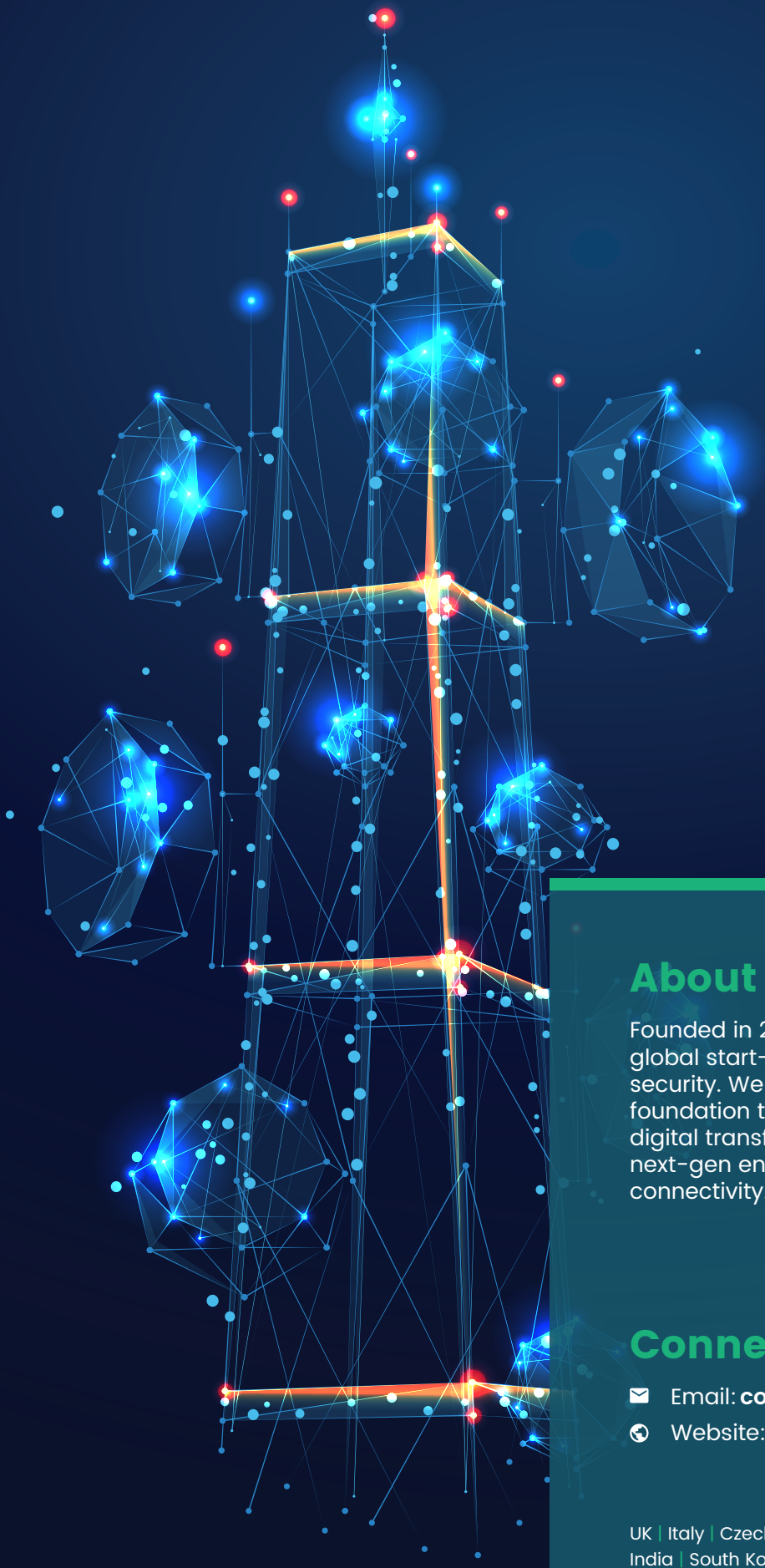
ACE empowers CSPs to conduct proactive inspections of the network for all known threats and offers diverse bypass techniques to ensure heightened security.

Assure 2FA protection - SMS

ACE ensures customer security by performing comprehensive checks to keep SMS data content thefts at bay allowing Communication Service Providers to withstand fraudulent SMS interception.

Compliance report by click

Communication Service Providers can now provide regulators with evidence of GSMA compliance or effectiveness of security measures implemented in the network with just the click of a button.



About SecurityGen

Founded in 2022, SecurityGen is a global start-up focused on telecom security. We deliver a solid security foundation to drive secure Telco digital transformations and ensure next-gen enterprise intelligent connectivity.

Connect With Us

Email: **contact@secgen.com**
Website: **www.secgen.com**

UK | Italy | Czech Republic | Brazil | Egypt
India | South Korea | Japan | Malaysia | UAE