Deloitte.
Insights

A report by the Deloitte
Center for Government Insights

Move faster, safer, and more privately with smart security

A new vision of citizen-controlled security for the digital era

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Deloitte offers national security consulting and advisory services to clients across the Department of Homeland Security, the Department of Justice, and the intelligence community. From cyber and logistics to data visualization and mission analytics, personnel, and finance, we bring insights from our client experience and research to drive bold and lasting results in the national security and intelligence sector. People, ideas, technology, and outcomes—all designed for impact. Read more about our National Security services here.

Contents

KEY FINDINGS

- Today's checkpoint-based security seemingly forces us to choose between security, ease of experience, and privacy. Smart, continuous security offers a new approach to security that can give all three.

- Managing diverse sets of data and finding ways to allow citizens to exercise effective control over their data remain significant challenges.

- However, successes such as the shift to continuous evaluation in security clearances show that a smart, continuous security approach is possible and can deliver the benefits we all want.

- Going forward, consolidation is likely as fintechs seek more traction in an increasingly competitive market and financial institutions (FIs) look for more sophisticated partners.

The value of exhaust

WITH EVERY BREATH, on average we exhale 20 milliliters of carbon dioxide.[1] Now imagine that every molecule of that carbon dioxide was as valuable as gold. We might imagine companies designing complex vacuum machines hovering near each of us to capture our valuable exhalations. That seems like an absurd vision—until we consider the digital world.

Every moment, we are "exhaling" huge volumes of digital data. Across the world, there are 2.5 million internet searches, 16 million text messages, and 18 million requests for weather forecasts every minute.[2] What is significant about these statistics is that our digital exhaust can reveal a lot about us: An internet search can reveal what we want to buy; a text message, who we know; and a weather forecast, where we want to go on vacation. All that data is immensely valuable to those who want to sell us vacations or goods or services.

What if instead of losing all that digital data, we were able to retain control of it and determine what we wanted to use it for? Citizens could use that data to move more quickly through airport security or ship goods more easily. That is the vision of smart security: improved user experience and uncompromised security that still respect the digital ownership of citizens. Such a vision does require significant advancements in privacy, technology, and even the culture of security organizations. Yet as the world moves faster, we need such new approaches to security more than ever.

An internet search can reveal what we want to buy; a text message, who we know; and a weather forecast, where we want to go on vacation.

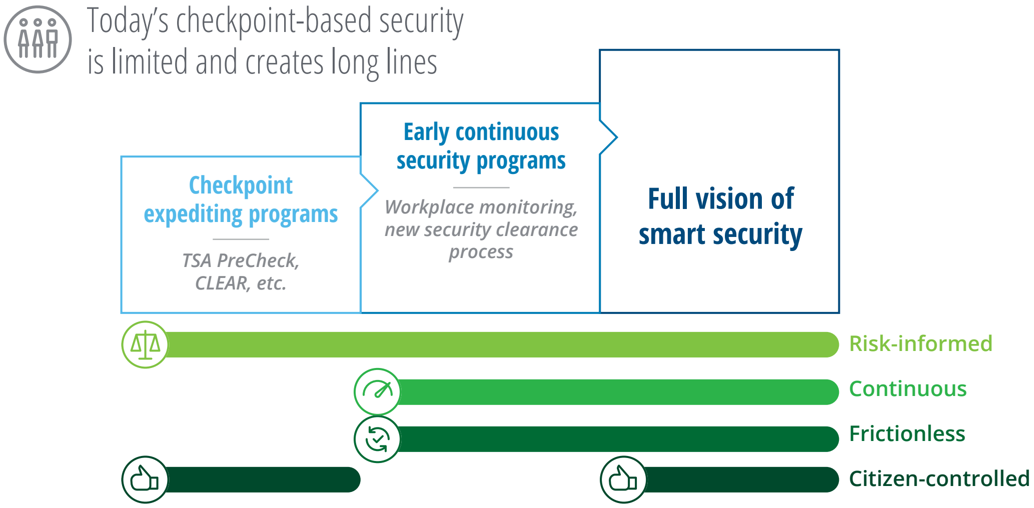
A new vision for keeping the world safe

TECHNOLOGICAL ADVANCEMENTS HAVE enabled a greater flow of people, goods, and information around the globe, while also promising even-greater movement in the future. However, this also means that more items must be tracked or inspected to ensure the security of physical public spaces, which has become increasingly important. Even when just focusing domestically, the sheer volume of goods or people to be screened can strain existing security measures, causing backlogs and delays. This can force citizens and security organizations into a perceived trade-off, either accepting less security for improved user experience, or sacrificing user experience in the name of improved security. That perceived trade-off poses a challenge: how to balance the need for security with the desire for an easy and rapid experience—all while respecting individual privacy.

Today, there are already a handful of small efforts that propose to break that trade-off, but they lack the scope or scale of a full vision of smart security (figure 1). Programs such as TSA PreCheck and CLEAR offer a risk-informed way to improve the experience of aviation passengers without compromising security,[3] but they still rely heavily on checkpoint-based screening. On the other hand, programs such as continuous monitoring in workplaces or continuous evaluation of security clearance holders come closer to encompassing the vision of smart security, but only do so for a very small fraction of users. Both efforts reflect the need to improve security practices, but they fall short of the promise that smart security holds for security professionals and users.

FIGURE 1

Examples of aspects of smart security exist today, but only at limited scope and scale


Today's checkpoint-based security is limited and creates long lines
Checkpoint expediting programs
TSA PreCheck, CLEAR, etc.
Early continuous security programs
Workplace monitoring, new security clearance process
Full vision of smart security
Risk-informed
Continuous
Frictionless
Citizen-controlled

Source: Deloitte analysis.

Smart security is ...

IF CURRENT ATTEMPTS at breaking the security-experience-privacy trade-off all fall short, it begs the question of what smart security is. To fully break the trade-off, smart security needs to be four things: **continuous**, **risk-informed**, **frictionless**, and **citizen-controlled**.

Continuous

WHAT IS THIS?

One of the main features of today's checkpoint-based approach to security is that security is largely enforced just at the checkpoint. That is partly how we get so many long lines and backlogs today. The first step toward smart security is to move from enforcing security at one point in space and time to a continuous process. Continuous security would draw on three categories of data:

- **Enduring data** such as a digital ID or biometrics
- **Pre-event data** such as shipping invoices, a person's travel history, or how an airline ticket was purchased
- **In-situ data** from screening and detection equipment throughout a protected space

By pairing these data sources with risk-informed interventions, security can be moved away from the checkpoint, expanding the secure perimeter all the way from curb to runway. And, importantly for passengers, it can do this all while allowing faster movement of goods and people.

WHERE IS THIS BEING USED TODAY?

One of the largest lines for a security "checkpoint" is the waiting list for US government security clearances. The yearlong investigation process often leaves the US government stuck with massive backlogs, which peaked at 725,000 in 2018.[4]

The security clearance process is now undergoing several major transformations, one of which is an increased focus on continuous evaluation. In place of intensive background investigations before granting access to users, the government now offers expedited checks paired with ongoing monitoring of the clearance holder. Continuous evaluation uses automated checks of work, financial, and other data to look for risky anomalies that warrant further investigation.

The results of this new approach to security clearances have been significant. In under two years, the backlog of clearances has dropped from the all-time high of 725,000 to a steady state of 200,000[5]—all while saving billions of dollars and without compromising security.[6]

Risk-informed

WHAT IS THIS?

A smart approach will simply lead to overload unless paired with a risk-informed approach to security. Not everything needs attention, everywhere at every moment. Rather, by continuously monitoring for unusual, anomalous, and risky events, security professionals can address an issue with the right level of intervention to keep things moving and secure.

WHERE IS THIS BEING USED TODAY?

Risk-informed continuous monitoring is a valuable tool for many companies looking to protect against both cyberattacks and insider threats. In today's digital world, an errant mouse click by an employee on the wrong link can infest sensitive systems with a virus or ransomware, while thousands of pages of proprietary information can be sent instantly across the globe. To help protect employees and guard against these types of losses, many companies are beginning to monitor how employees use company tools and computer systems. When an employee downloads large volumes of data or clicks on insecure links, the system generates a risk score that can help determine if an intervention is needed or if an action is just typical business.

Risk-informed continuous monitoring is a valuable tool for many companies looking to protect against both cyberattacks and insider threats.

Frictionless

WHAT IS THIS?

Improving user experience at public spaces ranging from stadiums to airports to land borders requires a frictionless design. Rather than imposing barriers in the forms of gates or checkpoints, smart security aims to validate users and their activities naturally and nonintrusively. The result? A frictionless experience where most users can walk right to their seats in a stadium or into an airport terminal.

WHERE IS THIS BEING USED TODAY?

You might notice that your bank's website asks you to enter a one-time passcode if it detects that you are accessing the site from a different computer; or that it requires biometric authentication if you try to modify your contact information or initiate a large external transfer. These simple examples of step-up authentication are part of a common strategy followed by many financial institutions to mitigate transaction risk by continuously evaluating patterns of use. When those patterns shift to suggest a risky activity, authentication can step up as needed to make sure the activity is valid.

The technology to implement this strategy is powered by an ability to process, connect, and interpret vast amounts of data on users' actions and behavioral patterns. An example is mouse-movement and click-behavior sensing technology, which can passively collect these behavioral biometrics over approximately 10 minutes of continuous user interaction with a website and generate a remarkably accurate signature that can be compared against future activity to help identify if another person or a bot is attempting to access your account.

Citizen-controlled

WHAT IS THIS?

Breaking the perceived trade-off between user experience and security is fantastic, but only if it does so in a way that respects society's values on privacy and individual autonomy.

WHERE IS THIS BEING USED TODAY?

Unfortunately, perhaps the most well-known example today is the lack of citizen control as seen in state-sponsored surveillance. These undesirable applications of technology help illustrate what smart security cannot and should not be. For example, residents at some apartment buildings in China had no choice but to use facial recognition to access their homes, recording who came in and out at what times.[7] Technology should not be imposed on individuals without allowing them to control when or how their data is used. Rather, smart security must allow residents to decide for themselves how their data is used and what they receive in return.[8]

People recognize the value of their data and are often willing to trade that data for personal benefit. A survey of 10,000 consumers and 1,000 businesses across 21 countries found that 90 percent of consumer respondents are aware that businesses collect their personal data, and 70 percent responded that they'd be willing to give up more information for additional convenience.[9] Presenting users with that choice in a natural and informed manner is key to the success of smart security. At its simplest, citizen control will give users an informed choice between trading some level of privacy for faster transit or other benefits. In more complicated forms, it can help answer questions about how much data is retained about a person, by what agencies, and when it is deleted.

What makes smart security smart?

DEVELOPING A SYSTEM that is continuous, risk-informed, frictionless, and citizen-controlled requires a number of different tools and infrastructure. A smart security system is built with several ingredients.

Variety of detection technologies

Smart security does not rely on one technology but instead uses a broad array of active and passive vetting and authentication methods. Rather than a single checkpoint security screening, enduring and pre-event data such as type of ticket purchased or length of stay can be combined with detection technologies spread throughout a space. These technologies can include everything from small radars that can detect concealed weapons in a crowd to chemical detectors that can find hidden explosives in real time or even biosecurity screeners that can detect individuals with fevers, all at ranges that allow for the free flow of people and goods. Collating data from all of these sources can be used in a continuous security assessment even as people and goods move through a space naturally. These technologies sound like science fiction, but many are already being deployed today at major conferences, sports stadiums, and universities.[10]

Smart security does not rely on one technology but instead uses a broad array of active and passive vetting and authentication methods.

Digital identity

To assess risk, smart security needs to be able to collate different pieces of information from the physical and digital worlds into a single digital identifier for a person or object. Examples range from something as simple as a package's tracking number to a more robust identifier such as a digital passport for an individual.

User control of data

Smart security is built on ideals of consent, transparency, and law, but it also requires personal information. Effective self-sovereignty of data requires advancements in user interfaces that provide an intuitive, interactive tool so users can easily understand when and how their data is being used and also what they can do to influence the use of their data. An analogy could be a credit-monitoring service, but for personal data rather than personal credit. The current standard of 100-page terms and conditions simply will not provide truly informed consent and control to users.

What could smart security look like in the future?

SMART SECURITY COULD be used in different ways in different spheres, as we see below.

Aviation security

Perhaps no single location is as associated with security checkpoints as airports. These days, travelers must arrive at the airport hours before their flight to go through airport security, which typically consists of a physical security screening process. The result is slow screening that results in delays for passengers, lost revenue for airports—with roughly US$1 million in lost sales in airport stores for every 10 minutes spent in security[11]—and incomplete security processes.

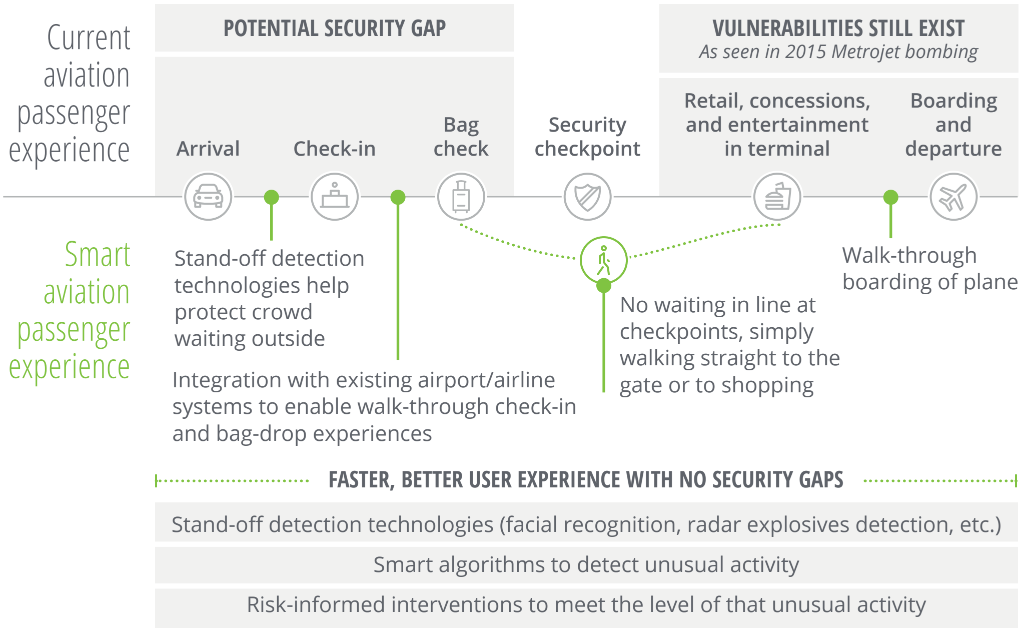
SMART SECURITY SCENARIO

Tony is a frequent traveler who appreciates the need for airport security while also understanding that technology can be leveraged to improve security and his experience at the airport. For these reasons, Tony is a member of a smart security program. By signing up for the program, Tony has given his informed consent for the program to access some of his user data already being captured by commercial companies via his smartphone or computer. In the same way a retailer might use Tony's smartphone data to better understand the products Tony might like to buy, smart security uses the same data to understand what level of security protocols Tony must go through when at the airport or other venues (such as a sports stadium) where security is important. So how does it work?

From the minute Tony purchases a plane ticket, the smart security program begins analyzing Tony's data to better understand what risks, if any, he may pose (figure 2). Even before Tony arrives at the airport, the airport's security team knows when he's expected to arrive and, based on his data, what risk profile Tony deserves. When Tony arrives at the airport, facial recognition confirms his identity and allows him to drop his bags with the airline without scanning an ID or waiting in line. As Tony moves through the airport, stand-off sensors including radar, thermal, and chemical detectors check for hidden weapons or explosives, offering even more security than current sensors locked into fixed checkpoints. These new sensors operate at significant ranges and in crowds, allowing Tony and other passengers who have opted into the program to move quickly to the gate, bypassing the physical checkpoints with now-smaller queues for those who have not opted in. Tony arrives at the gate and, his identity again confirmed by facial recognition, boards the plane and departs. Similarly, when Tony arrives at his destination and heads for baggage claim, an area that today is outside the security perimeter, he can still be protected and easily claim his bag without further checks of boarding pass or claim tag. Most importantly, at the end of his journey, Tony will have spent his time at the airport in a way he wanted, not waiting in line.

FIGURE 2

Smart security improves security and improves passenger experience


Current aviation passenger experience
POTENTIAL SECURITY GAP
VULNERABILITIES STILL EXIST
As seen in 2015 Metrojet bombing
Arrival
Check-in
Bag check
Security checkpoint
Retail, concessions, and entertainment in terminal
Boarding and departure
Smart aviation passenger experience
Stand-off detection technologies help protect crowd waiting outside
Integration with existing airport/airline systems to enable walk-through check-in and bag-drop experiences
No waiting in line at checkpoints, simply walking straight to the gate or to shopping
Walk-through boarding of plane
FASTER, BETTER USER EXPERIENCE WITH NO SECURITY GAPS
Stand-off detection technologies (facial recognition, radar explosives detection, etc.)
Smart algorithms to detect unusual activity
Risk-informed interventions to meet the level of that unusual activity

Source: Deloitte analysis.

Most importantly, at the end of his journey, Tony will have spent his time at the airport in a way he wanted, not waiting in line.

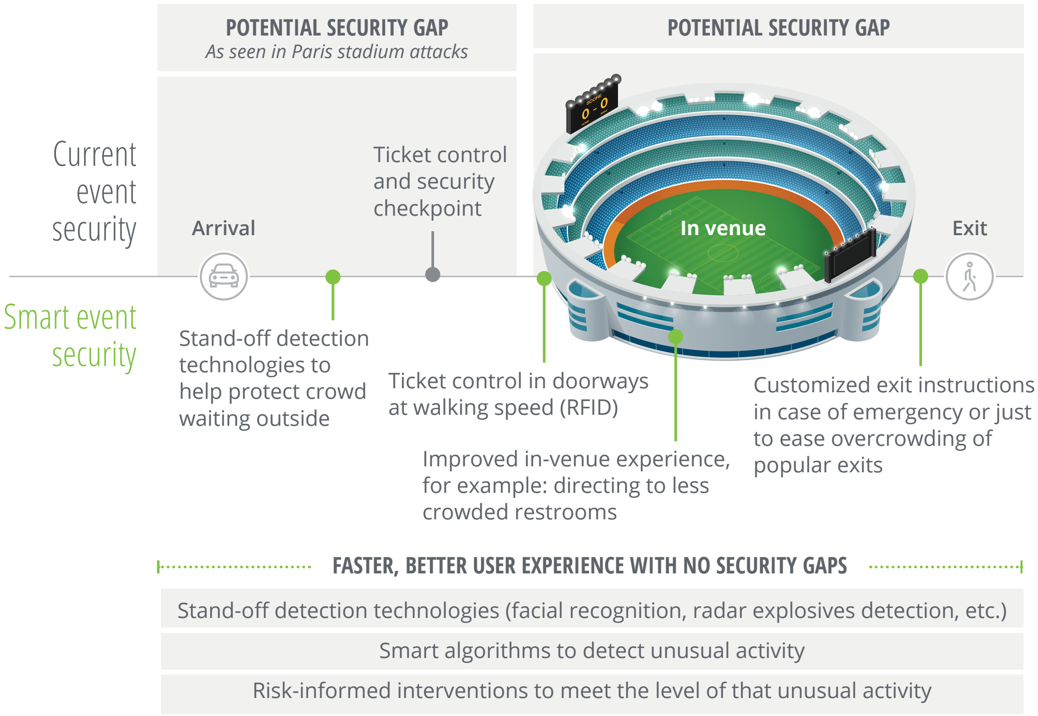
Stadiums, goods, and other use cases

Airports may be one of the most familiar examples of checkpoint-based security to many of us, but the same long lines and potential security gaps can be seen in other spaces such as stadiums, land border crossings, and even the transit of goods. As a result, smart security can offer significant benefits to these use cases, not just shorter lines. Much as airlines have worked with US Customs and Border Patrol to create facial recognition boarding gates, private companies could work with security organizations to offer improved services for checking tickets, giving directions to seats, or even pointing attendees to less crowded restrooms during halftime at the stadium (figure 3).

Smart security can offer significant benefits to these use cases, not just shorter lines.

FIGURE 3

Smart security can offer even nonsecurity-related benefits to users

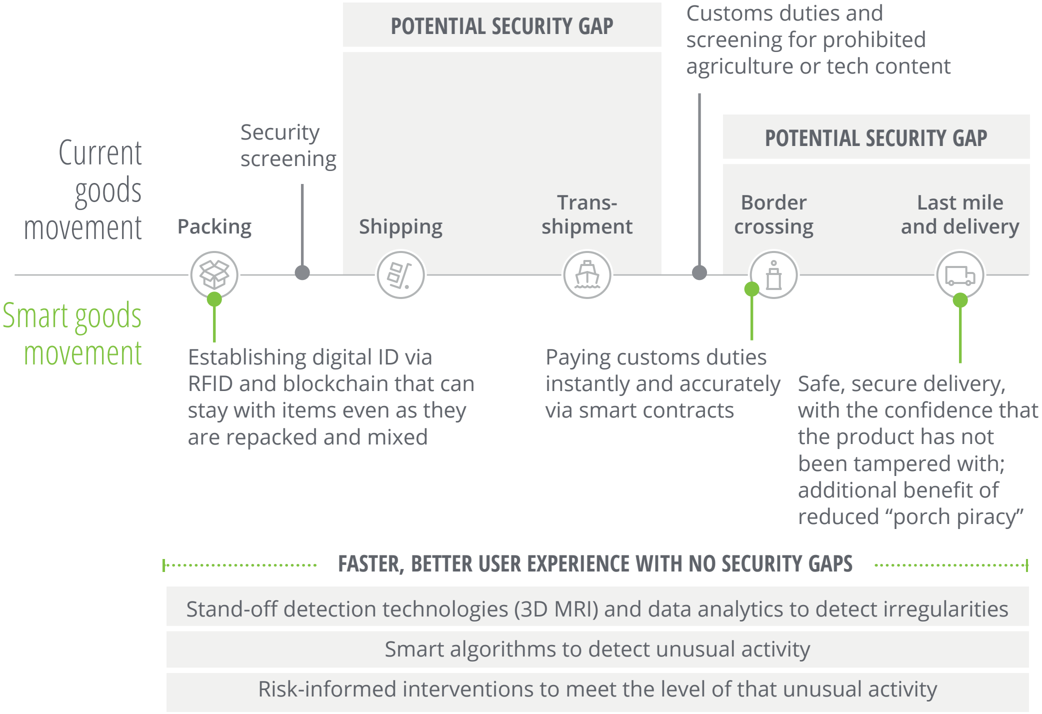

POTENTIAL SECURITY GAP
As seen in Paris stadium attacks
POTENTIAL SECURITY GAP
Current event security
Arrival
Ticket control and security checkpoint
In venue
Exit
Smart event security
Stand-off detection technologies to help protect crowd waiting outside
Ticket control in doorways at walking speed (RFID)
Improved in-venue experience, for example: directing to less crowded restrooms
Customized exit instructions in case of emergency or just to ease overcrowding of popular exits
FASTER, BETTER USER EXPERIENCE WITH NO SECURITY GAPS
Stand-off detection technologies (facial recognition, radar explosives detection, etc.)
Smart algorithms to detect unusual activity
Risk-informed interventions to meet the level of that unusual activity

Source: Deloitte analysis.

When it comes to the movement of goods, smart security is almost a reality today. Programs such as Customs and Border Patrol's Customs-Trade Partnership Against Terrorism (C-TPAT) have been using a risk-informed approach to screening cargo shipments since 2001.[12] At the same time, technologies such as GPS tracking and radio-frequency identification (RFID) can allow for continuous tracking and monitoring of goods at any stage in a journey. Pairing those technologies with smart contracts can create an increasingly frictionless flow of goods as even actions such as payment can be taken automatically just by a pallet arriving in a warehouse. By linking together these existing developments within the vision of smart security, even greater benefits can be realized (figure 4).

FIGURE 4

The movement of goods is already approaching the frictionless vision of smart security



Establishing digital ID via RFID and blockchain that can stay with items even as they are repacked and mixed

Paying customs duties instantly and accurately via smart contracts

Safe, secure delivery, with the confidence that the product has not been tampered with; additional benefit of reduced “porch piracy”

Stand-off detection technologies (3D MRI) and data analytics to detect irregularities

Smart algorithms to detect unusual activity

Risk-informed interventions to meet the level of that unusual activity

Source: Deloitte analysis.

Barriers to change

THE VISION OF smart security offers truly compelling benefits, but as with any significant transformation, it also faces several key barriers before those benefits can be realized.

Legal, ethical, and privacy concerns

Perhaps the largest barrier to smart security are concerns surrounding the legal and ethical use of personal data affecting personal privacy and other civil liberties. Both governments and the public are concerned about issues ranging from biases in AI algorithms, which incorrectly assess risk in minority groups, to the potential for misuse of personal data by government, law enforcement, and private companies.[13] This is not just a question of passing the right laws. While legal safeguards will continue to be necessary, with technologies evolving quickly, it often takes some time before there is legal consensus on how new technologies may or may not be used to collect and use personal data.[14] Therefore, staying on the right side of legal, ethical, and privacy concerns requires constant effort and monitoring by governments, citizens, private companies, and all involved.

Technology to process data

The biggest technology barrier is data. Collecting, integrating, analyzing, and securing data will be at the heart of any smart security system. In a smart security world, data will come in from different sources, some of it collected in the airport, some from the physical world outside, and some only from the internet. Some of it will be collected by the security organization, some by partners. Ensuring that the data is able to be integrated and seen together, and that partners are properly protecting private information is the table stakes of smart security. Clear contractual agreements and well-designed security protocols can keep the data flowing while still protecting the data citizens entrust to it.

Once that data is collected and integrated, there is still a problem of accuracy. The data must be used to appropriately train and validate machine learning algorithms. Without robust, tested models to curate the data, analyzing even well-integrated data would produce unorganized insights that would be hard to trust.

The biggest technology barrier is data. Collecting, integrating, analyzing, and securing data will be at the heart of any smart security system.

Finally, the technology of smart security cannot be static. It must be able to take advantage of new detection technologies or new data analysis techniques or it will quickly become outdated and irrelevant. Open platforms can help ensure the upgradability of smart security even when we can’t predict what the next big technology will be.

Organizational culture

A shift toward smart security will fundamentally alter how most organizations (government or otherwise) operate: from managing static checkpoints with little data-driven decision-making, to fewer checkpoints with a highly data-driven vetting process. Such a shift will require major operational and workforce changes. Leaders will need to re-evaluate everything from overall mission design down to the incentives for individual employees. They will also need to consider the composition of their staff to ensure enough diversity of thought is brought to each challenge, be it an emerging threat or protecting personal privacy.

Another area where organizational culture will be critical is the protection of minority rights. Smart security tools are designed to flag things out of the ordinary, so those communities that are often tagged as out of the ordinary, such as racial, religious, or other social minorities, may be subject to greater scrutiny, unless new systems are supported by an organizational culture that takes steps to avoid such bias. Such steps would cover both the design of algorithms and the implementation of risk-informed interventions, and would require significant and continuous involvement from leaders at every level of the organization.

Recommendations on how to get started

WHILE THESE BARRIERS may seem significant, smart security is already succeeding in the world around us if we know where to look. Examples from car insurance to companies such as CLEAR show that the method works for both security and users. Here are some concrete ways to get started.

Design with privacy and risk appetite in mind

One of the largest risks to privacy is "functional creep," where a product designed for one purpose is suddenly used for another purpose. A custom-built smart security system will be better able to protect the privacy of citizens than a patchwork of ersatz systems that may develop over time. Such a purpose-built system should offer its users greater awareness of what data is being collected and how it is being used, and the ability to control both. With such user controls, citizens can also adjust how much data they wish to share and for what benefits. This makes it much more difficult to use purpose-built systems for other objectives.

Don't go it alone

The technical, organizational, and communication challenges related to smart security are likely larger than any single organization can handle on their own. Ecosystems such as aviation and trade are complex, and it is likely that other players already have the data, technology, or expertise you need to solve your problems. Public-private collaboration has already begun to pay dividends in areas such as facial recognition in aviation, and expanding the cooperation between security agencies, transit providers, tech companies, importers/exporters, infrastructure owners, and even the general public will be critical to the success of the smart security concept.

Communicate to users

Communication with the general public and users will also need to be done regularly to raise awareness of what smart security is and allay fears about what it is not. Easy user access to a host of easily digestible resources will be key; the details of smart security cannot be buried in complex legal documents and jargon. Clear communication and effective user control of data may require novel user interfaces that go beyond just another smartphone app.

Smart security is already succeeding in the world around us if we know where to look.

Another critical part of the communications strategy will be managing user experience and related perceptions. For example, if seeing security officers and metal detectors can give people a sense of security, then removing them may create a sense of insecurity, despite the overall level of security being improved. As organizations move toward smart security, ensuring users of the service—or those who choose not to use it but who witness its use (for example, seeing people walk around physical security checkpoints may be alarming to some bystanders)—understand how their experience will change will be critical to avoiding confusion or insecurity.

Above all, get started today

While this vision of smart security may seem far off in the future, the groundwork already exists today. Take aviation for example. Most travelers' digital footprint already exists, and providing airport security access to it could be as simple as giving consent in exchange for an improved airport experience. Such an exchange is already happening at a smaller scale with services such as CLEAR, TSA PreCheck, and Global Entry (each with participants ranging from 4 to 8 million), showing that passengers can be comfortable with the concept.[15] Moreover, airports from Atlanta to Singapore and Amsterdam to Aruba are experimenting with more curb-to-gate biometric screening of passengers. For security officers, that can add layers of security within which to detect threats. For passengers, it represents an easier, faster travel experience that is, in the words of the Delta Air Lines COO, "removing the need for a customer checking a bag to present their passport up to four times per departure."[16] The world is moving toward smart security; if citizens and government agencies do not prepare today, we collectively take the chance that those who do develop the technologies may not value privacy and security as much as we may want.

Technological evolution promises to move people, goods, and information around the globe at ever-faster rates. When we can get almost anything delivered right to our doors within hours or days, no longer is it acceptable to have to choose between safety, speed, or privacy. The modern world cannot function with static security but demands a new approach—one of smart security.

Endnotes

[1] A. Stallinger et al., "The effects of different mouth-to-mouth ventilation tidal volumes on gas exchange during simulated rescue breathing," *Anesthesia and Analgesia* 93, no. 5 (2001): pp. 1265–9.

[2] Domo, "Data never sleeps 5.0: How much data is generated every minute?," July 17, 2017.

[3] Transportation Security Administration, "TSA PreCheck," accessed April 1, 2020; Clearme, accessed April 1, 2020.

[4] Aaron Boyd, "Security clearance backlog hits long-awaited 'steady state'," Nextgov, January 22, 2020.

[5] Ibid.

[6] David Luckey et al., "Assessing continuous evaluation approaches for insider threats," RAND Corporation, 2019.

[7] Jane Li, "Shanghai apartment buildings are secretly installing facial-recognition devices," Quartz, October 18, 2019.

[8] For more information on trust in biometrics, see: Experian, *2020 global identity and fraud report*, accessed April 1, 2020; for more information on autocratic uses of technology, see: Richard Fontaine and Kara Frederick, "The autocrat's new tool kit," *Wall Street Journal*, March 15, 2019.

[9] Experian, *2020 global identity and fraud report*.

[10] Teena Maddox, "PATSCAN platform detects hidden weapons, chemicals, and bombs," Tech Republic, January 10, 2020.

[11] National Academies of Sciences, Engineering, and Medicine, "A primer to prepare for the connected airport and the Internet of Things," 2018.

[12] US Customs and Border Protection, "CTPAT: Customs Trade Partnership Against Terrorism," accessed April 1, 2020.

[13] Chris DeBrusk, "The risk of machine-learning bias (and how to prevent it)," *MIT Sloan Management Review*, March 26, 2018; Fontaine and Frederick, "The autocrat's new tool kit."

[14] US Supreme Court, "United States v. Jones, 565 U.S. 400," 2012; US Supreme Court, "Maryland v. King, 569 U.S. 435," 2013; ACLU, "You are being tracked: How license plate readers are being used to record Americans' movements," accessed April 1, 2020; Ring, "Why do law enforcement agencies use the Neighbors app?," accessed April 1, 2020.

[15] As of July 2019, TSA PreCheck had 8.5 million participants (see: Dawn Gilbertson, "Interested in TSA PreCheck? It might soon be cheaper and easier to sign up," *USA Today*, June 19, 2019); Global Entry had 5 million in April 2018 (see: US Customs and Border Protection, "CBP announces 5 million global entry members," media release, April 3, 2018); CLEAR had 3.8 million in July 2019 (source: CLEAR, "CLEAR Launches at Birmingham-Shuttlesworth International Airport," press release, Business Wire, July 18, 2019).

[16] Future Travel Experience. "Delta officially unveils new biometric terminal at Hartsfield-Jackson Atlanta International Airport," December 2018; Thom Patterson, US airport opens first fully biometric terminal," CNN, December 2018; Kathryn Steele, "Delta unveils first biometric terminal in U.S. in Atlanta; next stop: Detroit," Delta Airlines, December 2018.

Acknowledgments

The authors would like to thank **Biff Lyons**, **Henry Ennis**, **Sam Wolter**, **London Swift**, and **Aditi Rao** for their research and editorial support.

About the authors

Dr. Mike Gelles | Mgelles@deloitte.com

Dr. Mike Gelles is a managing director with Deloitte Consulting LLP's Federal practice, consulting in the areas of law enforcement, intelligence, and security. Gelles is a thought leader and widely published author on critical national security issues including insider threat, security processing, secure workforce, asset loss, exploitation, sabotage, and workplace violence. Previously, he served as a naval officer and the chief psychologist for the Naval Criminal Investigative Service.

John Adams | Johnadams2@deloitte.com

John Adams is a managing director with Deloitte Consulting LLP. Adams joined Deloitte Consulting after a 22-year career with the Federal Bureau of Investigation. Drawing on his law enforcement, national security, and technology experience, he provides expertise to government clients at the federal, state, and local level to help organizations solve complex challenges. Prior to leading the FBI's technology branch, Adams served as assistant director of the FBI's Directorate of Intelligence. He previously served as the Special Agent in Charge of the FBI's Norfolk Field Office and as a deputy assistant director in the Counterterrorism Division.

Joe Mariani | jmariani@deloitte.com

Joe Mariani leads research into defense, security, and law enforcement for Deloitte's Center for Government Insights. His research focuses on innovation and technology adoption for both national security organizations and commercial businesses. His previous work includes experience as a consultant to the defense and intelligence industries, high school science teacher, and Marine Corps intelligence officer.

Adam Routh | adrouth@deloitte.com

Adam Routh is a research manager with Deloitte's Center for Government Insights and a PhD student in the Defence Studies Department at King's College London. His research areas include emerging technologies, defense, and security with a focus on space policy. Routh previously worked for the Defense Program at the Center for a New American Security (CNAS). Prior to CNAS, he worked in the private sector where he facilitated training for Department of Defense components. He also served as a team leader with the US Army's 75th Ranger Regiment.

Burak Sahin | bsahin@deloitte.com

Burak Sahin is a specialist master with Deloitte & Touche LLP with 22 years of experience in biometrics and security. Sahin holds an MBA, MS, and BS degrees in electrical engineering, is an IEEE-certified biometrics professional with 18 patents, and a project management professional. Prior to Deloitte, he was a program manager at MicroStrategy, leading teams in the development of biometric systems.

Akash Keyal | akkeyal@deloitte.com

Akash Keyal is a senior research analyst with the Deloitte Center for Government Insights. He focuses on delivering key insights on topics related to defense, security, and justice.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Mike Gelles
Managing director | Deloitte Consulting LLP
+1 571 814 7290 | mgelles@deloitte.com

Mike Gelles is a managing director with Deloitte Consulting LLP's Federal practice, consulting in the areas of law enforcement, intelligence, and security.

Center for Government Insights

William Eggers
Executive director | Center for Government Insights | Deloitte Services LP
+ 1 202 246 9684

William Eggers is the executive director of Deloitte's Center for Government Insights, where he is responsible for the firm's public sector thought leadership. His most recent book is *Delivering on Digital: The innovators and technologies that are transforming government*.

Joe Mariani
Manager | Center for Government Insights | Deloitte Services LP
jmariani@deloitte.com

Joe Mariani leads Deloitte's research into defense, intelligence, and justice issues for Deloitte's Center for Government Insights. His research focuses on how government agencies can cultivate innovation and emerging technologies.

Adam Routh
Manager | Center for Government Insights | Deloitte Services LP
adrouth@deloitte.com

Adam Routh is a research manager with Deloitte's Center for Government Insights and a PhD student in the Defence Studies Department at King's College London. His research areas include emerging technologies, defense, and security with a focus on space policy.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Aditi Rao, Blythe Hurley, Rupesh Bhat, Hannah Bachman
Creative: Kevin Weier and Molly Woodworth
Promotion: Alexandra Kawecki
Cover artwork: Chiara Verseci

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.