USE CASE: SMART CITIES

Providing the Keys to Local, County & State Governments both in the U.S. and Europe

SITUATION ANALYSIS

In 2018, the number of major metropolitan cities relying on or developing a comprehensive smart city plan – as opposed to implementing a few innovative projects without an overall smart plan – dramatically increased. For example, cities in the United States like Philadelphia, Newark and Chicago all have goals to upgrade and to become leading 'SMART" cities. Other large EU Cities like London, Paris and Berlin are also leading the SMART city initiative.

A significant investment is being made by cities in data connectivity providing a number of new technologies such as Wi-Fi 6, smart grid, and IOT sensor devices, all promising to enhance overall visibility and security. For example, the City of Newark recognized that providing companies with the ability to move large quantities of data quickly gives a city a competitive advantage over its rivals. And, cities like Newark, has the most dark fiber underground than any other city, with thousands of miles of high-speed fiber for business to gainaccess to the fastest internet in theregion.

But when cities decide to transform to a SMART CITY, they also serve as a technology hub and gateway to major institutions such as banks, hospitals, universities, law enforcement agencies, and utilities. This means the storage and transmission of customer data such as social security numbers, addresses, credit card information, and other sensitive data, is a potential goldmine for malicious actors.

In addition, many initial projects are being taken on by the Department of Transportation (DOT) to monitor roads, signs, traffic and traffic lights (infrastructure) notwithstanding metro services. Many cities now have mobile apps for "Where is My Bus" or apps for Smart City First Responders correlating with Smart buildings throughout the City. And, all of these SMART resources must be kept secure from threats at alltimes.

CHALLENGES

1 WHEN CONNECTIVITY & INNOVATION MEET INFRASTRUCTURE

When connectivity and innovation meet such large city infrastructures, they immediately become vulnerable to cyber threats from malicious actors waiting to bring all that hard work to a standstill. Many Smart City Vendors providing the new technologies do not employ strong encryption.

2 SENSITIVE DATA VULNERABLE TO DATA BREACHES

When a Smart City serves as a technology hub and gateway to major institutions, agencies and critical services, it is not a matter of if but when sensitive data may fall into the wrong hands, whereby citizens and major business and services could suffer harmful consequences.

So, any data breach must be detected immediately before the infection spreads from network system to network system, potentially shutting off critical services for thousands of companies, notwithstanding for those who reside in the City itself.

3 UTILIZATION OF THE MOBILE OUTSIDE OF A COMPANY'S NETWORK

More importantly, data breaches and the insertion of malware can be catastrophic to companies transmitting sensitive data to/from and outside of this massive network infrastructure. Most companies think data can be safely transmitted as long as it is within a company's network, but millions of customers access their mobile and cloud applications linked to their employer on a daily basis, all outside of the safety of the organization's network infrastructure.

4 PROTECTING LARGE VOLUMES OF DATA MOVING ACROSS A VAST & OLDER INFRASTRUCTURE

Protecting large volumes of sensitive data moving across a multi-user network, with numerous locations, can be extremely challenging. It is this complexity that often overwhelms a network security team's ability to ensure sensitive data is protected with encryption, especially when network infrastructures can be constructed using different vendor technology. This also includes many municipalities who have older Legacy, third party or disaggregated networks.

So, choosing the right encryption solution is critical and can be very helpful in mitigating damage caused by a data breach. Most cities find implementing these solutions disruptive and complex, especially for organizations that operate large and diverse networks. For example, manual configuration of encryption can lead to human error unknowingly exposing risk and managing multiple vendors can be burdensome and inefficient. Most importantly, network visibility is lost with many encryption solutions, which is a significant issue as it reduces the ability for security teams to detect and thwart malicious actors and cyber threats.

SOLUTION REQUIREMENTS

Before making a decision whether a city is ready to enter the SMART CITY arena, a market analysis of the technology available within that city must take place along with designing and testing of proposed new technologies with largeinfrastructure vendors. Cities have been aligning with a number of small companies, big network infrastructures and telecommunications vendors to get SMART CITY technology off the ground. Often a local City College is involved with testing and design to offset the limited resources the City may have.

As mentioned, many of the initial projects may be collaborations with or led by the Department of Transportation (DOT) in order to monitor a city's urban infrastructure. For example, DOT may want to ensure new metro smart technology can integrate and interoperate with the current transit technology before upgrading and incurring added expenses.

THE SOLUTION

PROVIDING THE KEYS TO THE SMART CITY

SIMPLE, SCALABLE & UNCOMPLICATED

As metro cities race to be the first SMART CITY, Certes Networks can help municipalities to overcome the disruption and complexity that comes with the deployment of a more automated infrastructure. The vulnerabilities and threats associated with trying to protect large volumes of data moving across a vast multi-user network involves a security strategy that is simple, scalable and uncomplicated in order to avoid any disruption of critical infrastructure services provided to businesses or citizens. And, as most local municipalities are governed by state or federal cybersecurity regulations, please be sure to understand which Certes Networks encryption solution will be best for compliance assurance.

CERTES LAYER 4 SOLUTION

While competitors offer encryption methods that are often disruptive and complex, the Certes Layer 4 solution enables encryption of data in transit independent of network applications and without having to move, replace or disrupt the network infrastructure. This is a significant savings in resources, time and budget.

VISIBILITY

Network blind spots due to problems, outages, and cyber-criminals using encryption to conceal malware, increase network security risk and are potential regulatory compliance issues. According to a recent survey from Vanson Bourne, roughly two-thirds, or 67 percent, of organizations say that network blind spots are one of the biggest challenges they face when trying to protect their data.[1]

At Certes Networks, we know it is not always possible to be aware of everything within and moving through your network and network monitoring remains one of the strongest defenses against blind spots. That's why we offer network visibility through our Layer 4 solution and encryption management tools that keep a close and constant eye on network traffic. Certes Networks network visibility tools allows existing applications and net performance tools to work after encryption is turned on without blinding the network.

OBSERVABILITY

With the Certes Observability feature, it is simple to provide this valuable add-on tool to assist in strengthening the customer's security posture. This feature is used to analyze and gain deeper understanding of network policy deployment ***and policy enforcement*** to analyze every application that tries to communicate across the network. And, all the while monitoring pathways for potential threats now that each policy is observable in real-time.

THE RESULT

By implementing Certes Networks encryption management solutions, SMART CITY projects are more flexible and secure. Through these solutions, cities can benefit from Certes visibility, micro-segmentation, and observability tools that can help cities make better network decisions and provide improved services. Certes can provide an initial SMART CITY architecture for City service key management through enforceable policies that can be analyzed to help identify network vulnerabilities and thwart potential threats.

Providing better technology is an ever-evolving, fast-paced race and caution should be given to those cities who move so fast that they risk building an infrastructure without equally giving precedence to the protection of data of those who work and live in their city. Make your SMART CITY a DATA SECURE CITY.

[1] Hide and Seek – Cybersecurity and the Cloud, VansonBourne, Aug 2017

CERTES NETWORKS

Contact CertesNetworks

300 Corporate Center Drive, Suite140
Pittsburgh, PA15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.