FORESCOUT

Organizational Challenges

- Protect sensitive systems and citizen data
- Securely embrace IoT and smart utility innovations
- Preserve investment in legacy infrastructure
- Leverage existing network security investments
- Ensure interoperability with current and future systems
- Maintain resiliency and availability for critical public services
- Comply with regulatory mandates

Technical Challenges

- Discover unknown devices that do not include security software
- Classify devices and determine their owners
- Ensure security software is up to date on devices
- Scale to address rapid growth and distributed networks
- Assess and monitor devices to detect anomalous behavior
- Prevent infected or non-compliant devices from spreading malware across the network

> Cybersecurity continues to be the lowest-rated core capability in state and territory self-assessment."
>
> **— 2015 *Nation Preparedness Report*, U.S. Department of Homeland Security**

Smart Cities

Smart Cities Require Smarter Cybersecurity.

Smart cities promise to automate critical public services, improve community interaction and drive untold levels of efficiency in a connected, technology-driven society. The potential benefits are boundless, but the cyber-risks are also considerable. ForeScout Technologies, Inc. has a proven history of helping government organizations, municipalities and businesses securely embrace smart technologies, mobility and the Internet of Things.

The Challenge

Smart city advocates envision sustainable cities that will provide residents with urban areas that deliver high-quality living as it applies to the environment and the economy. These cities will be made possible through the integration of technology, innovative design and automated processes.

With 54-percent of the world's population currently living in urban areas, old-economy cities are being *upgraded*, and huge investments are underway to fulfill the vision of the smart city. In fact, the smart cities market is expected to be worth a cumulative $1.5 trillion by 2020.[1] This massive retrofitting involves hundreds of thousands of sensors deployed throughout a city feeding big data city management systems and commercial applications that stream real-time information to residents about traffic flows, parking space availability, public transportation arrival times, air and water quality, energy consumption, developing emergencies and more.

While the smart cities promise is poised to deliver many valuable time- and resource-saving conveniences, these services require sophisticated cybersecurity. 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 sophisticated cybersecurity, unauthorized access to critical systems, information theft and malicious cyberactivity will thrive.

These smart devices and sensors, collectively known as the Internet of Things (IoT), are referred to as cyber-physical systems (CPSs), which are manufactured by various vendors with little or no built-in management or security capabilities. Put simply, they present an enormous attack surface that smart city planners must consider—one that is already being exploited. Here are just a few examples:

- The city of San Diego, California, which uses more than 400 different applications, experiences an average of 60,000 cyberattacks per day[2]
- 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[3]
- During the summer of 2015, three teenage boys hacked into a high school records system in Long Island, New York, and altered the grades of two students and the fall schedules of about 300 students[4]

1 Frost & Sullivan, "Strategic Opportunity Analysis of the Global Smart City Market"

2 http://www.marketwatch.com/story/the-mind-boggling-risks-your-city-faces-from-cyber-attackers-2016-01-04

3 "The Future of Smart Cities: Cyber-Physical Infrastructure Risk," U.S. Dept. of Homeland Security, August 2015

4 http://abcnews.go.com/US/ny-high-school-students-accused-hacking-computer-system/story?id=34617530

Customer Benefits

- Control access to your networks and confidential data
- Provide adequate security
- Help prevent infected or non-compliant devices from spreading malware across the network
- Enable government employees to use their personal devices while preserving security
- Provide secure wired and wireless access control in public schools, libraries and city administration networks
- Monitor vendor-provided/managed machines for security and compliance
- Help with compliance to North American, European and international regulatory mandates and directives designed to protect sensitive information, such as FISMA, NERC, ISO/IEC 27001 and the GDPR[5]
- Assist in demonstrating compliance with industry-specific regulations such as HIPAA and HITECH, as well as regulations established by OSHA[6]

Learn more at
www.ForeScout.com

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
Fax 1-408-371-2284

Are we prepared to address the cybersecurity threats that smart cities will surely face? How will the necessary core capabilities in cybersecurity be achieved? A recent Federal Emergency Management Agency (FEMA) State Preparedness Report highlights reasons for concern. Submissions were similar to the previous year, with cybersecurity once again receiving the lowest self-assessment rating from 56 states and territories. Cybersecurity accounted for the top three gaps in the report.

The ForeScout Solution

Modern and smart cities face constant threats as new types of devices expand the attack surface of their networks. ForeScout offers unique capabilities, including agentless visibility, to address these formidable challenges. Our solutions deploy quickly, without disrupting users, work with new and existing infrastructure and enhance the effectiveness of tools public sector IT teams already use. Equally important, they scale to meet the incredible growth needs of smart cities, with proven deployments in customer networks exceeding 1,000,000 endpoints. ForeScout solutions deliver value in three distinct ways:

See You can only secure what you can see. Smart cities will include video surveillance systems, traffic signals, kiosks, mobile devices, critical infrastructure sensors and countless IoT endpoints. ForeScout offers the unique ability to see these devices the instant they connect to municipal networks, without requiring software agents or prior knowledge of these devices. ForeScout can discover and classify devices and assess whether they are secure or not. Plus, our solution continuously monitors devices, ports and connections.

Control Smart cities must be able to enforce the appropriate level of access control based on the city's policies and the severity of the situation. For example, a city employee whose mobile device has risky applications or out-of-date security software can be directed to a self-remediation site before gaining network access. On the other hand, if water or waste treatment plant sensors have been compromised or a self-pay parking kiosk starts trying to access HR records, immediate blocking, quarantining and alerting must occur. ForeScout provides a broad range of automated control and remediation options.

Orchestrate Smart cities must support critical public safety services such as police, fire and other emergency response services. Securing this infrastructure and maintaining availability requires immediate response to security incidents. ForeScout extends its See and Control capabilities to leading network, security, mobility and IT management products, allowing a unified and automated security response while reducing the cost and complexity of securing smart city infrastructure. Plug-and-play integrations are available for third-party products through a rapidly growing number of ForeScout Extended Modules.

ForeScout helps municipal IT professionals by helping protect confidential data, assisting with their compliance of regulations and providing 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.

5 Regulatory legislation or standards: The Federal Information Security Management Act (FISMA), North American Electric Reliability Corporation (NERC), International Standardization Organization/International Electrotechnical Commission (ISO/IEC) and General Data Protection Regulation (GDPR).

6 Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH) and Occupational Safety and Health Administration (OSHA).