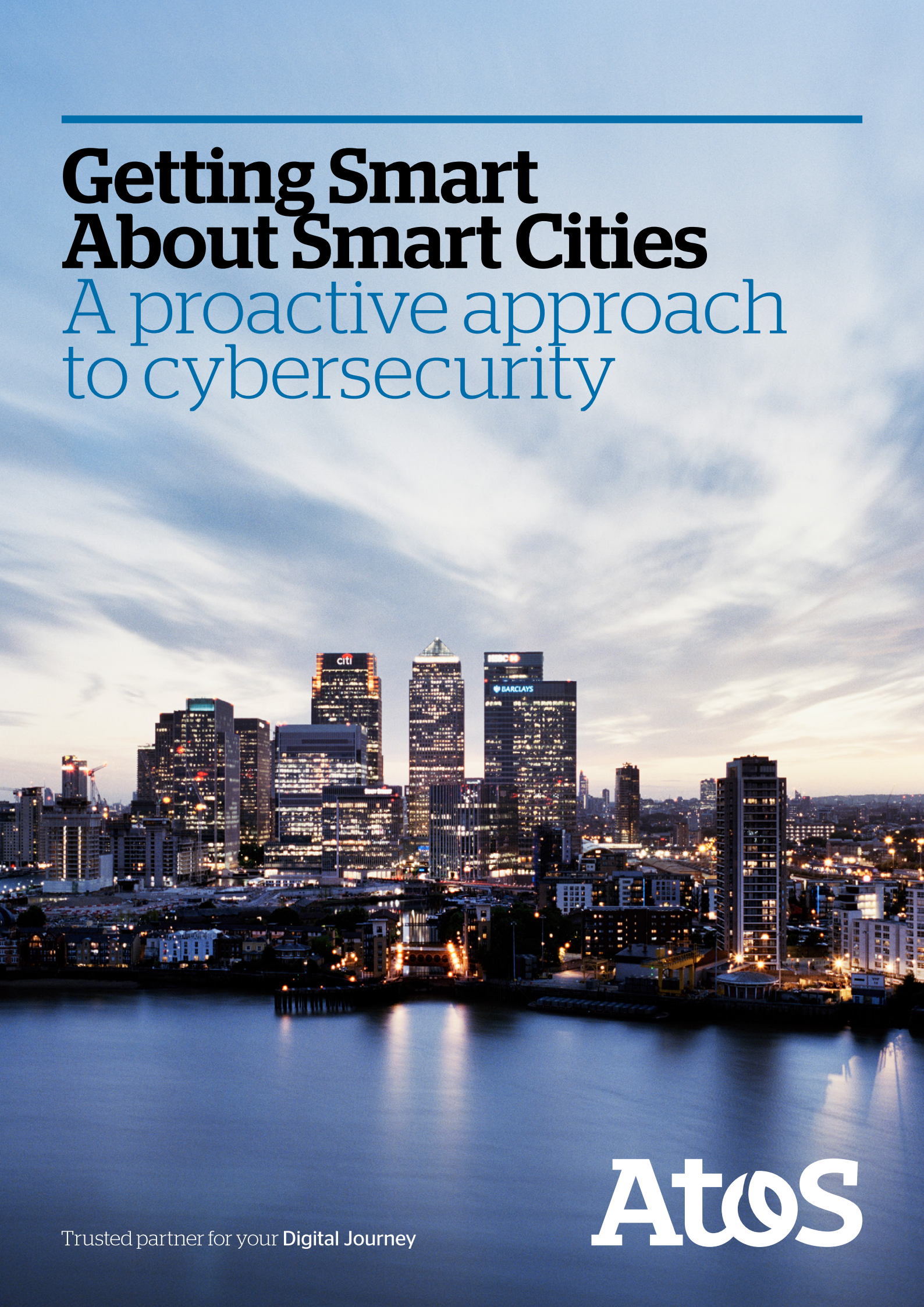
Getting Smart About Smart Cities

A proactive approach to cybersecurity



Trusted partner for your **Digital Journey**

Atos

Introduction

Cities have entered the digital era, and there is every indication this will continue to accelerate. But with the new 'connected citizen' and ongoing digitization of government and society, the risks of data breaches, service disruptions, theft, and loss of intellectual property also rise—and perhaps at an even faster pace than many Smart City leaders realize.

Catastrophic failures to power grids, healthcare facilities, and public safety networks are on the rise. Incidents such as the hacking of the emergency alert system in Dallas, Texas in April 2017, and the ransomware attack on the Atlanta, Georgia municipal government during the spring of 2018 underscore the serious need for city leaders to rethink how they approach risk and cybersecurity.

In March 2018, the Department of Homeland Security reported that since at least March 2016, Russian government cyber actors targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.

The sheer magnitude of the challenge of fortifying an entire city and all its public and private institutions from cyberattack and sophisticated attacks on applications and networks can be overwhelming for city leaders, security professionals say.

"We are not talking about attacks coming from individuals. The larger percentage of attacks are machine-driven and turning computing power against cities," said Robert Masterson, a security consultant with Atos, a leader in digital services, providing consulting and system integration services as well as big data and cybersecurity solutions.

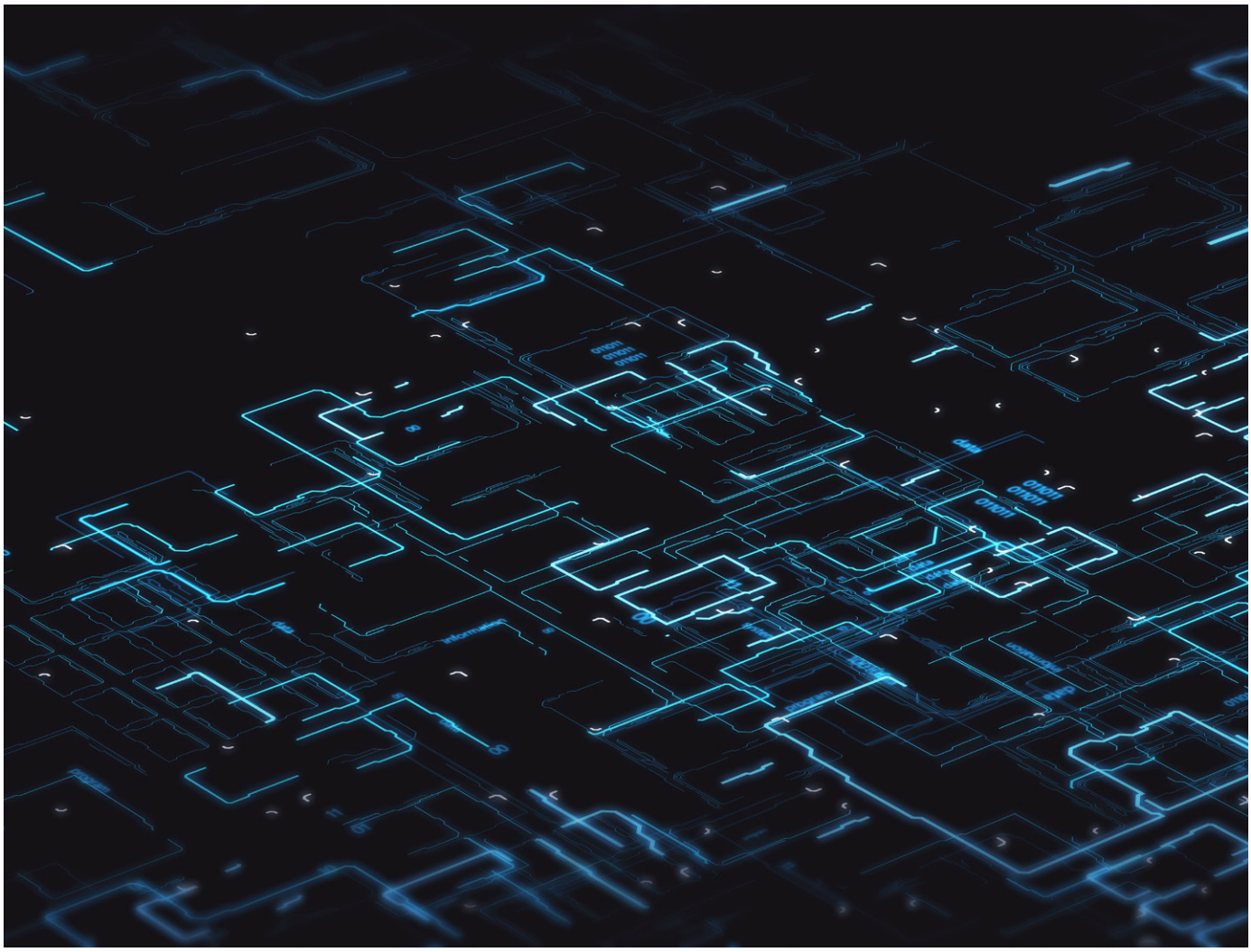
Automated attack techniques are being deployed by hackers, criminal organizations, and nation states on high-value targets such as banks, hospitals, city agencies and infrastructures. The challenge for city leaders and cybersecurity experts is how to manage and mitigate attacks as they expand in volume from five incidents to five million because of the automated mechanism involved, Masterson noted.

Clearly city officials and cybersecurity professionals must take a more proactive approach to solving the problem. The old school concept of siloed security strategies and multiple layers of nonintegrated security products is no longer effective. "You need to be talking about collaborative security among the elements," Masterson said. Atos calls this approach and mindset "prescriptive security." Just as in the medical profession where physicians take preventative measures to address illnesses and problems before they occur, prescriptive security makes changes in a networked environment before incidents occur.

How should smart cities think about cybersecurity?

First, more due diligence and awareness is needed among organizations and citizens over the security implications of the devices they use to connect to networks.

"People are charging ahead with new devices and instantly attaching them to other devices and networks rather than understanding the security implications of what they are doing," said David Storch, a security consultant also with Atos. They are either doing it themselves or it is happening in the background and they don't know. Within organizations there must be a better understanding of cyber hygiene as well as a better understanding of the security implications of often poorly-understood services, such as an online payment system or wireless applications. 'There is unwarranted blind trust in new devices and technologies and too often people rush ahead to implement without doing a proper risk assessment. Also, the days of assuming that you can keep attackers out is dead and has been dead for the last five to 10 years," Storch said. "You have to operate assuming that the attacker is already in." A malicious adversary from anywhere in the world can gain access into the networks of businesses or government agencies in any U.S. city.



Machines must fight for you

Identification and isolation of threats are a key to minimizing the impact of a threat and either stopping the threat or rendering it ineffective. To achieve this goal, several things need to happen:

Baseline normal activity must be established so that when there are deviations from normal, alerts can be raised.

The pattern of activity that could represent a possible threat needs to be identified.

The operational elements that facilitated the threat behavior are limited or stopped in as close to real-time as possible.

By utilizing artificial intelligence, machine learning, and big data, threats that might have been hidden in the past can now be detected. Machine learning is the process of taking in large amounts of information, or big data, churning it and learning from it, and then finding anomalies. The real key is to effectively limit the impact of an attack or threat by providing automation and orchestration of the defenses so that the threat is neutralized as quickly as possible via automated processes.

Security teams must think more about the use of automation and orchestration to get machines and systems fighting for them, Masterson said. "You cannot wait for the human element to kick in to start your defense," he said. The machines are much quicker and artificial intelligence and machine learning are being used to attack organizations' networks, so security teams need to use the same tools for their own defense.

Orchestration is the ability to organize multiple security products into a cohesive holistic system. There needs to be a bilateral communication mechanism between all the defensive elements, such as firewalls, web servers, intrusion prevention systems, and endpoints when an incident is detected—or before. Once the problem is flagged, someone can either act manually or automation can kick in to fix the problem rapidly.

7 tips to ensure smart city security readiness

1
Take a cyber-economic approach — Understand your most vital and high-risk assets, and invest in their protection on a risk-prioritized basis.

2
Design and implement a cyber-threat intelligence strategy to support government-wide strategic decisions and leverage the investments in security.

3
Ensure that all the stakeholders understand the need for robust risk management, strong governance, and accountability.

4
Build security in from the ground up and not as an afterthought.

5
Obtain visibility/depth of field with respect to how the enterprise is enforcing security and reporting non-compliance with the extended security program and all stakeholders.

6
Define and capture in a reference architecture the organization's extended cybersecurity ecosystem, including partners, suppliers, services and business networks.

7
Use forensic data analytics and cyber threat intelligence to analyze and anticipate threats.

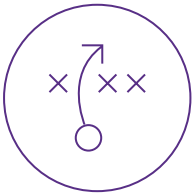
The trend is toward holistic security

It is imperative that security tools and strategies are up-to-date and are as adaptable as the tools being used to compromise the "Smart Solutions" in smart cities. Recent trends in IT security strategies support a shift toward a more orchestrated approach, replacing a siloed approach in which security tools are not integrated.

IT security professionals are using this holistic approach in collaboration with more modern concepts for their defense, which include:

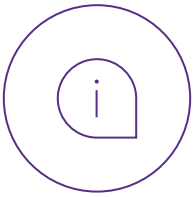
leverage big data
to identify previously difficult to find threats

smart systems utilization
to monitor and coordinate defenses, as well as prodivde a cybersecurity strategy that can maintain integrity of the data and services being provided

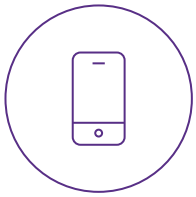


automize and orchestrate
defensive tactics & processes

machine learning



unify information silos
and operational silos



multi-factor identification

zero trust security

A holistic approach to cybersecurity lends itself to a flexible defensive position, combined with frameworks such as COBIT or ISO 27001, that provide core methodologies for governance and security. To provide effective defenses, city leaders will need to continue to invest in four key areas: strategy, technology, process, and people.

All of these investments might not be feasible or cost effective utilizing direct city-wide resources – in those cases city leaders need to recognize the advantages of managed service providers that can provide expertise, experience, and resources that can augment city staff and provide cost benefits to a never-ending race to maintain the safety of the users, information, and services provided by the smart components of a city.

While technology improvements, such as faster hardware, cloud computing, and smarter software in big data analytics and machine learning, will change the types of tools used in cyber-defense, it's the ability to create, integrate, and manage a multi-domain, cybersecurity-enabled architecture that will minimize the impact of the new attacker methods and tools.

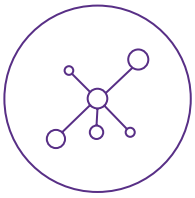
How to become a safe smart city

New initiatives should be constructed with security built in from the ground up, and not added on as an afterthought as too often happens. For already existing infrastructure, city leaders will need to overlay smart technologies to add "Smart Services." These types of infrastructure improvements will generally mean additional monitoring capabilities, improved communication among security personnel and technologies, and the addition of well-understood processes that will limit the risk for abuse or damage.

Three basic steps are required to establish a safety-conscious smart city. They include:

Perform a Comprehensive Risk Assessment.
Identify what is most at risk (what would 'hurt the most' were it to be damaged, stolen, or taken offline) and how to mitigate those risks. This is a cyclical process because security is never perfect – reviews must constantly be performed, updates to existing infrastructure refreshed, and people must be trained— and retrained. A comprehensive risk assessment will provide information about the types of issues that could create a risk, or be a detriment to the user base or the system by abuse, neglect, improper disclosure of information or other methods – and will include what the impact of these changes could have to both the user community and the administrators of the system being implemented.

Develop a Reference Architecture.
A reference architecture will generally provide documentation of accepted best practices, delivery methods for specific technologies, and a common vocabulary that describes the implementation so that all parties involved have a frame of reference for how the final implementation should look, behave, and function.



Establish Threat Modeling.
Threat modeling is the practice of optimizing the security of a given system by identifying the components of the system; identifying, enumerating, and prioritizing a given system and its vulnerabilities; and then defining countermeasures that can prevent or mitigate the effect of threats presented to the system. This practice is becoming a common requirement as it does not require building a solution to model the possible vulnerabilities and define the mitigation methods that would be required to qualify the risk of implementation.

Risk assessments, reference architectures, and threat modeling are necessary tools throughout the lifecycle of a smart solution. However, a well-defined and supported cyber-threat intelligence strategy is also a necessary tool for managing smart solutions. For any complex system such as a city-wide smart solution to be "safe," expertise in this area needs to be assembled and report directly into the city leadership just as emergency management personnel report to city leaders for catastrophe planning — such as earthquakes, fires, flooding, hurricanes, etc.

- Security professionals must be involved at all stages of the lifecycle of the project from initial design to regular audits and risk assessments to monitor and improve security effectiveness

How Atos prescriptive security aids in protecting smart cities

Atos Prescriptive Security, an integrated service, is helping organizations stay ahead of the growing complexity and volume of threats by continually learning and orchestrating automated security actions to resolve current threats and anticipate new ones.

The Atos service combines predictive capabilities with automation powered by supercomputing. Prescriptive security makes changes before incidents occur, anticipating them and shutting down vulnerabilities. Behind the scenes, the Atos service constantly learns from a wide variety of inputs, including threat feeds, network activity and endpoint agents. When these inputs are combined, they provide near real-time changes to the environment such as web and email gateways to avoid breaches and cyberattacks.

The increasingly digitally-connected world of smart cities is no doubt improving the lives of citizens and residents. And the interconnectivity of systems along with automation are helping cities to provide services more efficiently.

However, at the same time, the digital age has opened new complexities and expanded the attack surface that can be exploited by malicious adversaries, who deploy automated techniques to attack targets with greater precision and velocity. Smart cities and security teams need an even smarter, fully-connected architecture woven together into a continuous security fabric, like a nervous system. Within this single global system individual components react like a reflex to not only detect threats but stop them, in many cases, before they can act.

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of € 13 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

Find out more about us
atos.net

Let's start a discussion together

To learn more about Atos' approach to proactive security for smart cities:
https://atos.net/en-na/north-america/local-government-cities

CT_J1564_181024_RY_PAUL_BENDER_B_KEEPINGSMAR