STANLEY Security

THE POWER OF REMOTE SECURITY MANAGEMENT

THE POWER OF REMOTE SECURITY MANAGEMENT

Many functions in your company now likely allow for remote capabilities. Despite the explosion of technology enabling this growth, security teams have by and large stayed with traditional, on-premises-only security programs.

But as the nature of work moves toward remote capabilities, security solutions must keep pace and prepare companies for new threats and issues liable to emerge. Security teams wanting to be prepared should be considering how they can leverage remote security management to maintain their company's security program.

What is Remote Security Management?

Remote security management fulfills the same functions as traditional security solutions while giving professionals the power to conduct security measures from anywhere they work. Remote security programs leverage the use and design of cloud-based technology, as well as the services and programs built around it, to deliver the flexibility, ease of use and efficiencies needed to scale alongside businesses.

Remote managed services operate in the cloud, handle processing, storage, alerts and other security functions off-site. The promise of the cloud, coupled with the right advanced physical security components, can create a strong remote program capable of supporting a scaling enterprise. Equipped with tools accessible from anywhere and at any time, your security team can ensure the protection of on-premises assets and people regardless of physical location.

Even when disasters and other events prevent access to your locations, your remote security program ensures you can continue managing and protecting your company's assets. Cloud-based security tools also provide extra layers of security and risk mitigation, maximizing value while protecting against threats and issues both seen and unseen within your company.

The ROI of Remote Security Programs

The addition of new technology and capabilities will likely raise questions regarding return on a larger investment. After all, shouldn't a traditional security program be enough to protect your company?

While traditional security programs offer physical protection, remote security programs can offer a number of additional benefits businesses should consider.

Direct Cost Savings

Remote security programs, including the automation they offer, can reduce the number of maintenance calls and system downtime, costs that add up quickly when unchecked. Shifting services to the cloud also reduces resource consumption in terms of server and storage space — an important consideration as your company expands to new locations also requiring security. Accurate and backed-up data and stored video events and footage can also reduce fees or fines paid out due to claims and incidents.

Impact on Brand

A remote security program can let your security team manage all security-related aspects of your company at any time, protecting your company's brand even when you are not watching.

Features like video alarm verification can verify perimeter breaches and break-ins, while video investigation can help protect against liability events and provide the proper video evidence for investigations that could otherwise tarnish brand reputation.

Remote programs can also aid in reducing the potential for exposure to legal claims and negative perception, which could otherwise harm the company's value.

Preparation for Future Threats

Traditional programs can quickly become outmoded as new security threats emerge. Rather than chasing after emerging threats by purchasing new equipment, a remote program managed in the cloud can scale with threats and easily adapt to new security needs and the technology required to address new threats.

Elements of Remote Security Programs

A robust remote program incorporates several types of components to ensure broad protection. Common elements include:

Access Control as a Service (ACaaS)

Whether you're securing your physical locations or protecting user access to your systems, a cloud-based access control solution gives your team added flexibility and ensures security on a 24/7 basis. Remote access to identity and location management can allow security teams to grant or rescind access for any user at a distance. Physical components like access cards and mobile credentials as well as IT-based access can be managed and coordinated over a cloud-based system.

At times when having a physical presence to verify events would be challenging, ACaaS coupled with video surveillance provides instant verification on triggered events. Cloud-based access control also offers data backups and failover protection to ensure access is retained even when unforeseen issues arise.

Video Surveillance as a Service (VSaaS)

In traditional video surveillance systems, cameras relay data via your local network into local storage units. These on-premises systems can be a secure protection method, but they can also become inflexible and a greater risk as your company scales.

Today's VSaaS systems are built for ease and flexibility. Cloud-based systems are accessible from anywhere, offering remote access for your teams to follow through on investigations or provide continuous monitoring. Along with securing video data, cloud solutions can also expand more easily with your business needs than traditional on-premises systems can. There's no need to replace failed disks, patch servers or purchase and maintain additional hardware as you scale.

Intelligent Service Assurance

As you build your remote security program and install more physical and IT-related components, complexity increases. It can quickly become difficult to monitor all locations and vulnerability points, protect assets and people and ensure your total security infrastructure, services and components are fully operational. Intelligent service assurance platforms automate many of these points of concern as well as the process to alert security professionals to system issues. These platforms connect to each component of your security program and continuously monitor for faults in hardware, network communications or connections, software services and other issues affecting overall performance and functionality.

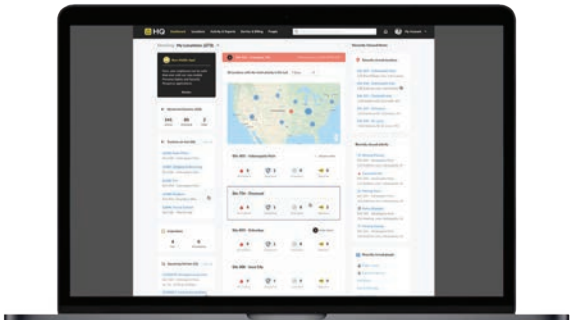
Monitoring and protection options are typically arranged in three ways:

- Customer monitoring — As the customer, you have full access to your service assurance platform. You must resolve any detected events or issues. Though it may be the lowest-priced service, it may not be the most cost-effective option for your business based on staffing and domain expertise needs.
- Professional monitoring — While the customer has access to the platform dashboard and reporting, security domain professionals monitor 24/7 and handle any issues that arise. Though this may be a higher-priced option, the total ROI can prove to be very beneficial to your business when you offset the staff, downtime and service calls.
- Hybrid monitoring — The customer has access to the monitoring platform, manages all the tickets and decides which issues or failures they will handle and then are able to pass more complicated issues on to their professional security partner for resolution. This is a compromise and gives you the best of both service model approaches.

Regardless of your setup option, your system should also provide automated alerts when events or failures occur. For example, if a camera fails a diagnostic test, the system will alert you to the fault and offer solutions to fix it. This way, your platform optimizes your company's security presence — and as a cloud-based solution, it's accessible from anywhere for teams to respond as needed.

Building Your Remote Security Program

Building and running a strong remote security program requires several steps and collaboration between different teams in your company. As you consider what remote functions would be best for your needs, be aware of the typical remote security installation and setup process:



Before You Install

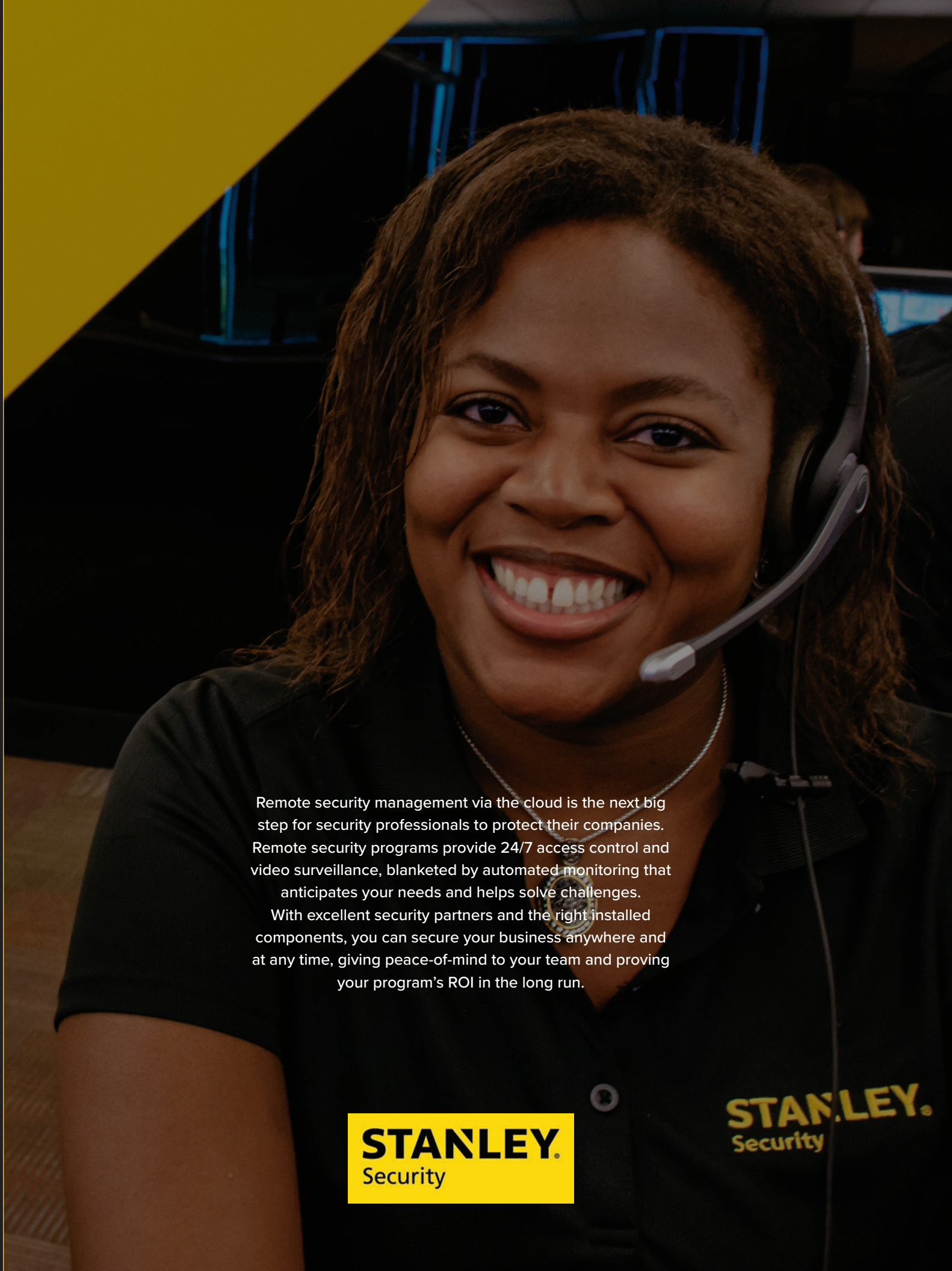
- Form a team who will champion the program. Ensure physical and IT teams are both represented, as you'll need to share capabilities and clear responsibilities between them.
- Analyze your locations to determine your needs. Pay special attention to cameras, access points and network bandwidth.
- Assess which remote program elements fit your needs. ACaaS, VSaaS and service assurance all provide different benefits and provide value to your business in different ways.
- Get buy-in from your company leadership. You will need them to sign off on budget requirements and your installation and usage plans. Build out your ROI calculation based on your existing security maintenance costs and liabilities due to downtime to help explain the benefits of a remote solution.
- Research security partners. See what remote offerings they provide as well as their support options and pricing model. ACaaS, VSaaS and service assurance monitoring typically involve monthly or annual subscription fees.
- Plan for installation with your chosen security partner. Once you select a partner, develop a plan that clearly outlines roles and responsibilities. Ensure your team agrees on the most important security priorities; without an understanding of priorities, it can be easy to interrupt a smooth installation process.

During Installation

- Communicate details with your security partner and internal team. To match with your installation plan, share specific details around the installation process: Does your IT team need to open any ports or provide server access? Does your physical security team need to run any additional cable lines?
- Ensure constant communication between your internal team and stakeholders. You want to ensure all priorities are being achieved as your security partner works through the installation process.
- Prepare for unexpected decisions as the situation changes. Ensure your plan can handle disruption and has action steps for how to handle on-the-fly changes.

Maintenance and Expansion

- Plan for updates and improvements. As your company builds more locations or changes its security makeup, ensure remote capabilities are updated if affected.
- Stay abreast of emerging trends. As you should be doing now, continue learning about new security trends or threats and be ready to address them.
- Lean on your security partner to develop stronger programs. As you grow and need to respond to new threats, your partner should provide options to help you scale.



Remote security management via the cloud is the next big step for security professionals to protect their companies. Remote security programs provide 24/7 access control and video surveillance, blanketed by automated monitoring that anticipates your needs and helps solve challenges. With excellent security partners and the right installed components, you can secure your business anywhere and at any time, giving peace-of-mind to your team and proving your program's ROI in the long run.

STANLEY
Security