



Video at the Door: Driving New Revenues

IN PARTNERSHIP WITH:  **ailient**



Video at the Door: Driving New Revenues

The front door is the gateway to the smart home. Smart door locks, networked cameras, and video doorbells are some of the best adopted smart home products because of the great value provided. These products – and integrations between them – serve the core convenience and comfort value propositions of the smart home: consumers want to know who is at the door, to easily grant entrance to the right people at the right time, and have the peace of mind that their home is secure.

Front door products, including video doorbells and smart locks, are among the most-adopted devices among buyers new to the smart home, acting as gateway to additional smart home product adoption.

Companies are working hard to differentiate products in a crowded video device market, adding new tech-enabling features and services that extend applications and use cases. Differentiation is a challenge in a market where competition is driving hardware commoditization. To stay competitive, connectivity is a minimum requirement, and with each generation, device manufacturers are racing to be smarter and more feature-rich.

Consumers benefit from the rapid pace of innovation in the smart home, as do the companies who monetize new value streams created by this wave of innovation.

This white paper investigates video innovation and integration in home access control. It assesses consumer adoption and demand for video analytics, face unlock features, and the ability to differentiate known people from strangers. It evaluates the service revenue opportunity for door lock manufacturers to move from video partners to video providers. Finally, it highlights research on consumers' willingness to share outside video streams and the best approaches to providing smart video access solutions while earning and keeping consumer trust.

— TABLE OF CONTENTS

Video at the Door: Driving New Revenues

Next-Gen Access: Convenient, Smarter, More Secure 4

- Consumers Want Video at the Door
- Consumers Want to Know Who is at the Door
- Consumers Want Convenience at the Door

Competitive Drive to Keep Innovating 8

- Differentiate Product Tiers with Biometrics
- Generate Service Revenue with Video

Video-based Access: Balancing Privacy with Innovation 12

- Consumers Have Data Security Concerns – and Video Can Help
- Delivering on Secure Video Biometrics: Best Practices

Smart Access Strategy: Video ROI 14

About Xailient 15

About Parks Associates 15



Next-Gen Access: Convenient, Smarter, More Secure

Smart video devices are hot, driving significant demand in the market due to their cutting-edge technological capabilities and innovative features that consumers value and are willing to invest in.

Cameras and video doorbells are the most adopted smart home devices, and adoption of both devices has more than doubled in the past five years.

- 22% of US internet households now own a video doorbell, and one in five own a smart camera.
- The average number of smart cameras and/or smart video doorbells is 2.21 per household, and strong market potential remains for both products.
- 30% of households in the US, almost 34 million households, have one of these devices.

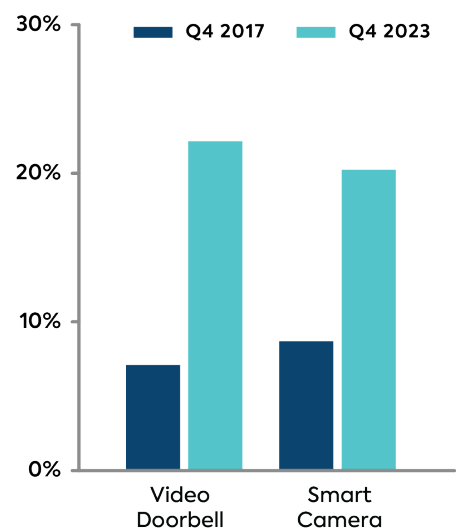
Consumers want to monitor what's happening in and around the home, and better context about who is coming to and into the home. Access control leaders in locks, garage doors, security systems, and even intercom systems at multifamily properties are experimenting with models that incorporate video to satisfy consumer demand.

In addition to providing value through the experience, this expansion creates new revenue opportunities.

Parks Associates estimates that smart video devices generated \$1.3B in stand-alone service revenues (that is, exclusive of security system-related revenues) and projects service revenue will grow to \$2.4B by 2027.

Biometrics are at the forefront of emerging features that differentiate brands and model offerings. By leveraging unique physiological and behavioral characteristics, biometric systems offer enhanced security, convenience, and personalization, setting new benchmarks for modern security solutions.

Smart Video Device Ownership



© Parks Associates

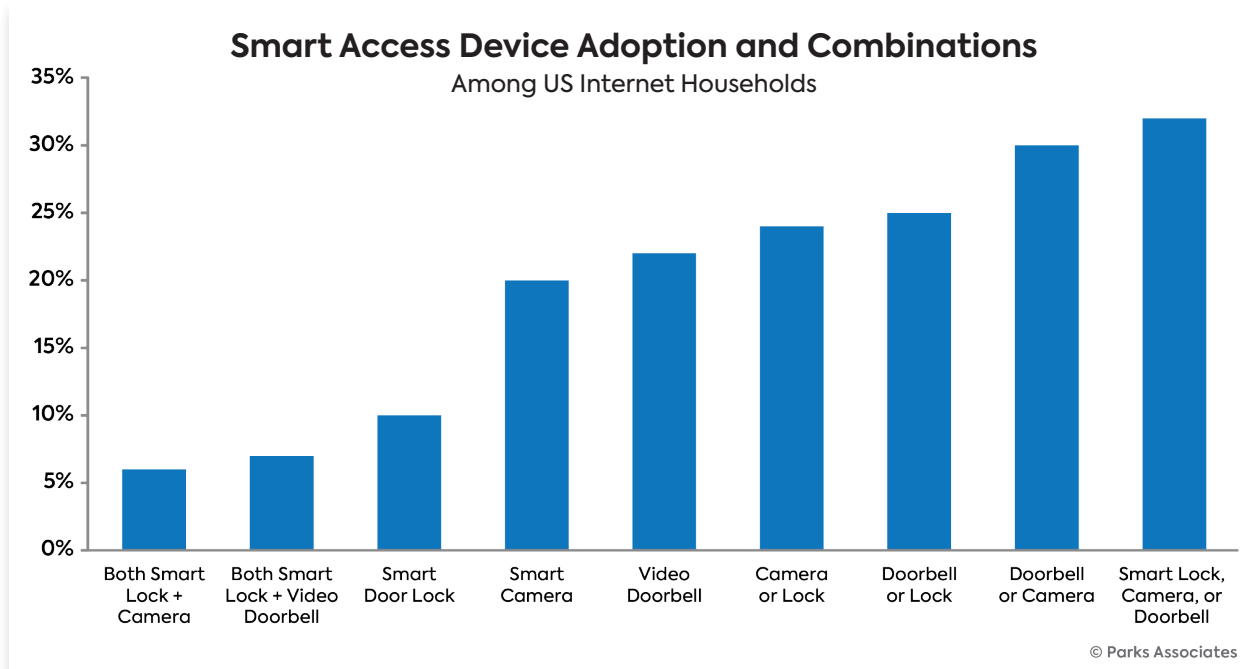
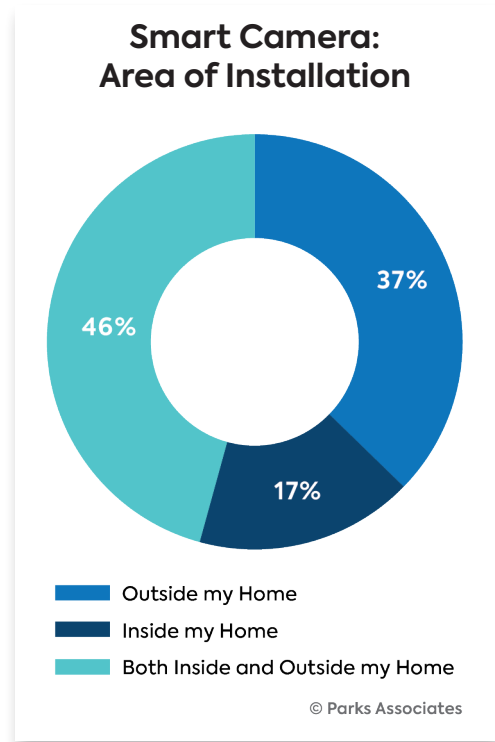
Consumers Want Video at the Door

The rising adoption of smart cameras is an extension of the demand for peace of mind traditionally provided by a security system. Where door and window sensors can detect intrusion into the home, cameras extend the home's perimeter out, often to the very edge of the property and beyond. Accordingly, most smart cameras are external: 83% of smart cameras owners have external cameras.

The most common areas monitored are access areas: the front entryway, front yard, driveway, and backdoor.

Consumer demand for convenient and secure access to the home has resulted in a growing uptake of smart access devices. Now, 32% of US internet households own a smart camera, video doorbell, or smart lock, and millions more are investing in two or more of these smart access technologies. **For instance, roughly eight million US internet households own both a video doorbell and a smart lock.**

There is great potential for combining functionality, and video devices are proliferating beyond cameras and video doorbells. Manufacturers are integrating video into other form factors on the exterior of the home, including flood lights, door locks, garage control systems, and vehicle dashboards.

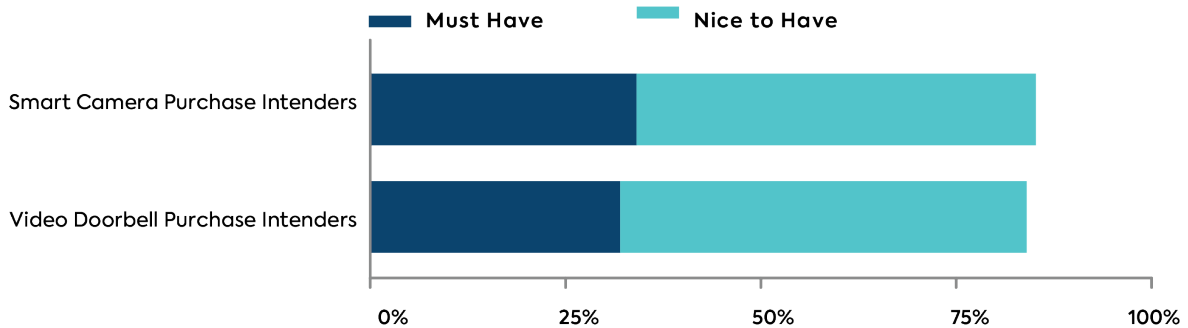


Consumers Want to Know Who is at the Door

Video provides situational context around who is at the door and why. Video analytics are widely used today to detect motion and distinguish meaning from noise, discriminating between moving objects like cars, tree branches, animals and humans. Facial recognition can further determine household members from unknown persons, creating a step change in value for alarm event verification. With integrated video-lock capabilities, users can grant entrance to the right people at the right time.

84% of smart video doorbell purchase intenders and 85% of smart camera purchase intenders want the product they purchase to have AI with facial recognition to identify family and friends; one-third rated it a “must have.”

Interest in AI with Facial Recognition to Identify Friends and Family



© Parks Associates



Consumers Want Convenience at the Door

Beyond safety and security, consumers also expect added convenience from their smart home devices. Core convenience features for access control include granting entry remotely using the associated smart phone app, receiving alerts when a door is left unlocked, and doors sensing authorized presence and granting hands-free entry.

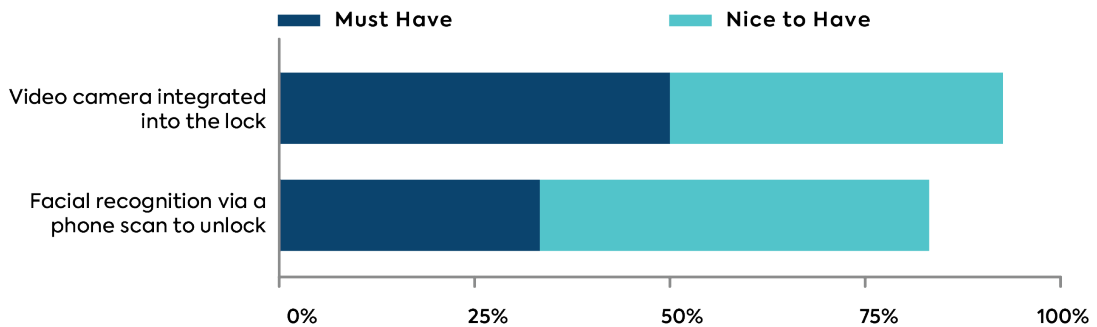
With video capabilities, facial recognition can support key-free and hands-free entry. Those in the market for smart door locks find the capability appealing.

93% of smart door lock purchase intenders want video integrated into the lock with their next door lock purchase – 50% rated it a “must have.”

83% of smart door lock purchase intenders want Face Unlock on their next door lock purchase – 33% rated it a “must have.”

Face unlock is a new advancement in convenience for locks but has been included in phones and tablets for more than five years. Face ID launched with the iPhone X in 2017, and Samsung and Google both offer face unlock on recent smartphone models. As consumers grow more comfortable with using facial recognition as an authentication and “unlocking” mechanism on their smartphone, smart device manufacturers need to be prepared for consumers to raise their expectations of receiving similar convenience in other product categories.

Preferred Features for Future Smart Door Lock Purchase



© Parks Associates





Competitive Drive to Keep Innovating

The smart lock space is dominated by large diversified global companies, but startups are putting pressure on the door lock giants. All smart lock providers offer core features of remote connectivity, unique codes for guests, and integration with key smart home platforms. Manufacturers seek premium features, form factors, and services that differentiate them from the competition and earn a premium price point.

Differentiate Product Tiers with Biometrics

Biometrics are established in the market as a premium feature today. Many leading brands, including Schlage, Yale, Kwikset, and August, have at least one model offering fingerprint unlock. Several more now offer video-based unlocking using one of several facial recognition methods:



Integrated video

A camera is integrated directly into the lock.



Smartphone face unlock

The user authenticates via facial recognition on their phone to trigger the door to unlock.












Routines with video devices

A video doorbell or external camera authenticates the user via facial recognition, communicating to the lock to open.

As of Q2 2024, Eufy and Lockly are early to market with locks featuring integrated cameras, and Yale offers European models with this functionality. In the US, Yale and August both offer facial recognition capabilities through smart phone face unlock.

More and more video device manufacturers are enabling facial recognition. Nest offers Familiar Face detection as part of its Nest Aware subscription that alerts users if unrecognized faces are detected. Smart home security provider Abode offers the Abode Edge camera that can distinguish between normal family activity and strangers on the premises.

Keyless Entry Methods – Leading Smart Lock Brands

									
Keypad	●	●	●	●	●	●	●	●	●
Wireless Sensing (Bluetooth, Wi-Fi, NFC)	●	●	●	●	●	●	●	●	●
Voice command voice assistant support	●	●	●	●	●	●	●	●	●
Fingerprint	●	●	●	●	●	●	●	●	
Facial Recognition smartphone face unlock	●	●							
Facial Recognition integrated video			●	●					

Early generation smart access control features are quickly commoditizing, and biometrics and integrated video features are setting brands and models apart. These capabilities are also demanding price premiums, with video-enabled models setting the highest price premiums:

Price Premium for Biometrics-enabled Models



Aqara’s fingerprint-enabled smart lock is priced at \$189 versus \$149 for its lock without biometrics.



Eufy’s video smart lock is \$349 compared to its \$99 base model.



Lockly’s Vision model is \$399, compared with its fingerprint-only models starting at \$139¹.

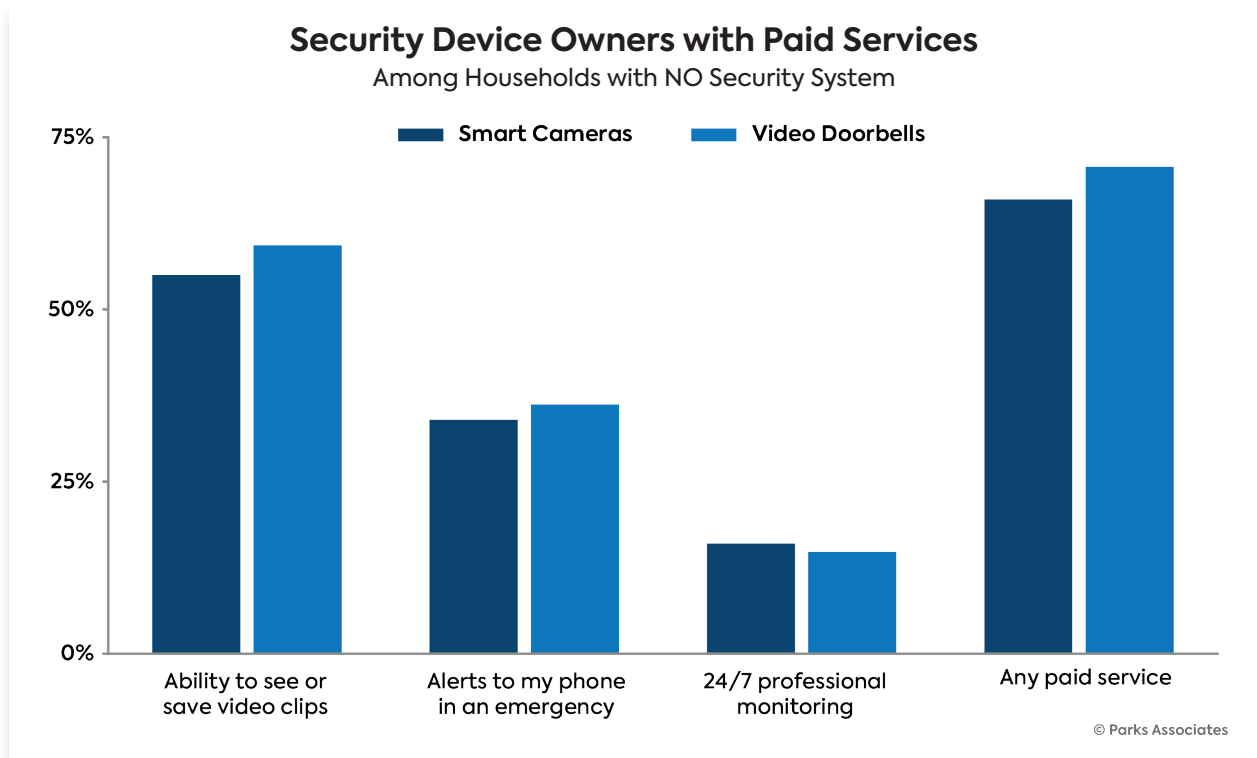
¹ All pricing as of June 2024.

Generate Service Revenue with Video

In addition to its ability to drive higher hardware revenues, integrated video services can add a recurring monthly fee for smart lock OEMs.

Generate annual service revenues: On average, smart camera and video doorbell owners pay between \$8 and \$16 per month, depending on the service received (video storage, self-monitoring, professional monitoring). With similar service options, lock brands can generate recurring revenue of \$120+/user annually.

Video attach rates are growing: 71% of video doorbell owners paid a monthly fee for alerts, monitoring or video storage in 2023, up from 62% the year prior. Service attach rates also rose for smart cameras, where 66% of owners report paying a monthly service fee, up from 51% in 2022.



Today, smart lock manufacturers may look to integrate with other camera/doorbell providers, but associated service revenues would accrue to the video platform provider. With an integrated camera, smart lock OEMs have the basis for a DIY security solution that could layer on professional monitoring services.

Parks Associates estimates \$13 billion in annual revenues for professional monitoring of residential security systems and video devices by 2025.

Going forward, we project the strongest growth for professional monitoring of stand-alone devices like video doorbells and cameras.

Service subscriptions also strengthen the relationship between the device manufacturer and the consumer.

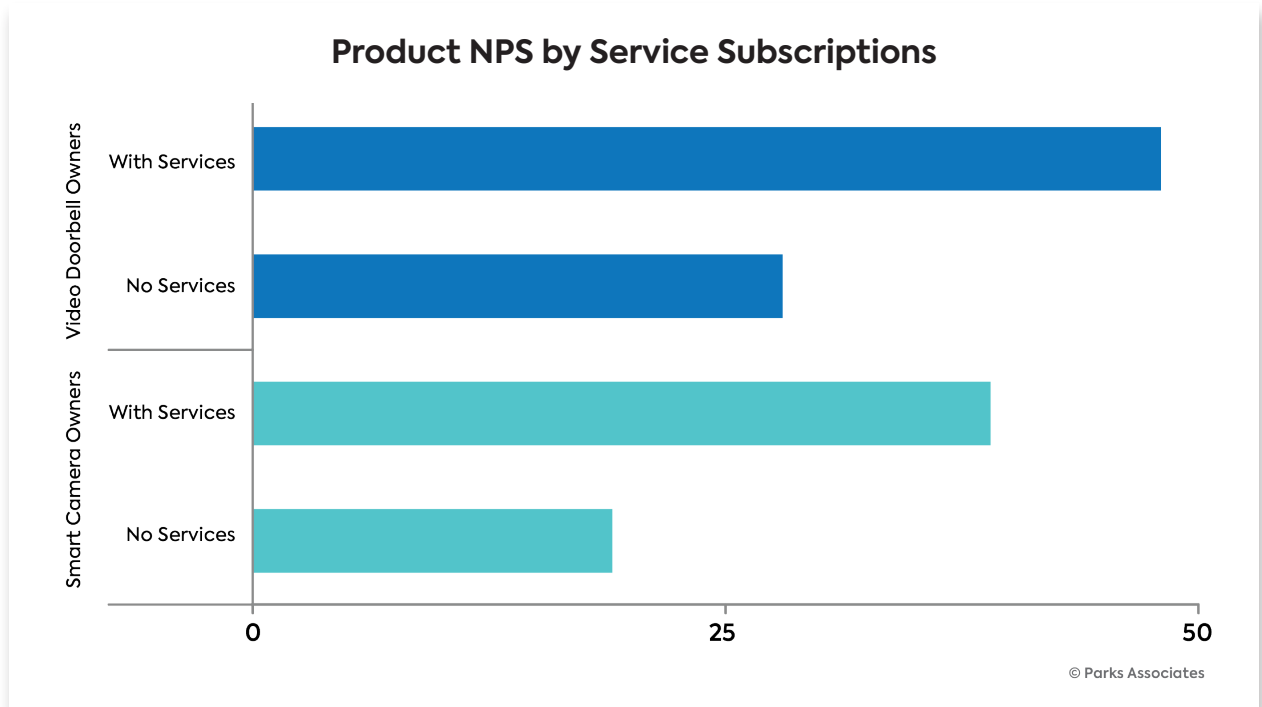
Retain customers

Professional security services typically retain ~85% of their subscribers year-over-year.

Improve customer satisfaction and create product evangelizers

Smart device owners with attached services give their devices higher Net Promoter Scores.

Most smart lock OEMs carry the cloud and support costs of the smart model over its lifetime, charging no additional fees for basic connected functionality today. Video opens a pathway to a recurring revenue model, and a driver for customer retention and brand loyalty at the next purchase.





Video-based Access: Balancing Privacy with Innovation

Consumers Have Data Security Concerns – and Video Can Help

Consumers have cybersecurity concerns about their smart locks—65% of smart door lock owners have privacy and cybersecurity concerns about their devices, making smart locks the #1 smart devices about which users have such concerns, followed by interior cameras and smartphones.

While the greatest vulnerability for any IoT device is likely to be theft of data or using the device as one in a network of compromised devices for a Distributed-denial-of-service (DDOS) attack against another party, consumers may perceive that a smart lock makes them vulnerable to burglars who hack the lock to gain entry to the home. In this scenario, integrating external video could assuage concerns by sending alerts if unknown persons approached the home, sounding an alarm for deterrence, and capturing evidence of a break-in.

Smart home device owners are more comfortable sharing outdoor video data than any other type of data generated by smart devices. Other data that consumers are particularly willing to share also revolve around peace of mind – emergency data and safety data.

50% of smart home device owners say they are comfortable sharing outdoor video with device manufacturers or service providers.

Data Types Smart Home Device Owners are Most Comfortable Sharing with OEMs/Service Providers

-  Outdoor Video
-  Emergency Data
-  Safety Data
-  Air Quality
-  Home Damage Detection

© Parks Associates

Delivering on Secure Video Biometrics: Best Practices

Privacy rules make video-based access complicated, but manufacturers can take steps to both deliver the video-based features consumers want and be mindful of their privacy.

Industry best practices:

- Minimize data collection
- Process and store data that is collected on the edge
- Provide consent management features to put consumers in control
- Provide an audit trail

Consumers echo these practices when sharing their expectations. Consumers consistently report three measures that would most assuage their privacy/data security concerns about smart products are by 1) giving them the ability to erase all collected data, 2) approve/rescind who has access to the data, and 3) decide which types of data will be collected. Additionally, 26% of internet households ranked storing data on the edge among their top 3 ways to overcome their concerns. This rises to 30%+ of smart home device owners.

Following industry best practices and moving to edge compute to minimize data transfer can balance the innovation the customers want with the security practices they demand.



Premises Secured. Privacy Secured.

Xailient's Privacy-safe AI enables face recognition at the edge with ethically sourced data, bias mitigation and governance.



On Device Matching

Face matching & identification occurs only on users' devices, not on servers



User Protection

Users choose whether to enable face recognition through easy-to-use settings



Stranger Protection

Only a preset group of people are identified - never strangers



Auditing & Improvement

System is audited to prevent bias & ensure accuracy



Distributed Architecture

Information is distributed across devices so face templates and identities are not stored together



Control Dashboard

Privacy settings are adjustable based on your jurisdiction

Available as SDKs, integrated modules, via API, or complete systems. Learn more at xailient.com



Smart Access Strategy: Video ROI

Access control brands employ three main strategies across their product portfolios to see the return on their investment in connected products.

- **Basic smart models** – some of the features that were differentiators yesterday are common to all smart lock brands today, including app-based control, wireless hands-free entry, personalized codes, and even voice integrations. Basic smart models will continue to see increasing commoditization; brands at this tier will compete on price and lean on channel partners to move high volumes.
- **Premium model innovation** – brands continue to invest in next-generation features to set premium tier products apart. Features such as video integration and biometric unlock increase purchase price, differentiate products from value-tier models, and create a foundation for services.
- **Attached video services** – video subscriptions help brands monetize IoT costs. By creating great customer stickiness, they also increase the lifetime value of the customer and create brand loyalty for future purchases.

Access control brands have an opportunity to give consumers the context, convenience, and security they want at the front door with a single, multifunctional product, and open a new business line with recurring service revenue through video integration.

About Parks Associates



www.parksassociates.com
info@parksassociates.com
972.490.1113

Parks Associates, a woman-founded and certified business, is an internationally recognized market research and consulting company specializing in emerging consumer technology products and services. Founded in 1986, Parks Associates creates research capital for companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, workshops, executive conferences, and annual service subscriptions.

The company's expertise includes new media, digital entertainment and gaming, home networks, internet and television services, digital health, mobile applications and services, consumer apps, advanced advertising, consumer electronics, energy management, and home control systems and security.

About Xailient



Xailient's computer vision AI for Edge devices enables innovators to bring their visions to life.

Our software solutions allow companies to deploy Face Recognition and detection features for continuous monitoring and updating while always ensuring privacy-safe data collection.

Xailient's software products run on exceptionally low power and make embedded Edge Computer Vision accurate, real-time, and cost-effective, solving the most difficult problems in the Enterprise CV lifecycle.

About the Author



Jennifer Kent, Vice President, Research, Parks Associates

Jennifer manages the research department and Parks Associates' process for producing high-quality, relevant, and meaningful research. Jennifer also leads and advises on syndicated and custom research projects across all connected consumer verticals and guides questionnaire development for Parks Associates' extensive consumer analytics survey program. Jennifer is a certified focus group moderator, with training from the Burke Institute.

Jennifer earned her PhD in religion, politics, and society and an MA in church-state studies from Baylor University. She earned her BA in politics from the Catholic University of America in Washington, DC.

ATTRIBUTION

Authored by Jennifer Kent. Published by Parks Associates. © Parks Associates, Addison, Texas 75001. All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher. Printed in the United States of America.

DISCLAIMER

Parks Associates has made every reasonable effort to ensure that all information in this report is correct. We assume no responsibility for any inadvertent errors.

RESEARCH & ANALYSIS

for Emerging Consumer Technologies

With over 35 years of experience, Parks Associates is committed to helping our clients with reliable and insightful consumer and industry research.



Entertainment & Video Services



Digital Media and Platforms



Home Networks



Digital Health



Support Services



Smart Home Devices and Platforms



Consumer Electronics



Energy Management



Home Control Systems



Home Security