Solution Brief

Smart Transportation

It’s time for a transportation transformation.

Transportation systems are at a crossroads. We can choose to tolerate increasing congestion of our city roads, airports and harbors, or we can forge ahead with increasingly efficient, environmentally friendly and secure modes of transport and transportation hubs that take advantage of smart technologies. At ForeScout Technologies, we’re forging ahead with security solutions that are helping transportation professionals embrace smart technologies that are the basis for tomorrow’s smart transportation systems.

Organizational Challenges

- Improve transportation safety and efficiency
- Securely embrace IoT and smart vehicle innovations
- Leverage existing network security investments
- Maintain resiliency and availability of critical services
- Comply with current regulatory mandates and anticipate future requirements
- Protect sensitive systems and data

Technical Challenges

- Discover unknown devices such as IoT sensors that do not include security software
- Ensure security software is up to date on endpoints
- Classify endpoints and determine their owners
- Scale to address rapid growth, distributed networks and smart transportation operations centers
- Assess and continuously monitor endpoints
- Correlate and analyze data to detect anomalous behavior
- Prevent infected or non-compliant endpoints from spreading malware across networks

Challenge: IoT and Cybersecurity

Smart transportation proponents envision efficient and sustainable intermodal transport systems and infrastructure that can deliver levels of intelligence and performance that make gridlock on roads and at airports and seaports a thing of the past. However, tomorrow’s smart transportation systems will be made possible through the integration of countless devices, networks and other key infrastructure, *all of which must be secured*. Otherwise, one rogue device or errant application can wreak havoc.

In fact, *every* device or sensor that connects to the network broadens the attack surface, creating a potential entry point for cybercriminals to hack to or hack through. Without advanced cybersecurity, unauthorized access to critical systems, information theft and malicious cyberactivity will thrive in the future’s ultra-connected, highly automated and data-driven environment.

Smart devices and sensors, collectively known as Internet of Things (IoT) devices, are manufactured by multitudes of vendors who haven’t put a premium on security. As a result, their products often feature few if any built-in management or security capabilities. And these highly vulnerable “Things” are already being exploited:

- On November 25th, 2016 the San Francisco Municipal Transportation Agency (MUNI) was hacked, shutting down ticketing systems and compromising more than 2,100 of the agency’s computers as cybercriminals demanded payment of $70,000 in ransom, forcing the agency to operate free service for two days.[1]
- In 2014, a University of Michigan team accessed a traffic light network using readily available hardware. Once inside the system, the team quickly gained the ability to change traffic signals, alter logic commands and disable signal devices.[2]
- IoT devices can be hacked in as little as three minutes, but can take days or weeks to remediate.[3]

Moving forward, the big question for smart transportation system planners will be, “Who is responsible when a device, network or infrastructure component is compromised?” Sophisticated tools and wide-ranging expertise will be required in order to ensure that responses to attacks are appropriate, immediate and effective.

> “Our unity as a nation is sustained by free communication of thought and by easy transportation of people and goods.”
>
> **— President Dwight D. Eisenhower, February 22, 1955**

Challenge: Information Technology Service Management (ITSM)

We’ve come a long way since the first electronic control units showed up in mass-production GM and Ford vehicles in the 1970s. Today, modern cars, buses, planes, trains, trucks and ships are mobile, network-connected datacenters with systems designed to ensure operational efficiency and safety. And that level of complexity pales in comparison to the autonomous vehicle fleets of the not-so-distant future. The connected devices within these vehicles and infrastructure will need constant attention. They will need to be identified, inventoried, analyzed and monitored. Everyone from fleet operators and maintenance staff to transportation crews, safety personnel and emergency response teams must have up-to-date device visibility and performance data. ITSM capabilities will be prized like never before.

Challenge: Rapid Incident Analysis and Response

The digital transformation required for smart transportation will result in vast amounts of data being generated by new devices—data that must be correlated, analyzed and acted upon in near real time. New levels of system orchestration and automation will be needed to bridge data silos and allow analysts and interconnected systems to quickly respond to security incidents, accidents, weather events, changing traffic flows and other unanticipated factors that impact smart transportation systems. Traffic operations teams will need this data to understand both short- and long-term trends, event relationships and consequences. In addition, they will need to continuously monitor and analyze security events and device behavior. This can help prevent cybercriminals from hacking through video cameras, printers or other IoT devices to steal data or wage distributed denial of service attacks on the network.

> Smart transportation operations centers must be able to continuously monitor the security posture and performance of managed, unmanaged and IoT devices—and share this data with SIEM and ITSM tools in real time.

The ForeScout Solution

Transportation system administrators and planners face constant threats as new types and higher volumes of devices increase the complexity and expand the attack surface of their networks. To address these formidable challenges, ForeScout offers agentless visibility, continuous monitoring and control of devices over wired *and* wireless networks. In addition, our solutions share contextual device data with third-party systems to dramatically improve the ability to correlate data and events in transportation operations centers, improve security, better-manage traffic flow and optimize smart vehicle management and maintenance.

Our solutions deploy quickly without disrupting users, work with new and existing infrastructure and enhance the effectiveness of tools that public- and private-sector IT teams already use. Equally important, they scale, as proven by deployments in networks exceeding 1,000,000 endpoints. ForeScout solutions deliver value in three distinct ways:

See The ForeScout platform’s agentless visibility capabilities allow it to see a comprehensive range of devices—managed and unmanaged, corporate and personal, wired and wireless—even personally owned Bring Your Own Device (BYOD) endpoints and rogue devices. Our heterogeneous platform also discovers and classifies the vast array of IoT devices that comprise smart transportation systems. It sees devices in incredible detail, identifying and evaluating network devices and applications as well as determining the device user, owner, operating system, configuration, software, services, patch state and the presence of security agents. In addition, it continuously monitors devices, ports and connections.

Control The ForeScout platform provides a broad range of control, notification and remediation options. For example, it offers real-time dynamic segmentation that allows you to limited access to users and specific IoT devices within secure VLAN segments based on device ID or user roles. Devices that contain risky applications or out-of-date security software can be quarantined within an isolated VLAN and directed to a self-remediation site before gaining network access, while non-compliant, company-owned devices can be remediated automatically. The platform also provides policy-based notifications to end users, IT management systems, maintenance staff or team members in the transportation operations center regarding security or operational issues.

Orchestrate The ForeScout platform offers extensive interoperability with leading switch manufacturers' products. It also offers straightforward integration with leading firewalls and more than 70 network, security, mobility and IT management products* via ForeScout Extended Modules. These modules share contextual device data with third-party systems, automate policy enforcement across disparate solutions, bridge previously siloed IT processes, accelerate system-wide response and more rapidly mitigate risks. For example, Extended Modules for Security Information and Event Management (SIEM) solutions dramatically improve the ability to correlate data and events in transportation operations centers and quickly act upon these insights. Extended Modules for ITSM solutions can optimize the management and maintenance of vehicles, fleets and myriad digital assets.

Benefits

ForeScout helps protect confidential data, demonstrate compliance with regulations and provide secure network access for a wide range of devices and user populations. What's more, ForeScout achieves this in a cost-effective, efficient and non-disruptive manner. Our cybersecurity and ITSM solutions help you:

- Control access to your networks and confidential data
- Gain visibility into device identity, compliance and ownership wherever in the transportation system a device resides
- Provide security controls for IoT endpoints and other network-connected devices that can't run agents or supplicants
- Prevent infected or non-compliant devices from spreading malware across the network
- Enable employees and guests to use their personal devices while preserving security
- Provide secure wired and wireless access control to vehicles, fleets and infrastructure
- Continuously monitor devices for security and compliance
- Comply with regulatory mandates and directives designed to protect sensitive information

FORESCOUT

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] *Forbes*, November 28, 2016 https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/#5ebc65947061
[2] "The Future of Smart Cities: Cyber-Physical Infrastructure Risk," U.S. Dept. of Homeland Security, August 2015
[3] How Hackable Is Your Smart Enterprise, https://www.forescout.com/wp-content/uploads/2016/10/iot-enterprise-risk-report.pdf

*As of March 31, 2017