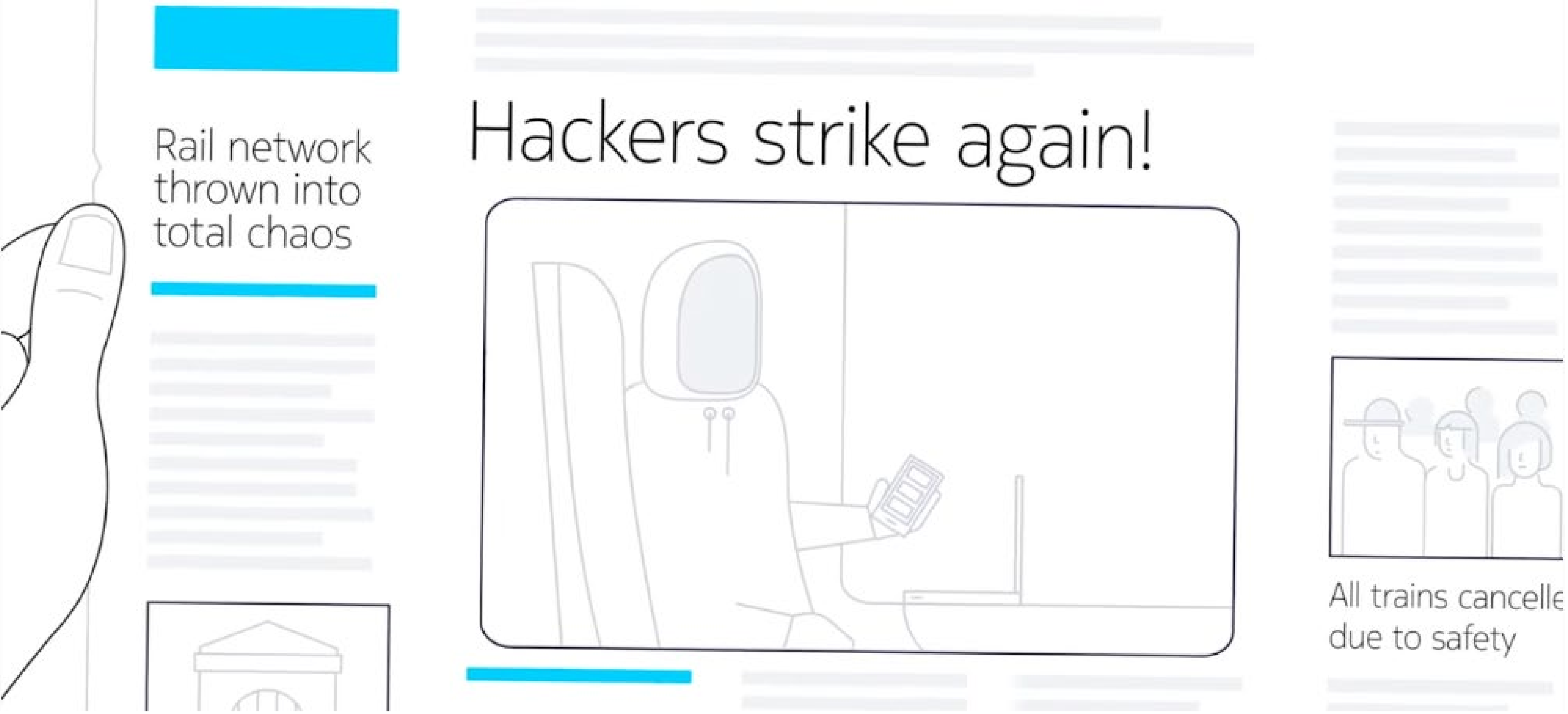
European national railway operator ramps up cybersecurity defense

State-owned operator provides nationwide passenger rail service, and is enhancing security through the modernization of its railway communications network, a state-of-the-art infrastructure ultimately expected to cover nearly 14,000 km, the largest such project in Europe.

NOKIA



Benefits

Protection of core infrastructure and services
End-to-end traffic separation and multi-zone concept hinders the spread of cyber-attacks, reducing impact and helping speed mitigation.

Topology Hiding
Key IP address information such as route and contact headers are hidden to lessen the risk of identification of users and networks to reduce the threat of targeted attacks.

Addresses regulatory and compliance requirements
Strong security access control, including central logging and review of activities, users and processes enables enforcement of access policies based on relevant roles and responsibilities.

Needs

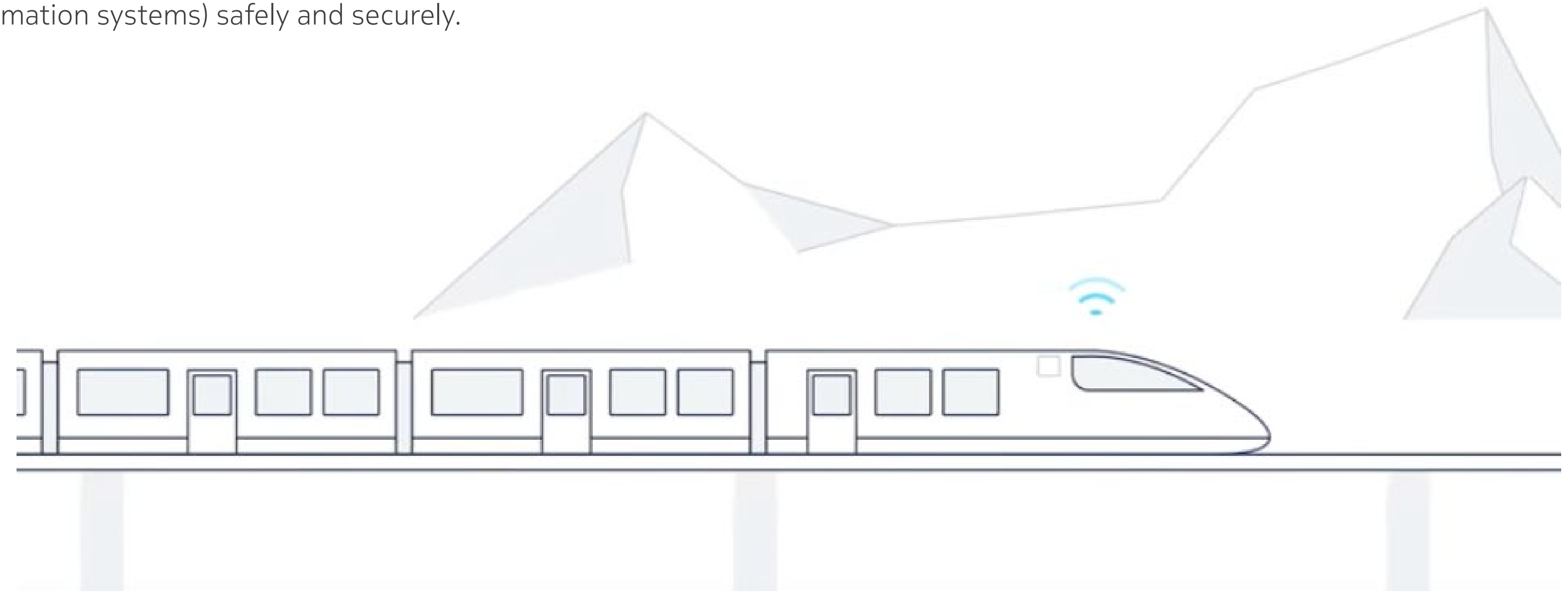
To keep trains running on time and ensure that passengers arrive at their destinations safe and satisfied 'The Railway' needs to continue the modernization of its mission-critical communications network to enhance the reliability and safety of nationwide railway operations. At the same time, it must address the increased vulnerability to cyber-attack that accompanies the advanced, IP-based technologies that are at the heart of a modern communications networks.

The railway is seeking to:

- Benefit from the dramatic improvements in operational and cost efficiency offered by IP technology, without sacrificing security
- Provide best-in-class protection for radio, core and IP network assets
- Address 'insider' and human error-related cyber-threats through the alignment of access-oriented processes and policies such as password management
- Enhance the flexibility of security functions to better adapt to fast-evolving network topology
- Exceed compliance requirements for network access and security, a substantial concern in the heavily regulated railway industry

Employing a comprehensive, in-depth cyber-security regime will enable the Railway to adopt new IP-based applications for a variety of critical functions (train control, signal control, maintenance monitoring, video protection and passenger information systems) safely and securely.

It must address the increased vulnerability to cyber-attack that accompanies the advanced, IP-based technologies that are at the heart of a modern communications networks.



The Railway's Approach

As part of a broader digital transformation, The Railway is engaged in a large-scale overhaul of the communications network infrastructure on which its operations depend. The project involves the deployment of a wireless network based on GSM-R, and a mission-critical backhaul and core network utilizing Internet Protocol/Multi-protocol Label Switching (IP/MPLS) and Dense Wavelength Division Multiplexing (DWDM) optical networking infrastructure installed alongside its nationwide rail network.

The benefits of moving to an advanced communications infrastructure are enormous, offering The Railway substantial improvements in terms of operational cost, efficiency, flexibility and scalability. Because they are more interconnected, however (unlike traditional railway communications systems, which tend to be isolated), these networks are also more exposed to potential attackers.

While cyber-criminals and state-sponsored hackers draw significant attention in the public imagination, many incidents can actually be traced back to human error, such as non-compliance with security regulations and policies or unintentional configuration errors. As important, many successful attacks are aided by simple mistakes such as the use of stale or insufficiently robust passwords.

To counter these threats, The Railway is adopting a multi-tiered approach, built around the following products:

- The Nokia NetGuard Identity Access Manager (IAM), which secures physical and virtual network functions and resources. NetGuard IAM provides unified identify access control, single sign-on with centralized policy management and advanced access management to minimize unauthorized incursions. It logs all activity that The Railway (or their contractors) performs on the network - either through direct network element access or through the relevant EMS. This ensures that all GUI access is video logged and all Command Line Interface (CLI) actions and responses are captured which allows The Railway to audit and pinpoint the cause of any erroneous or malicious activity on the critical network.
- The Nokia NetGuard Virtual Firewall (VFW), a telecom grade firewall that delivers extreme performance, making it the fastest virtual security gateway on the market today.

The Railway's new cyber-security architecture will help eliminate or quickly mitigate threats, allowing it to focus on its primary operations, delivering people quickly and safely to their destinations, by:

- Contributing to The Railway's fulfillment of the European Union requirement for ERTMS (European Rail Traffic Management System), a Europe-wide railway signaling standard
- Addressing regulatory and compliance requirements through the enforcement of centralized security access controls for The Railway's personnel
- Reducing the vulnerability of individual network elements and employing firewalls to limit the spread of attacks.

On-time arrival

The Railway aspires to provide best-in-class rail service throughout its nationwide footprint, maintaining its commitment to safety, security and passenger satisfaction. With Nokia's cyber-security solutions, The Railway is able to keep its attention squarely on its core mission, delivering their passengers to their destination.

How this approach keeps network security on track

End-to-end security protects all network technologies: The end-to-end security approach adopted by The Railway encompasses the entire network and its security processes, such as: access management and audit compliance; network security; and security management for connected devices. This expansive approach helps ensure operations are free from disruptions.

Network segmentation and firewall confine threats: Network segmentation enables different types of traffic and different parts of the network to be isolated, hampering the lateral movement of threats and limiting their impact.

Ensuring security compliance: Railway operators face increasingly stringent legal, regulatory and compliance requirements. The Railway's new cyber-security infrastructure offers built-in features designed to simplify compliance tracking and reporting requirements.

Protection against financial damage: Security incidents can be costly, in terms of the loss of revenue from disrupted passenger services, recovery and restoration costs, potential lawsuits, damage to brand reputation, compensation to users and non-compliance penalties. The enhancements to The Railway's cyber-security infrastructure can help reduce these risks.

Focusing on running rail operations: The Railway can reduce the burden of tracking and responding to security events and focus more attention on its transportation mission.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID 206737

NOKIA

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.