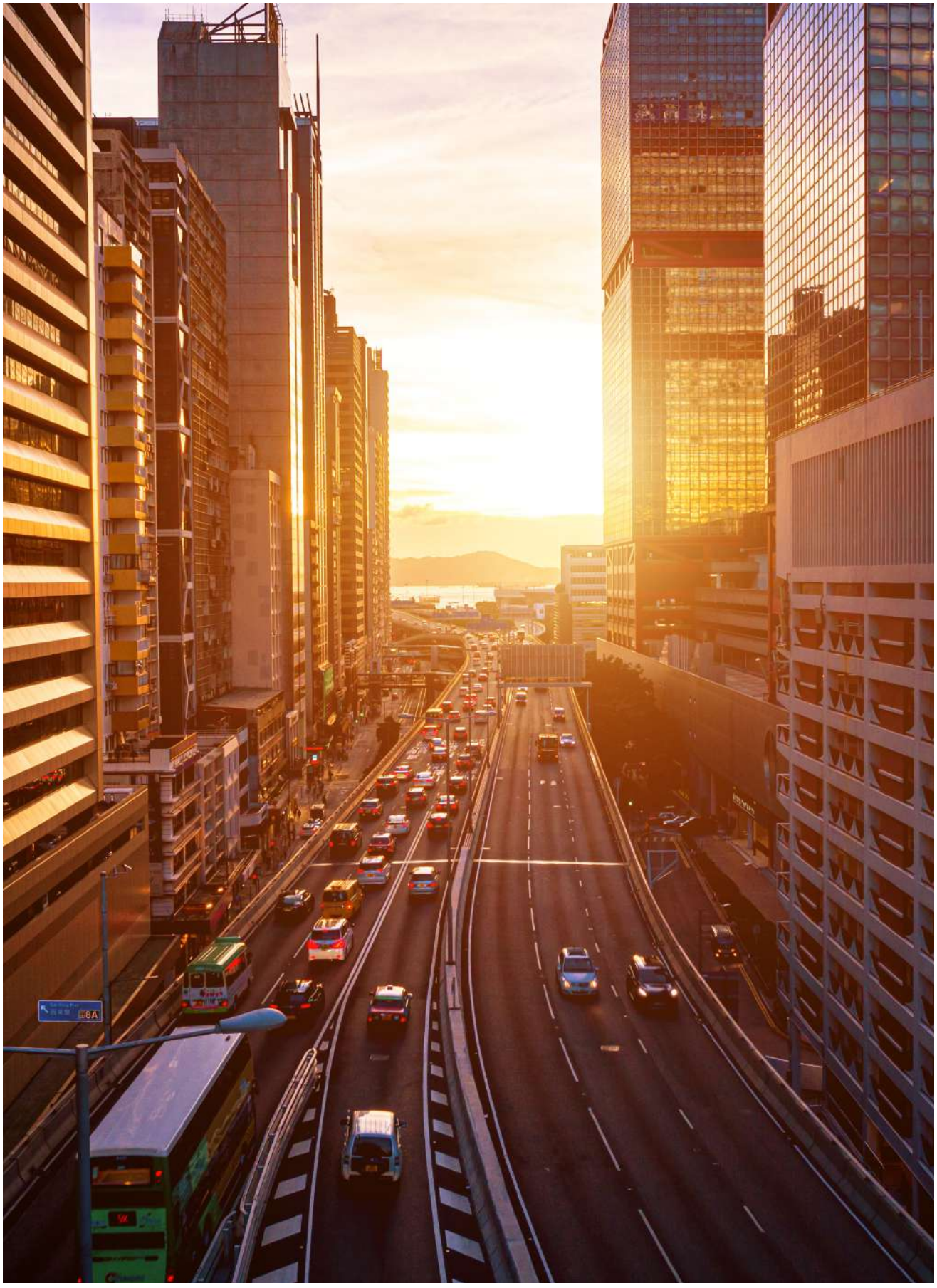
Whitepaper

# Building a successful smart city

## The foundational elements

Genetec™



# Contents

# Executive summary

Cities everywhere are growing at a rapid pace. With that, so are the technologies that public safety agencies use to keep people safe and urban landscapes running smoothly. In fact, the IDC expects smart city technology spending to hit $135 billion by 2023. Another report by Statista suggests that spending on smart city initiatives worldwide will top 189.5 billion by that same time.

Even with all these technological investments, some municipal officials and agencies are still struggling to move public safety and smart city initiatives forward. Their challenges often stem from a few common trends: data overload, demand for transparency, and departmental silos.

As more devices are added to a network, more public safety agencies are inundated with data. Trying to make sense of the information not only slows emergency response but also limits a city's ability to spot issues or patterns and make changes that can positively impact their communities.

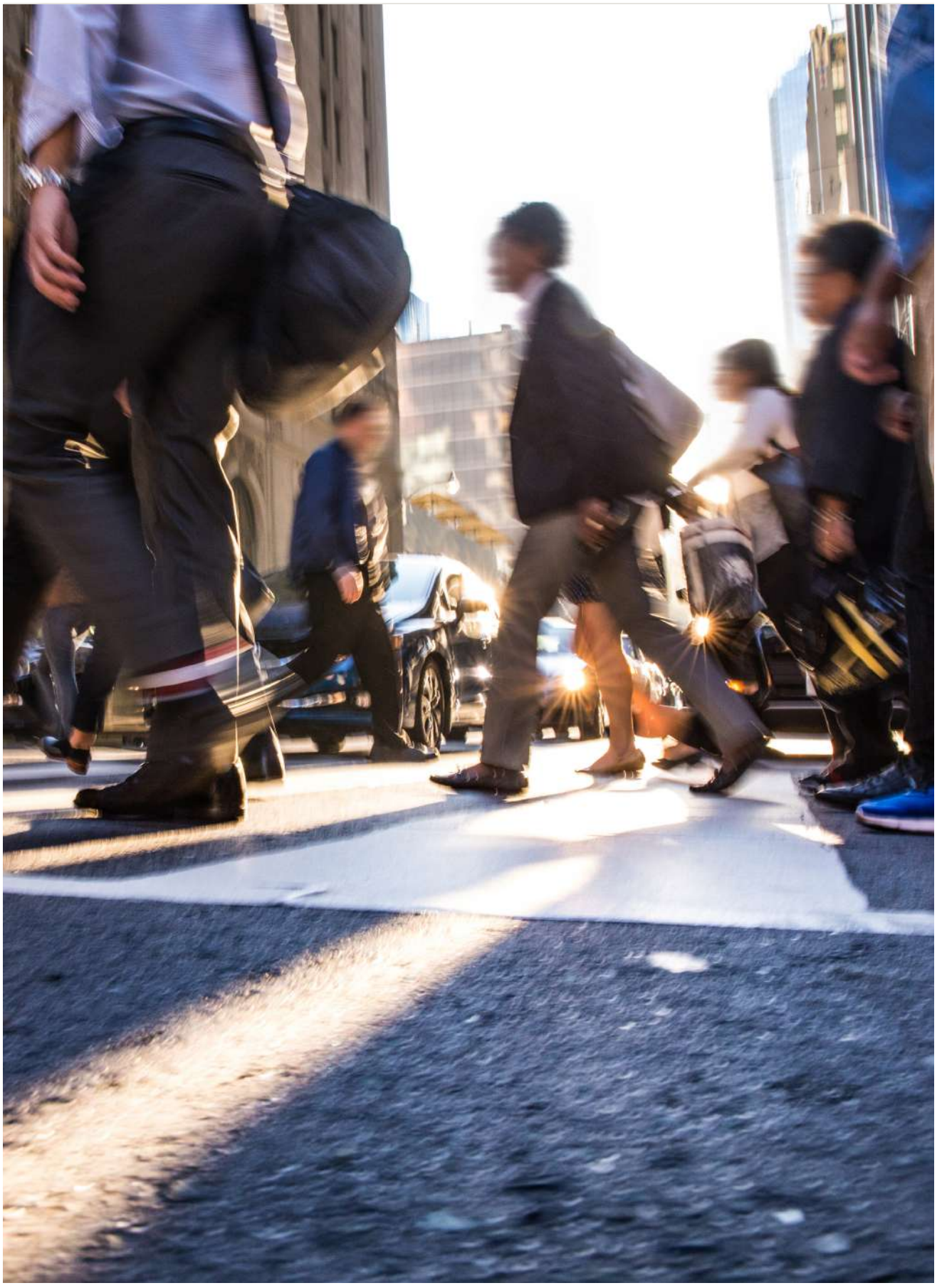
Public apprehension over how and when personal data is being used also creates points of contention for city stakeholders. More now than ever, key decision-makers are being asked to not only prioritize privacy and cybersecurity at all levels of their smart

city framework but also openly engage with the community to address their needs and concerns.

Finally, investments in technologies across the cityscape have traditionally been made by independent departments. This siloed decision-making has kept departments isolated and unable to effectively share information. Yet, when departments from all over the city can come together and collaborate through a shared lens, they are better able to protect and serve all members of their community.

Faced with all these obstacles, how can city stakeholders turn raw data collected from smart city technology into powerful insights and share information across departments, while addressing public concerns head-on? How can they implement a smart city framework that will meet current demands and set them up for smooth future expansions?

This whitepaper discusses three fundamental success criteria that top cities in the world prioritize when building out and evolving their smart city frameworks; these include intelligence, transparency, and collaboration. This paper also outlines critical steps that help cities grow to become smarter and safer as the digital world continues to evolve.



1

# Challenges and trends in public safety today

While many cities around the world have set ambitious goals to become 'smart', this hasn't come without hurdles. Whether a growing urban town or large metropolises, public safety agencies everywhere are facing similar challenges on the road to digitizing and modernizing their urban landscapes. Below are some common challenges and trends that are holding cities back from becoming smarter and safer.

## Challenge #1 – Data-rich and information poor

Most cities have already made significant investments in various technologies to protect their citizens. These might include solutions such as video surveillance, analytics, automatic license plate recognition (ALPR), various traffic sensors, and much more. All this technology generates a massive output of data. In fact, a Cisco Global Cloud Index report stated that a city of only 1 million people produces 50 petabytes (50 million gigabytes) of public safety data daily.

This build-up of data has made it difficult for public safety agencies to organize and truly understand what's happening in their city. For many city stakeholders, piecing information together during an emergency response is challenging; but spotting patterns in information that lead to meaningful improvements in response protocols or city living has become nearly impossible.

While cities might dedicate resources to compiling and analyzing data, it's a monstrous, time-intensive task. This is why more police departments are now realizing the importance of criminal intelligence analysis for better decision-making. According to the Atlas of Surveillance, there are currently over 85 real-time crime centers (RTCCs) in the United States, all leveraging modern technologies to analyze data and make better decisions about response strategy and proactive crime deterrence.

Adding new sensors and collecting more information isn't enough. To better serve communities and make a more meaningful impact, public safety agencies must implement tools that help transform raw data into intelligence that they can act on.

## Challenge #2 – A growing need for transparency

Rising polarization and geopolitical issues are breeding mistrust around the world. While cities have always contended with the 'big brother' label, growing apprehension about how and why governments are using physical security technology is at an all-time high.

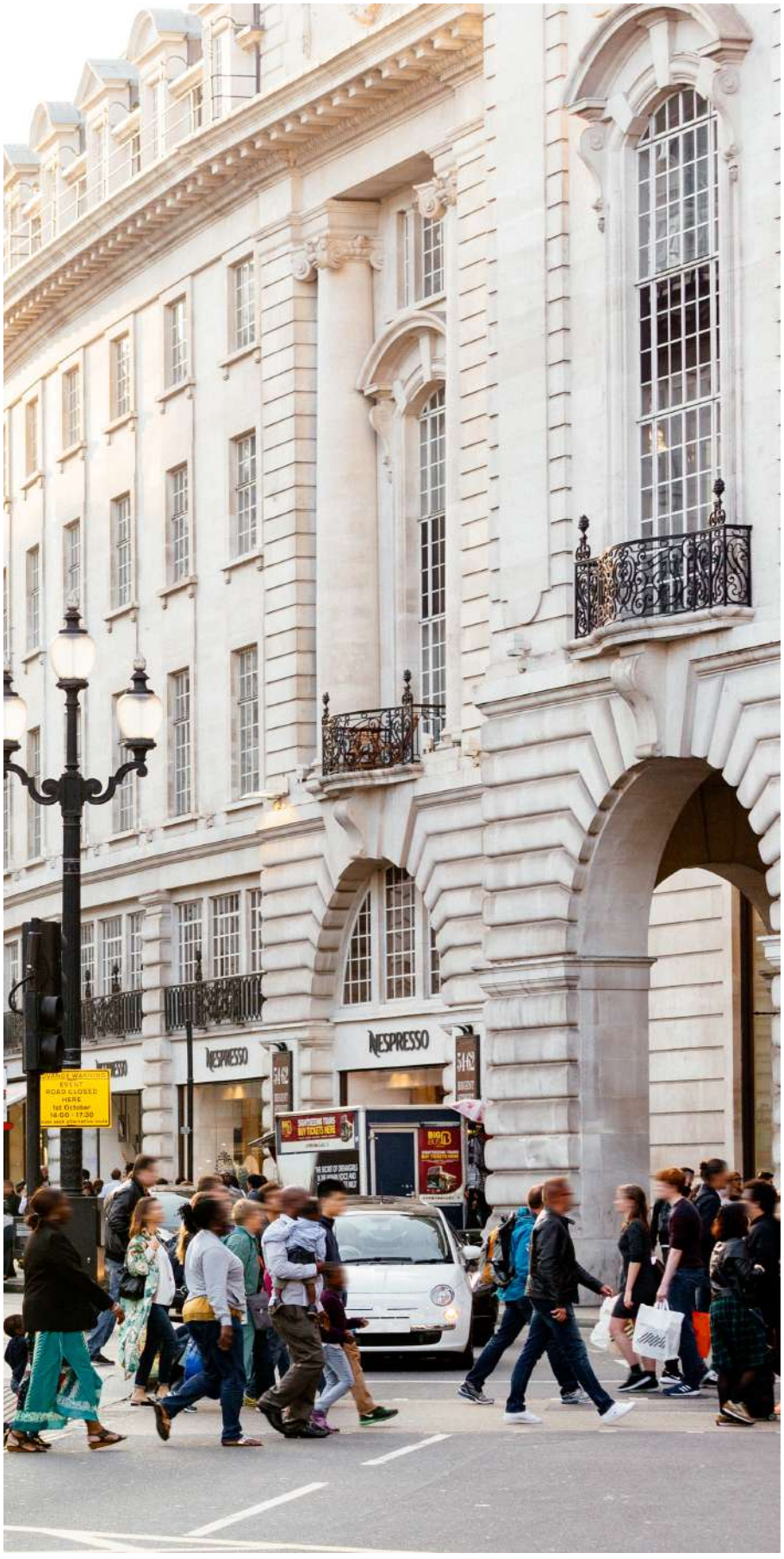
This heightened sensitivity to privacy violation is pressuring public entities and private businesses to enhance data protection. New privacy legislation is also supporting citizens' grievances, mandating that organizations take ownership of how they collect, manage, and share personal information.

Compliance not only involves upholding strict internal privacy protocols but also maintaining a comprehensive cybersecurity strategy too. The issue is that only 33% of cities feel very well prepared for cyber attacks, according to a Smarter Cities 2025 report by ESI ThoughtLab. In many cases, existing technologies can't adapt to emerging threats, and are holding cities back from reaching higher levels of resilience.

Another important aspect in addressing mistrust is ongoing community engagement. Initiatives that offer greater transparency are critical to the smart city movement because they open public discourse and minimize skepticism. These might include informing citizens about data protection protocols before the technology is implemented, regularly sharing statistics on response times to incidents, or hosting open-houses for community members to witness the full-scale RTCC operations.

In a world of increased unrest, protecting privacy and increasing transparency both go a long way in getting more public buy-in and enhancing trust with local residents, businesses, and institutions.

Existing technologies can't adapt to emerging threats and are holding cities back from reaching higher levels of resilience.




While some cities use custom solutions to stitch all existing systems together, ongoing maintenance and compatibility issues stretch budgets and resources to breaking points.

## Challenge #3 – Ineffective department and data siloes

Since legacy technology has been disjointed for so long, city departments have been too. Years later, as more cities recognize the benefits of sharing information within departments and across entities, these antiquated and disconnected technologies are creating major roadblocks.

In many cases, city agencies are forced to manage and extract data from these disparate solutions. During investigations or emergencies, this means they are jumping between various applications and trying to piece information together to make decisions. All of this wastes valuable time and resources, amplifies operator burnout, and slows response to incidents.

Trying to integrate all data from older, stand-alone solutions is a complex and costly task. While some might resort to custom solutions to stitch all existing solutions together, ongoing maintenance and compatibility issues stretch budgets and resources to breaking points. Bigger siloes also exist between various city agencies such as law enforcement, mass transit, traffic management, and other key public entities. That's because, in the past, it was commonplace for these agencies to make independent decisions about the technologies which they use to secure and manage their operations. Yet protecting a city isn't the sole responsibility of a single organization. A city's resilience often depends on the successful connection and interaction of a wide variety of enterprises, including the private business community at large.

To foster these networks of collaboration, cities need to have the right frameworks and technologies in place. When all stakeholders can effectively communicate and share information, cities can unlock better quality responses and develop the strategies necessary to keep urban life safe and vibrant.

2

# What smart cities need today

While technology spending has been steadily increasing over the years to support smart city initiatives around the world, technology alone does not lead to greater efficiencies and community-wide benefits. Public safety, law enforcement, and other city stakeholders must consider how the smart city solutions they currently have will allow them to achieve specific goals and outcomes.

Considering the common challenges facing cities around the world, there's a need to prioritize three key components in the smart city movement: intelligence, transparency, and collaboration. Below, these themes will be explored alongside real-life examples of how cities have achieved incredible results by keeping these smart city pillars in mind.

## Smart city objective #1 - Intelligence

### How can you leverage the data you are sitting on?

There is tremendous value in the data cities are collecting every day. Transforming this data into information that fuels better decision-making across the urban landscape requires the right technology.

Investing in a platform that can consolidate data from multiple sensors and systems around the city is just one part of the equation. There's a more pressing need today to choose technology that can analyze and correlate the vast amount of information being collected and help operators make sense of it all.

### A data-driven view of the city

Many smart cities are investing in decision support systems to empower public safety departments to build a deeper, data-driven understanding of what's happening in their city.

This forward-thinking technology continually examines and connects information from thousands of sensors and data points such as cameras, 911 calls, social media posts, vehicles, weather reports, and other devices and systems around a city. It then displays relevant information through dynamic maps as events unfold. This gives dispatch operators and frontline personnel deeper situational awareness at the right time to coordinate an effective response.

Decision support software can also enable automated responses as soon as activity is detected within an area. For instance, if an analytics system detects a gunshot, notifications are immediately sent to nearby officers and street lights in the area will become brighter.

### Trendspotting over time

The more data that's collected over time, the more intelligence becomes available to cities. With a built-in correlation engine, a decision support solution allows cities to spot trends in the data that can lead to significant operational improvements.

For instance, a city could identify a rise in vehicle thefts in the vicinity of an annual event and start allocating more police resources to the area around that time. Another city could find ways to improve response to certain situations that keep responding frontliners safer. A city might also be able to retrieve a report that shows a drop in crime rates after installing gunshot detection systems in specific hotspots.

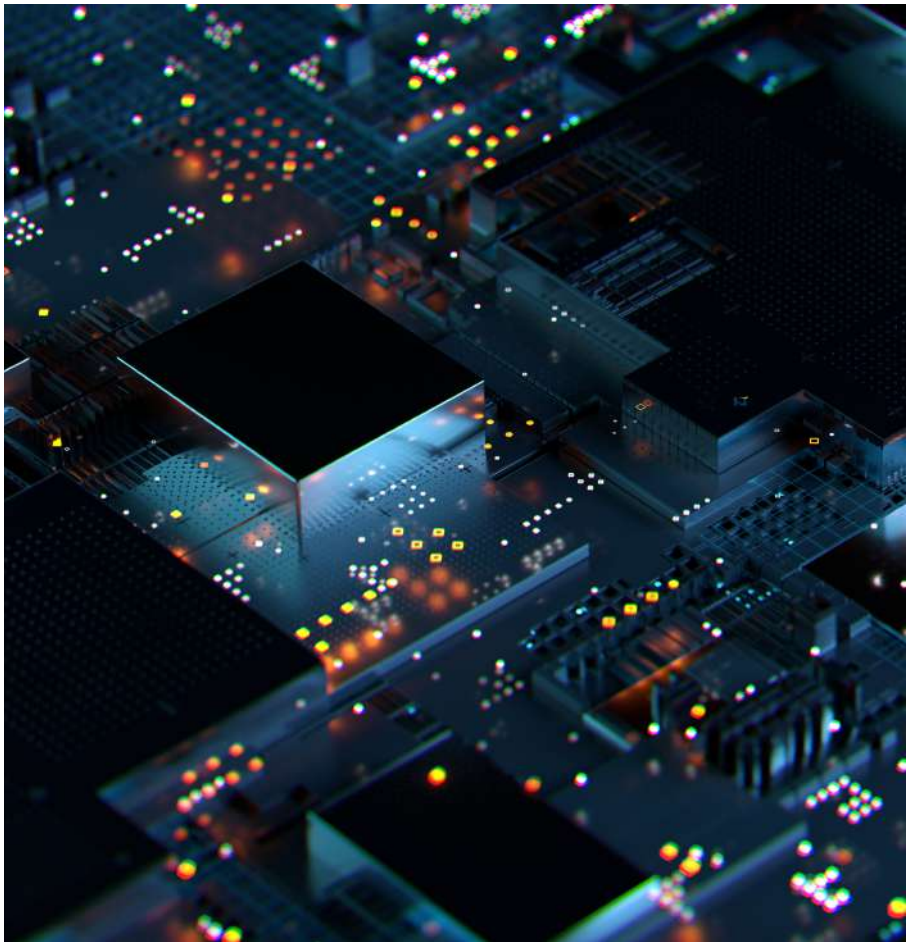
Ultimately, the right technology gives cities intelligence that they can act on. It helps public safety agencies measure the effectiveness of initiatives, understand the progression of incidents, and stay better prepared for all types of events.

## A real-world spotlight on city intelligence

A County Sherriff's Office in Alabama needed a more effective way to manage information from all their public safety systems. Not only did law enforcement want to enhance real-time situational awareness on incidents in progress, but they also wanted to speed up investigations and close cases faster.

To achieve these goals, they decided to invest in a decision support platform that includes a powerful data correlation engine. Today, all information from their computer-aided dispatch (CAD) system, records management system (RMS), video management systems (VMSs), automatic license plate recognition (ALPR) systems, and other sensors across the jurisdiction are now fed back into this centralized platform.

With a common operating picture and intelligence at hand, sheriff deputies have a better understanding of incidents as they unfold. They're also maximizing resources to provide the most effective response and keep their communities safer.



## Smart city objective #2 - Transparency

### How can you make it easier to protect privacy and remain transparent?

Building a smart city doesn't need to come at the expense of citizens' privacy. As more technology is added to the cityscape, it's important to invest in solutions that are built with privacy and cybersecurity in mind from the ground up.

Having built-in data privacy and cybersecurity measures, city agencies are better equipped to use data and technology responsibly. Having the right mechanism in place creates an opportunity to inform and reassure citizens about how their privacy is being respected and protected.

### A solution built with privacy by design

Trust is essential to the continued growth and sustainability of our digital world. And the best way to build trust is to partner with organizations that prioritize data protection and privacy.

Vendors who take responsibility for their role in helping to protect data and privacy offer technology that is built with Privacy by Design. This framework ensures that cybersecurity and privacy protection features are more accessible, and when possible, enabled by default.

These can include varied lines of defense such as encryption, multi-layered authentication, and authorization. They also include tools that offer more proactive threat monitoring, helping agencies stay on top of potential vulnerabilities and critical updates.

Restricting system access and user privileges, dynamically blurring identities in video footage, and automating retention policies further bolster a city's data and privacy protection strategy.

### Getting the community involved

When people don't know how their information is being collected and used, it's understandable that they'd feel apprehensive about security technology. By establishing the right privacy policies and implementing comprehensive data protection strategies, cities are in a better position to have open conversations with citizens and businesses about their concerns.

In many smart cities, there is an opportunity to not only share how, when, and where data is being collected and stored but also showcase how this information is being used to keep people safe and city life vibrant.

After a major US city implemented a decision support system, shootings were down 22% in the two most at-risk districts.

## A real-world spotlight on transparency

A major city in the US sought to enhance operations in six police districts. The goal was to reduce response time for reported shootings and crime in these areas. At the time, operators were working with many disparate solutions including a CAD system, 911 calls from residents, gunshot detection sensors, and other technologies.

To bring all this information together, the department invested in a decision support system. This provided a unified view to all dispatchers and responders, helping them respond more efficiently.

Following the implementation, the city announced that response times from dispatch to on-scene arrival time had been reduced by 39% and 24% respectively, in their two most at-risk districts. They also shared that shootings were down 22% in these districts.

As a result, public support and buy-in to expand the use of these technologies grew significantly. Today, the city continues to openly showcase results with their communities, sending a strong message that crime and gun violence get a swift response.

## Smart city objective #3 - Collaboration

### How can you enhance collaboration and automate procedures?

Technology isn't a magic solution that can stop crime before it happens; and it certainly can't replace the knowledge, instinct, and experience of frontline personnel.

That said, crime-fighting technologies can enhance these strengths by delivering actionable data and enhancing inter-agency collaboration. This technology gives city agencies a better understanding of their environment, allowing them to shave valuable seconds off response times and determine when, where, and how to best deploy their resources.

### Keeping everyone on the same page

Forward-thinking cities understand that bringing multiple data sources together into a single pane of glass is the key to enhancing collaboration, improving response time to incidents, and ultimately—keeping cities safer. For this reason, more smart cities want technologies that unify information into a shared view.

During a large city event, law enforcement, transport agencies, traffic management personnel, and first responders can all work together and stay on the same page to keep everything running smoothly and people safe. Should an incident occur, agencies will be able to access the same timely information and coordinate the safest and most efficient response.

Specifying system privileges and access rights ensures only authorized city departments and personnel have access to the information they need.

Even during investigations, collaborative technologies allow police officers to close cases faster and share evidence with authorized individuals such as the district attorney's office. This happens through a digital evidence management system that allows users to securely upload reports, interviews, video evidence, and all other case information into a centralized repository from any location.

Not only does this save them tremendous amounts of time, but they can also keep evidence protected and easily accessible as the investigation continues.

### Community outreach made simple

Public-private collaboration and community participation are key components for developing an effective smart city. In a city environment, many large and small public and private enterprises have their own physical security systems. When law enforcement

can securely access video footage or other data from privately-owned systems, they can become more efficient at responding to incidents and closing cases.

Many cities today are enabling this connection using compatible cloud services. Incentivizing participants can include installing a free camera outside their business in exchange for on-demand access to the video footage when a crime is reported in the area. Businesses commit to paying an affordable monthly subscription to access their video surveillance system and benefit from a safer community in return.

## A real-world spotlight on collaboration

A big city in the US knew technology was a force-multiplier that could help their officers drive crime rates down, but the cost of implementing a city-wide system was a major roadblock. They needed to find a way to keep expanding surveillance coverage without going over budget.

The city invested in a unified security platform and brought all disparate security systems from their agencies into one solution. This enhanced real-time situational awareness and offered additional support to officers in the field.

Today, the city has access to over 500+ cameras, but the law enforcement department only owns and maintains about 60 of those cameras. That's because many private businesses have agreed to share video feeds with the police department, giving officers enhanced city-wide visibility without any additional spend. They also have 40+ automatic license plate cameras which have all been procured in cooperation with the private sector, offering even greater cost savings.

To keep expanding its footprint, the city also created a community outreach program. Law enforcement invited local businesses to implement security solutions that would connect back to their RTCC. After an initial pilot project, the community was excited to get involved because they saw the goal of a comprehensive security plan.

3

# What can you do to build a safer and smarter city of the future?

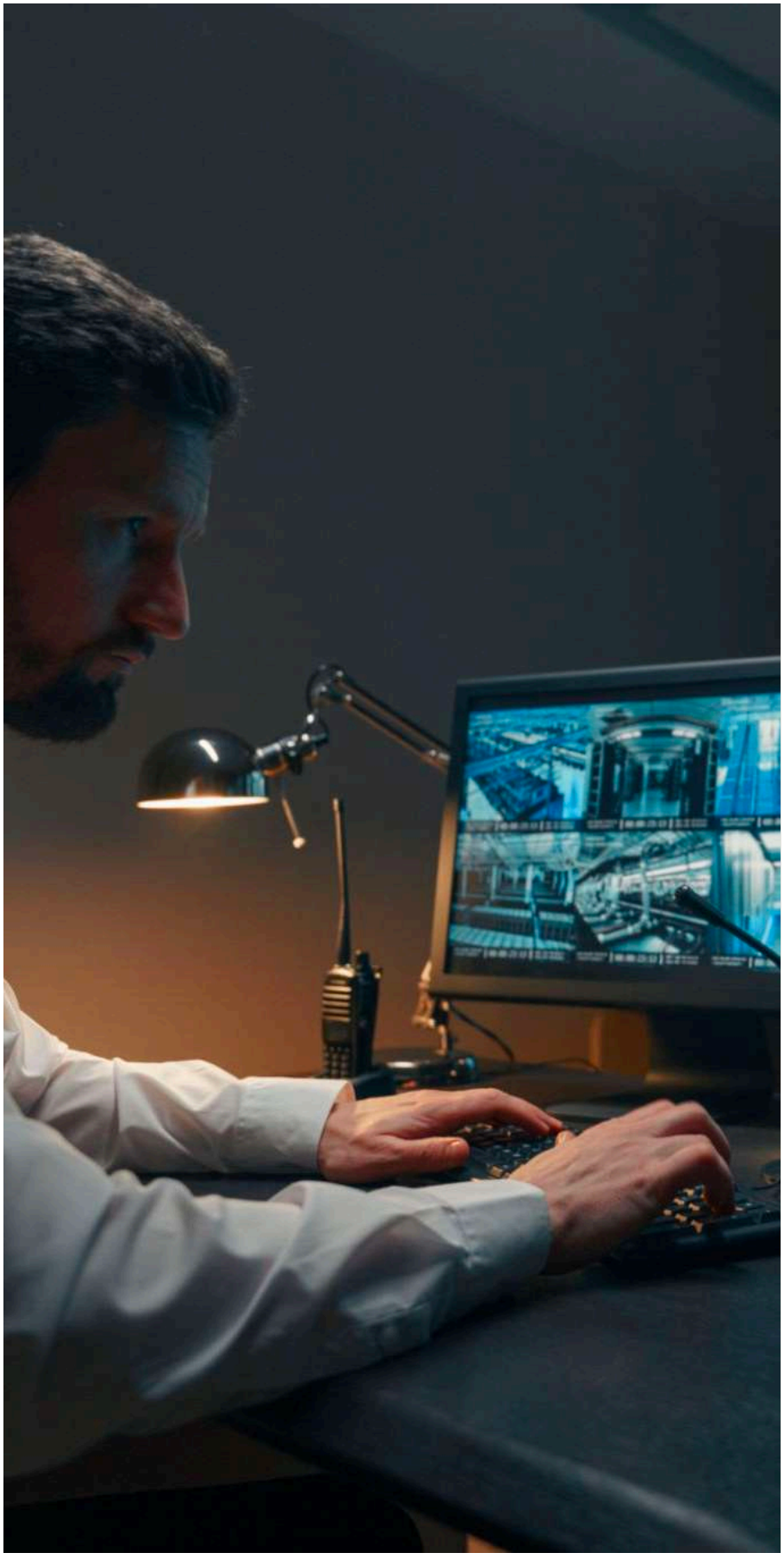
## Step 1 – Identify your goals

The piecemeal approach to building a smart city has long failed city officials. To enact an effective framework for a safer city, it's important to bring all stakeholders (law enforcement, transit agencies, public safety teams, traffic departments, IT leaders, city planners, etc.) to the table to discuss immediate concerns and identify long-term objectives.

The discussion should also weigh the opinions of citizens and businesses to better align with community priorities and get more buy-in. This not only creates more sustainable value but allows decision-makers to become more strategic about technology investments and implement solutions that will lead to positive outcomes.

Planning a phased project roadmap helps to prioritize foundational elements while offering the flexibility to make continual improvements and adapt to new requirements as city life evolves.

A standard security operations center has 20+ systems of which 70% of activities are common. A unified security platform makes it easier for operators to do their job more effectively.



## Step 2 – Set up a strong technological foundation

Having the right foundational technologies in place is imperative to building a resilient smart city.

At this stage, considering everything from network and IT infrastructures, cloud services, fixed and mobile broadband, and even the very platform from which agencies will manage video surveillance, analytics, ALPR, and other security technologies and sensors is vital. This architecture or backbone of technologies can either facilitate and optimize new cutting-edge city initiatives or hold cities back.

Part of the digital transformation plan must also include considerations for systems that are open, modular, and scalable. By prioritizing these criteria, city stakeholders will have the freedom and flexibility to build layers of innovation, choose best-of-breed solutions, and capitalize on new technologies as they emerge.

Finally, partnering with solutions vendors that prioritize cybersecurity and privacy is a must. It's the first step in ensuring cities can reach the highest levels of protection against evolving cyber threats.

> Openly sharing the steps city stakeholders are taking to protect and secure information help to appease public concerns and establish higher levels of trust.

## Step 3 – Unify your operations under one platform

A standard security operations center has 20+ systems of which 70% of activities are common. Bringing all systems together within a unified security platform makes it easier for operators to understand what's happening and do their job more effectively.

Cities can start by combining video surveillance and analytics with the platform, and then gradually add other systems such as ALPR, access control, gunshot detection, decision support, evidence management, traffic sensors, and so much more.

Working from one central map-based dashboard gives operators all the information they need in real-time. Since all core functions and workflows remain the same across all systems, they'll be able to resolve any situation confidently and quickly.

Having a single platform also streamlines upgrades and maintenance. This demands fewer resources and minimizes operational costs as the years roll on.

## Step 4 – Implement data security protocols and offer transparency

Determining how to best protect data and privacy must happen before smart city technologies go live. City agencies must come together to map out a data protection strategy and leverage the right tools and technologies to ensure compliance across all departments and operations.

A solution built with Privacy by Design helps city stakeholders gain complete control over the data they collect, handle, and share. Relying on trusted technology vendors and smart city experts can also bolster data protection methods, ensuring all possible lines of defense are optimized and systems are hardened.

Informing the public about how data is collected and used by city agencies is the critical final step. Openly sharing the steps city stakeholders are taking to protect and secure information help to appease public concerns and establish higher levels of trust.

## Step 5 – Share information across entities and leverage data for better insights

Cross-agency collaboration is essential for a more proactive approach to public safety and emergency response. With the right backbone of technologies in place, cities can centralize operations and allow agencies to tap into the systems and information they need.

True collaboration offers a bird's-eye view of what's happening across the smart city. City officials, law enforcement, and department managers can then use that collective data to gain deeper insights into their operations and identify opportunities to better serve their community.

Cities can take collaborative efforts further by fostering connections with private businesses and other public institutions. From restaurants and retailers to schools and hospitals, all types of organizations can work with law enforcement to expand surveillance coverage and play an integral role in moving a smart city forward.

## Step 6 – Plan for future expansions and operational gains

A smart city depends on its ability to evolve and adapt. City leaders should always be thinking about what's next, but what's possible comes down to the technology they choose. Investing in scalable and open technologies allows agencies to embrace the latest innovations and remain at the cutting-edge of the smart city movement.

This includes broadening applications beyond public safety and looking at ways to capitalize on security data to improve city operations, flow, and liveability.

For example, a city could learn why traffic backs up on certain streets at specific times or confirm that a pothole has been fixed. Another city might track illegal dumping at known spots and identify patterns in parking and ride-sharing data to inform future city requirements.

Regularly reviewing objectives with all city stakeholders ensures strategic progress and maximizes existing technology investments for even bigger returns.

## Step 7 – Re-assess and revise your plans, policies, and procedures

In the smart city environment, there is no such thing as 'set it and forget it'. The very nature of bringing multiple systems together and aggregating information from many sources requires constant engagement and frequent re-evaluation of practices.

As time goes on, it's important for city stakeholders to review objectives and make sure system configurations, operating procedures, and overall policies best reflect and support forward-moving progress.

Prioritizing change management is critical in the advancement of smart initiatives. Not only does this allow cities to quickly address key issues, optimize technological performance, and seize new opportunities, but it also ensures higher levels of resilience as social and digital trends continue to evolve in big ways.

4

# Investing in the right partnerships

According to the Worldwide Smart Cities Spending Guide by the International Data Corporation (IDC), up to 30% of smart city internet-of-things (IoT) projects are going to fail because of poorly organized frameworks for effectively deploying new technologies.

As the urban landscape becomes increasingly digitized and data-centric, cities must set clear objectives that prioritize intelligence, transparency, and collaboration. With these key success elements in mind, stakeholders will be able to acquire the most effective technologies to move their smart city initiatives forward.

Decision-makers should also understand that smart cities aren't built alone. Developing strategic partnerships right from the start with trusted experts such as consultants, system integrators, and technology vendors will streamline the process and ensure higher levels of success.

With forward-thinking technology and strong partnerships, local governments can keep building more resilient, informed, and efficient cities – ones where all community members feel safe and are proud to call home.

**Established in 1997, Genetec is the global leader in unified security platforms, with a broad offering across a range of security specialties.**

**Operational decision support:** Create efficiency for incident handling and decision making with advanced workflows that guide operators from situation alerts through policy-based procedures to detailed case compilation export.

**Investigative case management:** Simplify case management and speed up investigations with a platform that allows you to centralize digital evidence and securely collaborate with investigators, outside agencies, and the public.

**Cloud services:** Extend the capabilities of your on-premises security system and reduce IT costs with highly scalable, on-demand cloud services that allow your city to easily cope with rapidly changing security requirements and operate with greater efficiency.

**Automatic license plate recognition:** Automate the detection of vehicles of interest, increase parking enforcement efficiency and accelerate public safety investigations through the ability to share license plate data with selected agencies and partner organizations, without forfeiting ownership and privacy.

**Video surveillance:** Achieve greater situational awareness and enhance security within your city with the ability to share cameras across agencies and organizations, providing a common operational picture and improving incident response time.

**Access control:** Heighten your organization's security, effectively respond to threats, and make clearer and timelier decisions with a unified, IP-ready platform, whether deploying a new access control system or updating an existing installation.

**About Genetec**

Genetec Inc. is a technology company that offers on-premises and cloud-based solutions encompassing security, intelligence, and operations. The company's flagship product, Genetec™ Security Center, is a physical security platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security in the communities in which we live.

For more information about Genetec, visit **www.genetec.com**

**About Insight**

Today, every business is a technology business. Insight Enterprises Inc. empowers organizations of all sizes with Insight Intelligent Technology Solutions™ and services to maximize the business value of IT. As a Fortune 500-ranked global provider of Digital Innovation, Cloud + Data Center Transformation, and Connected Workforce solutions and services, we help clients successfully manage their IT today while transforming for tomorrow. From IT strategy and design to implementation, management, and supply chain optimization, our 11,000 teammates help clients innovate and optimize their operations to run business smarter.

Discover more at **www.insight.com**

**Genetec Inc.**
genetec.com/locations
info@genetec.com
@genetec



UPDATED:30-SEP-21