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 USE OF THE MOBILE OUTSIDE A COMPANY 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 PROTECT 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

Certes Networks Provable Security™

To help network security teams to achieve their goals of keeping SMART CITIES and their data safe, the team must begin to think of data security as a measurable contribution to the organizations.

Certes Networks Provable Security™ introduces a new way to think about data security and the effectiveness of your security strategy based on the Certes Five Pillars, key performance indicators (KPIs) that are ***quantifiable, measurable and outcomes driven.***

How We Deliver on Provable Security

Certes Networks Provable Security™ is supported and interconnected by the Certes Five Pillars. Each pillar is a KPI that measures the value that the security strategy delivers to an organization as a whole.

The Certes Layer 4 technology solution delivers on these KPIs and is able to quantify security's role to build, modify and measure a security strategy that aligns and protects the needs of SMART CITIES, and their vendors offering new technology, while mitigating risk.

The Certes Five Pillars

PILLAR ONE: POLICY ENFORCEMENT

Certes Networks Provable Security™ starts with the premise that policy enforcement is only as good as the policy defined and how that policy is enforced

While threats are virtually infinite, access to data is defined and is, therefore, finite and measurable. By enabling policy and enforcing that policy at a highly granular level, risk can be eliminated and data security can be quantified, measured and outcomes driven.

PILLAR TWO: CRYPTO-SEGMENTATION

Crypto-segmentation, removes the implicit trust we traditionally place in our network and creates a reduced scope of trust per policy, protection by encryption, to securely separate data flows between applications and workloads as defined by fine-grained policies.

This security control is simple to deploy, however it increases the complexity involved for any attacker trying to exploit a network over which targeted data flows. This is a quantifiable and measurable metric.

PILLAR THREE: SCALABILITY

Scalability refers to the Certes Layer 4 technology, a simple and scalable, end-to-end encryption management solution that is network agnostic easily integrating into any network infrastructure, fully interoperable with the existing security stack with zero impact to performance.

Certes Networks offers the ability to support multiple deployments across a multi-vendor environment on any network or transport. With Certes Layer 4 technology, a customer can be sure that their data assurance posture will scale to support the depth and breadth of a customer's environment, whether deployed top-of-rack, in a virtual environment, between data centers and applications (east to west) or simply just across the WAN or SD-WAN.

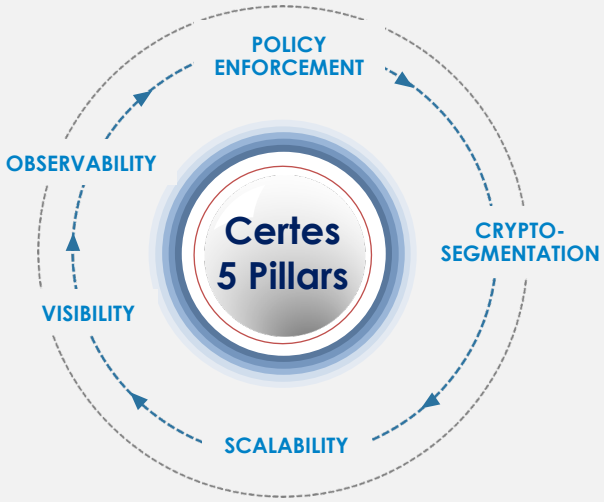
PILLAR FOUR: VISIBILITY

The Certes Layer 4 solution encrypts data in transit allowing for secure encryption of only the payload enabling transparent deployment that operates independently of applications and the underlying network with zero changes to routers, switches and firewalls. Network visibility and operational functionality are thereby fully maintained with zero impact to performance.

PILLAR FIVE: OBSERVABILITY

Certes Observability is the linchpin that provides real-time contextual meta-data enabling rapid detection of out-of-policy data and fast response and remediation to any non-compliant traffic flow or policy change to maintain the required security posture on a continuous basis. Certes Observability provides evidential and visual proof that an organization's security strategy is effective.

CERTES NETWORKS PROVABLE SECURITY™



Quantifiable, Measurable and Outcomes Driven

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

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

info@certesnetworks.com
sales@certesnetworks.com