Publication: Business Chief Europe
Date: 09.03.20
URL: https://www.businesschief.com/leadership/8582/Providing-the-keys-to-the-smart-city
Title: Providing the keys to the smart city
Author: Sean Wray, VP NA Government Programs, Certes Networks

Providing the keys to the smart city

Sean Wray, VP NA Government Programs, Certes Networks

Smart cities seem inevitable. According to IDC, Smart City initiatives attracted technology investments of more than $81 billion globally in 2018, and spending is estimated to grow to $158 billion in 2022. Similarly, 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.

In the US, for example cities like Philadelphia, Newark and Chicago all have goals to upgrade and to become leading 'SMART' cities, while UK innovation is being spearheaded by major conurbations such as Bristol, London and Manchester.

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. However, as we extend the reach of technology and connectivity, there will increasingly be cyber-risks to take into account. As part of their transformation, smart cities 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. Not to mention an increasing number of projects monitoring roads, traffic, traffic light and metro services, all of which must be kept secure from threats at all times.

Security Challenges

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. And, the routes in are manifold.

We are increasingly dealing with connected versions of devices that have existed for a long time, such as CCTV cameras, and as a consequence, digital security is not very often incorporated into their designs.

In addition, cybersecurity will have to extend far past personal, or internal corporate networks, to encompass far-ranging technological protection for vast city networks at a scale and a pace many are struggling to respond to.

Moreover, the sheer volume of data being collected and transmitted across a multi-user network, with numerous locations, can be extremely challenging to protect. London's City Hall Datastore, for

example, holds over 700 sets of big data that helps address urban challenges and improve public services, and the rise in cashless payment methods for transport.

It is the complexity that the above factors represent 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, many of whom do not provide strong encryption. This also includes many municipalities who have older Legacy, third party or disaggregated networks.

It is therefore not a matter of if but when sensitive data may fall into the wrong hands. Network security teams have to ensure that 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.

Providing the Keys

Choosing the right encryption solution is critical and can be key in mitigating damage caused by a data breach. Most cities find implementing these solutions disruptive and complex, especially for organisations 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.

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, not to mention be compliant with governmental cybersecurity regulations and / or code of practices.

Whereas traditional Layer 2 & 3 encryption methods are often disruptive and complex, a 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.

In addition, 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[i], roughly two-thirds, or 67 percent, of organisations say that network blind spots are one of the biggest challenges they face when trying to protect their data.

With network monitoring one of the strongest defences against blind spots, Layer 4 encryption and encryption management tools offer network visibility by keeping a close and constant eye on network traffic. Network visibility tools allows existing applications and net performance tools to work after encryption is turned on without blinding the network.

Finally, adding in network observability allows smart cities to analyse and gain deeper understanding of network policy deployment and policy enforcement by scrutinising every application that tries to

communicate across the network, all the while monitoring pathways for potential threats now that each policy is observable in real-time.

For organisations and teams tasked with implementing smart technology in residential, commercial and public spaces, plans on how to do so will have to be part of the design and planning stage – including how we securely implement and maintain these smart spaces. It is integral that all connected aspects of smart cities have undergone extensive planning and designing, with a smart city architecture for service key management at the core. Defining standards and enforceable policies that can be analysed to help identify network vulnerabilities and thwart potential threats is critical.

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.
