STANLEY Security

# THE FUTURE OF SECURITY: A LOOK AT THE TECHNOLOGIES PROPELLING US FORWARD

## THE FUTURE OF SECURITY

In December 2019, we identified 10 trends we expected would impact security consumers in 2020 and published those in our first annual Industry Trends Report. These trends were based on insights from leaders across STANLEY Security, survey data from decision-makers across North America and Europe and monitoring data from more than 400,000 STANLEY Security customers. Today, many of those trends ring true more than ever before, and we're seeing new and renewed interest in specific security solutions. This white paper details those solutions, including:

- **ADVANCED VISITOR MANAGEMENT**
- **INTEROPERABLE EMERGENCY COMMUNICATION**
- **ALARM VERIFICATION**
- **CYBERSECURITY**
- **DATA ANALYTICS**
- **CLOUD-BASED SOLUTIONS**
- **REMOTE SERVICES**

## OVERVIEW

Our world has changed. An increasing number and variety of threats exist that require organizations to think differently about how they protect their people, property and assets. The sweeping impact of COVID-19 brought new challenges to light that exposed security vulnerabilities organizations didn't know existed in their environments. This has not only accelerated new technology innovation but also has driven adoption of security technologies that have been around for years.

As organizations plan for the future, many will need to re-evaluate not only what security systems they have in place, but also what security means to them – and redefine the value and purpose of security altogether.

- ***Is it still about protecting against theft, or is it about creating a virtual command center that integrates their security and communication systems in one place, easily managed and viewed from anywhere?***
- ***Is it about ensuring their network is secure from the growing number of cyber threats or is it about securing their finances and reducing unnecessary truck rolls and service calls?***
- ***Is it the ability to track and manage traffic flow and understand exactly who is coming and going from their facility, while ensuring they've been properly screened?***

Security challenges have changed and so have the solutions organizations need. As they re-evaluate and rebuild their security program, many are turning to the technologies outlined in this white paper. As a result, we expect that many of these technologies will be central to organizations' security strategies for the duration of 2020 and will be fundamental in helping organizations navigate new challenges in the future.

## ADVANCED VISITOR MANAGEMENT

Visitor management has become a topic of heightened interest as organizations across the globe are taking steps to ensure they can more effectively screen individuals accessing their property. Importantly, visitor management has moved beyond the visitor. Some systems have evolved to include contractor, vendor and employee identity management. This type of advanced system has a much broader appeal to both traditional security and now EHS professionals by offering the ability to automate through workflows and ensure proper compliance with ever-changing policies around vetting those who enter organizations' facilities.

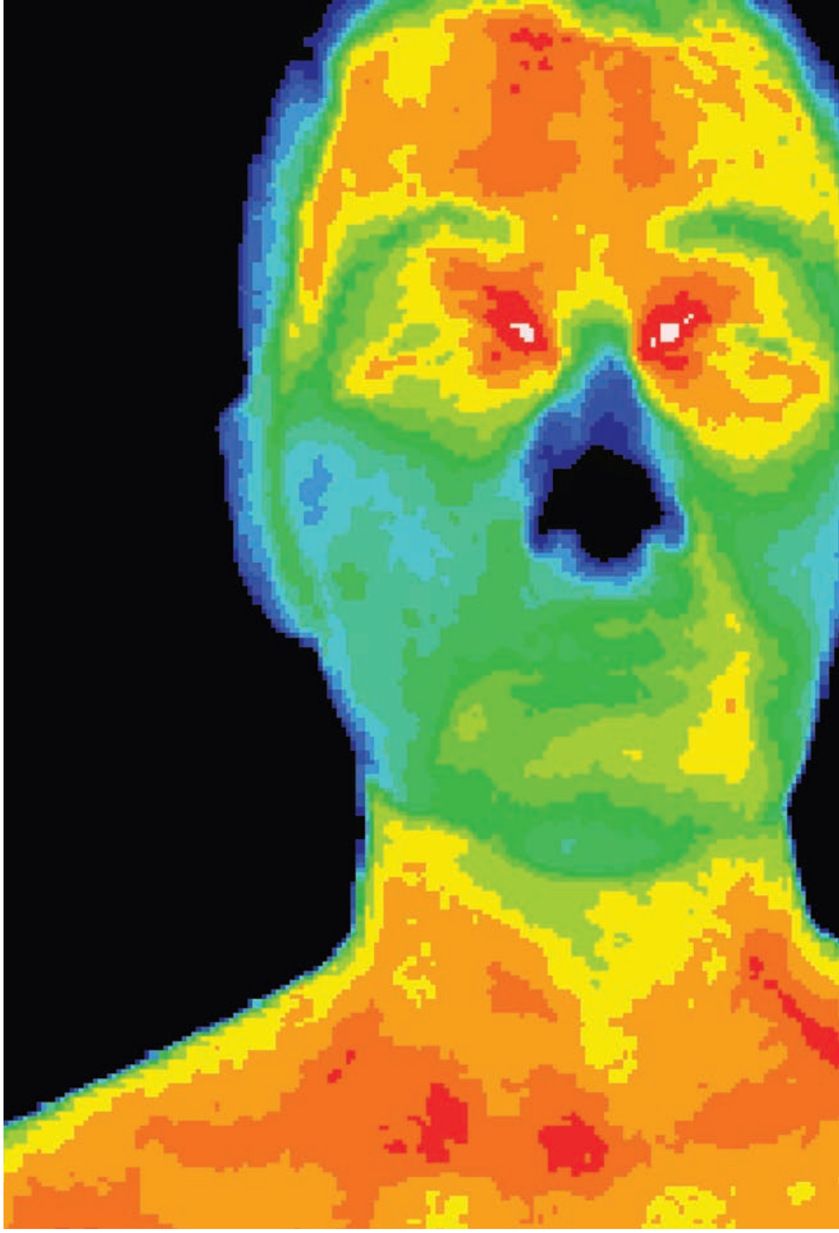
As a result, there's been an explosion of demand for advanced visitor management technologies that can automate certain processes, enforce organizations' policies and compliance and integrate with existing security systems.

### Human Temperature Screening

One of the fastest-growing security technologies today is the human temperature screening device. This technology – which uses thermal imaging sensors – is intended to detect elevated temperatures of people entering a facility. Many organizations are deploying or seeking to deploy these devices for an extra layer of screening and detection for staff and visitors. As popularity and adoption increases, human temperature screening is becoming an important component of many organizations' security programs.

### Electronic Visitor Management

Visitor management kiosks are quickly replacing pen and paper logs, as they allow organizations to easily screen and track individuals, produce visitor badges and more – all without requiring a front desk associate to manually manage this process. Whether an organization has one site or multiple, these systems provide all the benefits of convenience, compliance and visibility across the entire organization.



**Interoperable communications and signaling** is the merging of technologies on one specific platform, enabling first responders and incident stakeholders to share voice communications, cellular communications, data and video

## INTEROPERABLE EMERGENCY COMMUNICATION

Effective, streamlined communication is paramount during emergencies. When organizations are responding to a critical incident, breakdowns in communication can delay incident response time and potentially lead to fatal consequences. In some parts of the world, funding is now available for increased infrastructure as it relates to crisis management and emergency response, leading to a growth in demand for interoperable emergency communication platforms.

These platforms provide enhanced situational awareness and allow for streamlined cross-communication and real-time incident response. By bridging disparate systems on a single, secure network, interoperable communication platforms connect multiple agencies and organizations – as well as multiple departments and facilities within a single organization – when an emergency strikes. In doing so, they enable first responders and organizations to:

- Send and receive crucial data instantly
- Collaborate and coordinate in real time
- Rapidly respond in the event of a critical incident

## ALARM VERIFICATION

COVID-19 has had a lasting impact on communities across the globe, and as they continue to navigate this new norm, many law enforcement agencies have implemented measures to limit human contact where possible. In some cases, this means not responding in person to certain calls, such as breaking-and-entering reports in which there are no suspects or possibility of property recovery. It's yet to be seen whether these differential response plans will remain in effect indefinitely, but one thing is clear: Alarm verification is becoming more critical to protecting businesses and improving usage of limited police resources.

Alarm verification uses video and audio technologies to provide information crucial to the verification of crimes in progress and allow a monitoring center operator to quickly confirm human presence and begin the process of assessing threat levels. In contrast to traditional alarms that may be tripped by a tree blowing in the wind, a stray animal or the sound of a freezer kicking on, verified alarms provide actionable intelligence that confirms a crime is in progress.

This can lead to a priority dispatch of authorities and – for audio-verified alarms – has contributed to over 180,000 documented apprehensions, many of them prior to entry. In addition to enhancing the probability of apprehension, alarm verification technology is particularly appealing for organizations that want to avoid costly false alarm fees, while potentially decreasing police response time.

Some alarm verification solution providers have reported that the average police response time in the case of a verified alarm is up to **85% faster** than if the alarm was not verified as potentially legitimate

## CYBERSECURITY

Across companies of all sizes, cybersecurity remains a top priority, especially with the influx in demand for cloud-based technologies and remote services. However, the shortage of cybersecurity skills in the marketplace, lack of resources for dedicated cybersecurity staff and increased complexity of managing enterprise networks has organizations turning to technology for help mitigating risks of cyber threats to their environment.

While many cyber attacks are attributable to attackers targeting traditional endpoints, there's been a steady rise in the number of attacks targeting IoT and other IP-connected devices. These devices are designed to communicate with each other using internet protocols that allow them to be connected and managed remotely. As such, they're connected to the larger corporate network, making them a liability if not managed and maintained properly. By leveraging network protection solutions, organizations can keep their network, devices and data safe from cyber attacks, such as intrusion, malware, ransomware, phishing, malicious files and more.

## DATA ANALYTICS

In the simplest terms, data analytics allows organizations to make sense of all the disparate streams of data coming from their security systems. This data could include, for example, a video stream from a security camera. Layered on top of that, security systems also produce metadata – or information (data) about data itself. Whereas data is the video stream, metadata could be the IP address or frame rate of the camera. By leveraging data analytics and machine learning, organizations can utilize this data to become more proactive in addressing short-term challenges and driving long-term efficiencies.

Can my security system help me enforce social distancing and building occupancy limits in real time? How can I use my security system to automate loss prevention efforts? From enabling organizations to solve specific problems like these to helping them understand their risk profile and find innovative ways to enhance the customer experience, harnessing Big Data can provide major benefits for organizations of all sizes.

## CLOUD-BASED SOLUTIONS

The value of cloud-based security solutions is more apparent now than ever before. The ability to access on-site security systems remotely and rapidly respond to emerging threats or changing environments is key to ensuring an organization’s security. During times when organizations may feel like they lack control over their facility and its physical security, cloud-based solutions can offer eyes and ears on-site, restoring that control and providing the organization a deeper level of operational insights. The following cloud-based solutions are particularly relevant today:

### Cloud Access Control

Cloud access control enables organizations to remotely manage processes, such as adding or revoking user access, without requiring any hardware. This is especially critical during situations in which organizations must quickly and efficiently update access privileges to ensure only authorized personnel are able to access a facility.

Mobile credentials continue to play a key role in cloud access control, as organizations seek to implement contactless solutions that are not only easier to manage but also help to reduce the spread of germs. Additionally, mobile credentials – which are equivalent to access control cards but are digitally stored in individuals’ phones – can be integrated with fingerprint and facial recognition capabilities, allowing for an even more secure solution.

### Cloud Video Surveillance

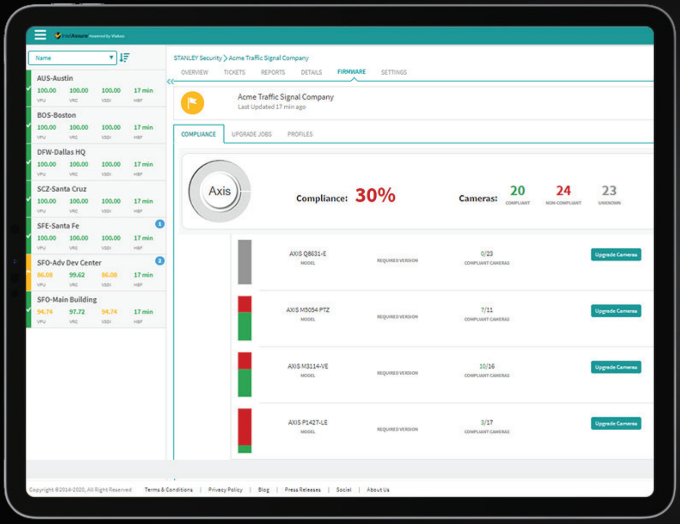
With the potential for increased storage, readily controlled remote access to data, extensive utility and minimized cost, it’s no wonder why cloud video surveillance has emerged as a top security technology that organizations are considering. By integrating IP cameras with cloud infrastructure, organizations can access, manage and monitor video surveillance footage for various locations from a single, remote platform. This offers myriad benefits for organizations – including extreme scalability, operational efficiencies and cost-effectiveness – but perhaps one of the greatest benefits is the increased data security.

One of the biggest misconceptions about cloud video surveillance is how and where organizations’ crucial, sensitive data will be stored. For many who may not be fully informed, sending video data “into the cloud” seems in and of itself to be a major risk, with the perceived ambiguity of the cloud offering no tangible sense of security. However, without the presence of open ports, on-premises software or the need for on-site firewalls, cloud video surveillance can eliminate several crucial avenues by which traditional video surveillance systems are left vulnerable to cyber attacks and potential data breaches.

### Intelligent Automation & Service Assurance

As organizations look for ways to reduce costs and limit staff exposure to external vendors coming on-site, solutions that allow for remote monitoring and which automate many security processes are becoming increasingly important. One such solution is a service assurance platform, which helps organizations monitor the health of their IP-connected and IoT devices as well as mitigate cybersecurity risks.

Service assurance platforms – cloud-based solutions that are accessible remotely – automate processes like maintaining an inventory of devices on the network, managing critical firmware updates and more. They connect to each component of a security program and continuously monitor for faults in hardware, network communications or connections, software services and other issues affecting overall performance and functionality – including potential cybersecurity vulnerabilities, video camera downtime and retention issues and other common device failures that may have previously required a technician to investigate on-site. In doing so, they help organizations save time and money, while providing enhanced visibility across an entire security program.



STANLEY Security > Acme Traffic Signal Company

| | VPU | VRC | VSDI | HBF |
|---|---|---|---|---|
| AUS-Austin | 100.00 | 100.00 | 100.00 | 17 min |
| BOS-Boston | 100.00 | 100.00 | 100.00 | 17 min |
| DFW-Dallas HQ | 100.00 | 100.00 | 100.00 | 17 min |
| SCZ-Santa Cruz | 100.00 | 100.00 | 100.00 | 17 min |
| SFE-Santa Fe (1) | 100.00 | 100.00 | 100.00 | 17 min |
| SFO-Adv Dev Center (2) | 86.08 | 99.62 | 86.08 | 17 min |
| SFO-Main Building | 94.74 | 97.72 | 94.74 | 17 min |

Acme Traffic Signal Company
Last Updated 17 min ago

Axis Compliance: 30% Cameras: 20 COMPLIANT 24 NON-COMPLIANT 23 UNKNOWN

| MODEL | REQUIRED VERSION | COMPLIANT CAMERAS | |
|---|---|---|---|
| AXIS Q8631-E | | 0/23 | Upgrade Cameras |
| AXIS M5054 PTZ | | 7/11 | Upgrade Cameras |
| AXIS M3114-VE | | 10/16 | Upgrade Cameras |
| AXIS P1427-LE | | 3/17 | Upgrade Cameras |

Copyright ©2014-2020, All Right Reserved Terms & Conditions | Privacy Policy | Blog | Press Releases | Social | About Us

IntelAssure™
Powered by Viakoo

## REMOTE SERVICES

Just as demand for security technologies shifts toward more cloud-based solutions, remote security services will become even more prevalent. This was already a growing trend prior to the COVID-19 pandemic, but with additional strain on company resources – both in terms of personnel and budgets – as well as increased restrictions for on-site visitors, remote services will play a key role in helping organizations operate within their new norm. The following remote services are particularly relevant today:

- **Remote Managed Services:** Dedicated off-site security professionals are trained to manage and service all or part of an organization's security program. They're employed by a security provider but work full time as a dedicated resource for the organization.
- **Security Management Platform:** Security providers typically offer free access to online portals that can allow organizations to place and schedule service calls, review billing, view reporting, make changes to user lists, place systems into test and more.
- **Remote Guard Tours:** Operators in the monitoring center use the video surveillance system on-site to visually patrol a given area and can even talk to people to identify them and confirm if they should be on-site. This solution can result in up to 80% cost savings when compared to the cost of an on-site patrol.
- **Audio Talk-down:** When a video surveillance camera detects motion where there shouldn't be any, a pre-recorded warning message can be played or operators from the monitoring center can issue a live warning.
- **Remote Interactive Response:** This round-the-clock service enables monitoring center operators to utilize all security systems on-site – such as access control, video surveillance and intercoms – to take over the duties of on-site patrol. This could include visitor validation, vehicle access, lockdown of specific areas and more.
- **Time and Attendance Remote Tracking:** Enhancements to traditional time and attendance systems allows organizations to track remote staff hours, breaks, overtime, absences and more through remote clocking-in capabilities.

Remote guard tours can result in up to **80% cost savings** when compared to the cost of an on-site patrol

## SECURING OUR FUTURE

Technology itself isn't going to solve today's challenges; rather, it's the use of differentiated technology combined with an integrated approach that will lay the foundation for a more secure future. In the past, organizations may have fared well managing disparate systems with different platforms and interfaces, but today's security challenges require a robust, integrated program backed by a holistic strategy.

As organizations adapt to the changes brought forth by COVID-19, it's critical to keep an eye toward the future when implementing and integrating new security technologies. In considering these technologies as part of a long-term strategy, as opposed to a short-term solution, organizations can develop a more resilient security program that can propel them forward and prepare them for the future.

# Here For You

We hope you've found this resource helpful. If you'd like more information on any of the technologies detailed in this white paper or would like to discuss how we can support you, please don't hesitate to reach out.

CONTACT US