Resilient Transportation Security Solutions

Cyber resilience in transportation is essential to reduce risk—at the individual incident and global economy levels. If any segment is affected (air, sea, or ground), the impact can be felt across the supply chain, sometimes with life or death implications.

Secure Digital Transformation

The transportation industry relies heavily on technology for improving the customer experience, efficiency, and operations. Industry 4.0 capabilities such as Industrial IoT (IIoT), “smart” systems, cloud infrastructure, and mobile devices and applications are at the root of the digital transformation in transportation. These technologies can provide increased automation, self-monitoring/healing, and greater efficiency. The next phase of this transformation includes artificial intelligence, machine learning, and self-managed ecosystems. For example, vehicles that self-detect issues and proactively notify the owner, the manufacturer, and dealership can schedule a service appointment according to the owner’s schedule. The same can happen across a fleet of vehicles, planes, trains, or ships. However, this increased reliance on technology also opens these systems to cybersecurity risks. Targeted attacks or outages could cause significant damage with major, life-altering impacts. Including security in the development phase of the technology helps ensure that IIoT or smart devices have protective controls built in, applications are secured prior to production, and data is secured at collection to reduce future fleet recalls.

CyberRes Security Operations and Application Security portfolios provide protective security controls for IIoT devices, cloud, and mobile applications.

Big Data Protection with Data-Centric Security

The benefits of Industry 4.0 and 5.0 include self-monitoring/healing systems, improved efficiency, and increased automation. They require high volumes of data to provide real-time visibility into the performance, activities, and behaviors of the different transportation modes and the things with which they interact.. This data can include product performance, inefficiencies, reactions to external situations, and personal information (such as geolocation, biometric data, passwords, financial information, travel habits/routines, passport information, and much more). Once collected, it can be centralized, and analyzed to provide real-time route optimization, identify design inefficiencies and cost savings, and offer customer insights that drive innovation. Additionally, global privacy and industry-specific regulations provide requirements on how personal and financial information should be handled. The transportation industry must consider the impact of big data initiatives and protect sensitive data–including who has access to what types of data.

CyberRes Data Privacy and Protection portfolio and the Identity and Access Management portfolio are designed to provide a governance framework, data-centric security, and monitoring controls for data and identities.

Trusted Mobile Experiences

For transportation sectors that focus on direct interactions with end customers, mobile and web experiences provide a competitive differentiator. All modes of transportation now include a mobile interaction option. Examples include SMS text messages for deliveries or an in-app experience to interact with a vehicle; a seamless, human interaction-free check-in experience; or purchasing tickets and confirming booking details. This enhanced experience also opens the door to new areas of attack. The transportation industry has experienced numerous breaches on mobile and web applications because of unsecure applications, unencrypted data, and unauthorized access. Customer-facing applications must be secured as part of the software development lifecycle prior to release into production. Once data is provided by the customer, it must be encrypted throughout its lifecycle. And, for further protection, granular access should be applied to authorized customers and employees once they are provisioned.

CyberRes portfolios for Security Operations, Data Privacy and Protection, and Identity and Access Management are designed to provide a seamless, secure experience during all customer interactions.

CyberRes Capabilities for Resilient Transportation Security

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world's largest security portfolios to help 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 can provide solutions that drive resilience in the transportation sector and enable desired business outcomes.

The CyberRes Security Operations portfolio includes the ability to protect sensors and devices embedded into transportation vehicles or backend systems. It also builds a unique profile at scale across an entire fleet of devices. This capability automatically protects and monitors for previously unknown attacks, resulting in a more resilient connected device ecosystem. We leverage the power of an analytics engine that includes over 450 algorithms to analyze data at scale to detect insider threat, data exfiltration, lateral movement, and privileged escalation.

CyberRes Data Privacy and Protection portfolio augments a data governance framework with technology that can discover, classify, and protect data collected for business purposes within the structured and unstructured systems used to store it The data can be secured in its original format, ensuring that downstream processes use the data. It is pseudonymized using AES-256 encryption to remove the risk of unauthorized access and ensure near zero impact of a successful breach.

CyberRes Identity and Access Management offerings provide frictionless identity benefits to mobile apps—including those for connected vehicles, airplanes, trains, and ships—while elevating security with adaptive access. It takes into account the past behavior of a user and the sensitivity of the application, and then determines the authentication required to access the application. Adaptive access reduces risk of access to sensitive resources by asking users to further demonstrate that they are who they say they are. CyberRes Identity and Access Management offerings provides governance and management for millions of customer accounts in existing transportation industry customers. Leveraging our established industry offerings, transportation customers can build a seamless and secure customer experience across the mobile and web landscape.

Contact us at **CyberRes.com**

Like what you read? Share it.