INDUSTRY TRENDS

Next generation technologies like 3G, LTE and high-speed broadband have revolutionized the way we communicate. Voice, video and data traffic have increased exponentially and continue to grow. To support this growth, service providers are in the process of migrating from legacy TDM access and transport networks to all IP networks. During this migration, there is a need for a more scalable, flexible and secure network that can support heterogeneous technologies.

This IP migration has also resulted in increased security breaches, DDS (Distributed Denial of Service) attacks, intrusions and network failures of core wireless and wireline elements such Circuit Core, Mobile Packet Core, RAN, IN, VAS, OSS, BSS and NGN elements. The role of CISOs (Chief Information Security Officer) in service providers has expanded beyond the CIO organization. They are now responsible for end-to-end network security, which spans IT, wireless, wireline, OSS and BSS domains. Many CISOs are now CSOs, and others are now part of the CTO organization. That’s because end-to-end network security is more than a legal issue, it can affect network performance, the customer experience and revenues.

As a result, operators worldwide are exploring how to enhance network security and create a highly secure, resilient network with the least capital and operational expenditures possible.

BUSINESS CHALLENGES

Recently, service providers across the globe have experienced damaging security incidents, such as:

- Core network outages, resulting in high emergency recovery/restoration and investigation costs
- Millions of dollars in lost revenue
- Degraded network performance
- Poor customer experiences

Plugging security gaps can require significant new CAPEX and OPEX. But this investment does not generally increase ARPU or overall revenues, so operators often make only the investments necessary to comply with security regulations.

CSOs want to use both new and existing infrastructure, such as SIEM, Probing Solutions, and Big Data platforms while implementing advanced procedures to detect and prevent security incidents—making affordable, end-to-end network security a huge challenge.

WIPRO’S OFFERINGS & VALUE-PROPOSITION

Wipro’s Telecom Network Security practice addresses all the above challenges and many more. We have extensive experience with multiple operators and equipment vendors around the globe as wireless and wireline security experts in: 2G/3G/LTE, Mobile Packet Core, Mobile Circuit Core, IMS, IN, OSS, BSS, VAS, FTTx, xDSL, PSTN, NGN.
Wipro's offerings include:

- Wireless security audits covering: 2G/3G/LTE RANs, Mobile Circuit Core, Mobile Packet Core, IMS, VAS, MPBN, OSS and BSS
- Wireline security audits covering: xDSL, FTTX, PSTN, NGN, Carrier WiFi, OSS and BSS
- Recommendations on re-using existing SIEM, probe, Big Data, analytics and reporting platforms, and closing gaps identified in security audits
- Implementation of recommended use-cases
- Managed SOC for IT, wireless and wireline networks

Ask for Wipro's IT, wireless and wireline network security references from Tier-1 CSPs across the globe in consulting, audits, design, deployment and SOCs.

Our Value proposition is: End-to-end network security with maximum reuse and minimal investment.

**SOLUTION DIAGRAM/ARCHITECTURE/BLOCK DIAGRAM**

The following diagram gives an overview of solution approach:

- **AS-IS assessment**
  - Assessment of current security infrastructure
  - Assessment of current security processes & protocols
  - Domain wise deep dive

- **Gap Analysis**
  - Identification of gaps domain wise & node-wise
  - People gaps
  - Process gaps
  - Tool gaps

- **Recommendations & Remediation Roadmap**
  - Identification of use cases to cover identified gaps
  - Recommendations on re-use of existing gear
  - Benchmarking
  - Best Practices recommendation

- **Implementation**
  - Implementation of identified use-cases
  - End-to-end program governance

**BUSINESS BENEFITS DELIVERED TO CSPS**

<table>
<thead>
<tr>
<th>ENHANCED CUSTOMER EXPERIENCE</th>
<th>BETTER PROTECTION AGAINST FRAUDS &amp; REVENUE LEAKAGES</th>
<th>ZERO NETWORK DOWNTIME ON ACCOUNT OF SECURITY INCIDENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Where customer's identity and data are critical, Wipro proposed use-cases for reducing number of incidents and help enhance customer experience</td>
<td>• Our use-cases enable proactive monitoring &amp; co-relate events &amp; logs across multiple nodes which provide better coverage against frauds &amp; revenue leakages</td>
<td>• Our use-cases ensure end-to-end network security &amp; hence provide better network protection</td>
</tr>
<tr>
<td>Upto 32% reduction in identity &amp; data theft incidents</td>
<td>Upto 18% reduction in fraud &amp; 23% reduction in revenue leakage cases</td>
<td>• Moreover, our innovative solution ensures proactive monitoring &amp; identifies events &amp; patterns which eventually lead to service disruption &amp; degradation</td>
</tr>
</tbody>
</table>

**DO BUSINESS BETTER**