Datacipher

SERVICE BRIEF

How Switching to Corero Network Security Transformed Network Security for RailTel

RailTel, one of India's largest neutral telecom infrastructure providers, faced significant challenges in maintaining network uptime due to sophisticated DDoS attacks. To address these challenges, RailTel implemented Corero Network Security's hybrid DDoS protection solution, which provided a flexible and comprehensive approach to mitigating DDoS attacks.

Customer

Established in 2000, RailTel is one of India's largest neutral telecom infrastructure providers, focusing on modernizing railway communication systems and providing nationwide broadband and VPN services. RailTel is dedicated to maintaining robust network security to ensure uninterrupted services and protect sensitive data.

Challenge

Strengthening Network Security Against DDoS Attacks

RailTel faced increasing challenges in maintaining network uptime due to sophisticated DDoS attacks. The existing security measures were insufficient to handle the evolving threat landscape, resulting in significant network downtime and operational disruptions.

To ensure robust protection against these attacks, RailTel needed a comprehensive DDoS protection solution that could integrate seamlessly with its existing infrastructure and provide real-time threat detection and mitigation.

Solution

Corero Network Security: Flexible Hybrid DDoS Protection

Datacipher implemented Corero Network Security's hybrid DDoS protection solution, which provided a flexible and comprehensive approach to mitigating DDoS attacks. The implementation process was meticulously planned and executed over a 3-month period, involving the following key steps:

Process Description

- **Initial Assessment:** Conducted a thorough assessment of the client's existing network infrastructure.
- **Customization:** Customized the DDoS protection solution to align with the client's specific requirements.
- **Deployment:** Deployed the solution in a phased manner to ensure seamless integration with minimal downtime.
- **Testing:** Conducted rigorous testing to validate the effectiveness of the solution.
- **Training:** Provided comprehensive training to the client's IT team on managing and monitoring the solution.

Datacipher

SERVICE BRIEF

Challenges and Overcoming Them

- **Integration with Existing Infrastructure:** Initially, integrating the solution with the client's legacy systems posed a challenge. This was overcome by developing custom scripts and configurations tailored to the client's environment.
- **Minimizing Downtime:** To ensure minimal disruption, the deployment was carried out during off-peak hours and in stages.

Results and Benefits Immediate Changes/ Benefits:

- **Reduced Downtime:** The client observed an immediate reduction in network downtime from an average of 20 hours per month to less than 1 hour.
- **Enhanced Security:** The client's network became significantly more resilient against DDoS attacks, with real-time threat detection and automated mitigation in place.
- **Integration with Existing Systems:** The solution integrated seamlessly with the client's existing network monitoring tools, providing a unified view of network health and security status.

Before We Go

RailTel faced significant challenges in maintaining network uptime due to sophisticated DDoS attacks. The existing security measures were insufficient, leading to substantial network downtime and operational disruptions.

By implementing Corero Network Security's hybrid DDoS protection solution, RailTel effectively addressed these issues, reducing network downtime from 20 hours per month to less than 1 hour and significantly enhancing network resilience.

For further guidance and customized network security solutions, reach out to Datacipher. Our experts are equipped to help you navigate the complexities of network protection, ensuring your infrastructure remains robust and resilient against evolving threats.

Talk to Expert: 1800-8892-877

info@datacipher.com

Contact Us