Resilient Telecommunications Security Solutions

The world is entering into a new era of ultra-connectivity as more people and devices than ever before tap into telecommunications operator networks and come online. In this environment, resilient telecommunications operator networks are critical to ensuring service delivery.

Overview

The world is entering into a new era of ultra-connectivity as more people and devices than ever before tap into operator networks and come online. By 2025, GSMA Intelligence forecasts that figure will grow by more than 1.75 billion to reach a total of 5 billion.[1]

In the same timeframe, GSMA Intelligence predicts the market will experience massive growth in the number of IoT connections across cellular and non-cellular technologies, reaching 25.2 billion in 2025,[2] offering operators a $1.1 trillion revenue opportunity.[3]

Operator networks provide the magic to fuel this march. Uptake of 5G technology, with its lightning-fast speeds and ultra-low latency, has the potential to enable entirely new user experiences and a more intelligent kind of connectivity.

Building Trust through Automated Security Operations

Communications Service Providers (CSP) need to build "trust" into their digital environments, giving customers the confidence that their data will be protected and secure on the 5G network. But how can they do that when a growing number of services, features, and interfaces have broadened the attack surface, requiring security operations teams to deal with a higher volume and velocity of potential threats? And with the network divided into isolated slices and each 5G use case demanding different levels of security, the pressure to monitor, prioritize, and respond to incidents could be overwhelming. But it doesn't have to be.

CSPs need a new approach to security operations characterized by four capabilities: adaptation, speed, integration, and automation. Implementing these four capabilities in practice requires five critical security functions: reducing threat mitigation, maintaining compliance with ease, mitigating people-centric attacks, implementing cognitive threat detection, and applying automated response.

When combined, these five capabilities will help CSPs ensure that their 5G services and ecosystems are reliable and secure.

Managed Services Offerings

Enterprises are facing competing pressures. Digital transformation, high SaaS application use, extensive numbers of roaming workers, and expanding remote locations accelerate enterprise businesses, but also increase cybersecurity risk and compliance reporting needs. To account for the increased risk, enterprises are focusing on core competencies and outsourcing security management to trusted providers with experienced and knowledgeable professionals.

Managed Security Service Providers (MSSPs) tackle that risk for their customers by providing various SaaS offerings. CyberRes supports MSSPs with world-class identity, application, and data security SaaS solutions that can be deployed in real-time with minimal end-user friction.

With CyberRes solutions, MSSPs can:

- Minimize time to value with fast provisioning.
- Stay up to date with the latest releases and unlimited upgrades.
- Reduce capital expenditures and eliminate up-front costs.
- Free up internal resources.
- Quickly scale and only pay for what they need, when they need it.

“We were particularly impressed by ArcSight ESM’s extensive integration capability, flexible settings, high level of performance, and possible scalability in case of increasing events flow and system load.”

ALEKSANDR TURLO
Head of IT and Information Security LLC
Lifetech, subsidiary company of Belarusian Telecommunications Network

Contact us at **CyberRes.com**
Like what you read? Share it.

Big Data Protection with Data-Centric Security

The world is radically changing, with data at the center of new value creation for businesses. Smart connected devices are everywhere—from connected cars, to all manner of IoT devices—including billions of mobile devices carrying sensitive data in the hands of users across the globe. All of these connected devices feed massive volumes of sensitive data into data lakes and warehouses, enabling enterprises to gather intelligent insights about customers, operations, and competitors through analytics. Big data drives the modern enterprise, enabling business users and data analysts to identify and understand data outliers, variations from baseline, interesting data clusters, and more. But broadly enabling data access carries risks. How safe is your data in light of today’s modern threat landscape?

Among the massive volumes of data captured by enterprises is sensitive information that, if stolen, results in harmful consequences to the consumers affected and the business breached. In the age of big data, this risk exposure is exponentially more dangerous. With enterprises capturing personal information, intellectual property, health information, and more new classes of sensitive data than ever before, information in a data lake can form toxic combinations that reveal identity. Even data not apparently sensitive at face value could be combined with other disparate pieces of data to reveal personally identifiable information—and, if stolen, be used for fraud and trigger penalties due to privacy legislation.

CyberRes Capabilities for Telecom Security

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world’s largest security portfolios to helping our customers navigate the changing threat landscape by driving both cyber and business resiliency within their teams and organizations. We are here to help enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility.

We are a part of a larger set of digital transformation solutions that fight adverse conditions so businesses can continue to run today to keep the lights on and transform to grow and take advantage of tomorrow’s opportunities.

CyberRes capabilities for security include:

- Identifying, protecting, detecting, responding to, and recovering from incidents—reducing your overall risk profile and creating a modern, secure IT ecosystem.
- Maintaining data privacy, mitigating the impact of data and application breaches, and monitoring threats for compliance audit visibility.
- Applying effective risk management practices at all levels—aiding senior decision-makers with greater visibility regarding responsibility and accountability, and providing automated controls.
- Applying data and identity governance policies, detecting and responding to data breaches, and optimizing backup and recovery—and, ultimately, protecting data in use, in transit, and at rest.
- Jumpstarting your application security journey in a single day and scaling as your needs grow.

CyberRes specializes in finding and protecting sensitive data, detecting advanced threats, and helping customers adapt and evolve their security posture for the future.

Learn more at
cyberres.com/industry/telecom

1. GSMA Intelligence, “Unique subscribers and mobile internet users,” February 2018.
2. GSMA Intelligence, “IoT: the next wave of connectivity and services,” April 2018.
3. GSMA Intelligence, “IoT: the $1 trillion revenue opportunity,” May 2018.

CyberRes
A Micro Focus line of business