

---

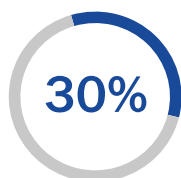
# Automatically Monitor CCTV Cameras

In Under Four Hours

White Paper

ARGENT

## Introduction

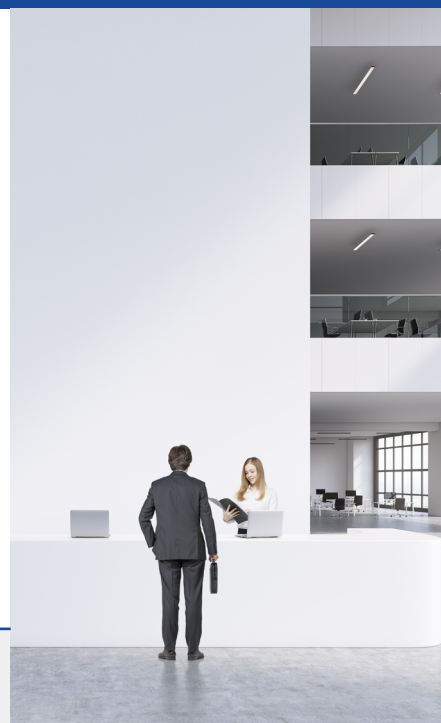


Industry researcher IHS Markit expects the number of cameras used for surveillance to rise above one billion by the end of 2021, marking an almost 30% increase over the 770 million such cameras in December 2019.

Putting aside the endless debate between security and privacy, **CCTV cameras are ubiquitous and will continue to be that way.**



Read the full article here: [Source Link](#)





## There Is No Lack of Headlines About Compromised Surveillance Systems

Thursday, 28 Dec 2017 - The Washington Post

*“... hackers took over two-thirds of the District’s outdoor surveillance cameras just before President Trump’s inauguration, according to a federal criminal complaint unsealed ...”*

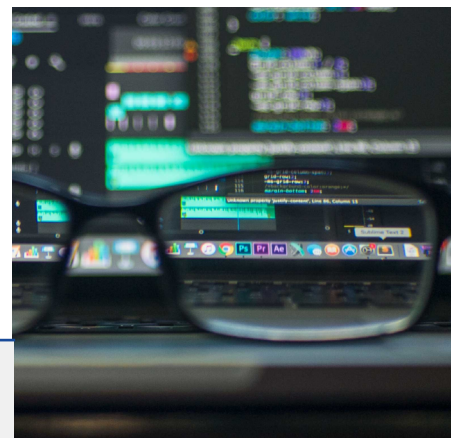
*“... attack affected 123 of the D.C. police department’s 187 outdoor surveillance cameras, leaving them unable to record for several days...”*



Read the full article here: [Source Link](#)

Monday, 7 May 2018 – The Japan Times

*“More than 60 security cameras made by Canon Inc. have been hacked and rendered unusable at places including key waterways...”*



Read the full article here: [Source Link](#)

Wednesday, 24 November 2021 – UK Government

*“In 2016, malicious actors hacked into 300,000 products such as routers and smart cameras, as part of the ‘Mirai’ attack and used the products’ collective computing power to attack major internet platforms and services, leaving much of the US East Coast without internet.”*



Read the full article here: [Source Link](#)



## Enable And Maintain Full Visibility On Your Surveillance System

What is your surveillance system’s topology?

---

How many cameras and NVRs are online today?

---

Any offline surveillance endpoint? If so, When and How often?

---

Any repeated Failed Logon Attempts to your surveillance system management console?

---

When was the last health check on system log?



**If you are unsure about any two of the above questions, perhaps it is time to rethink and act proactively.**



## Network Fortification Starts With Learning Network Topology

Surveillance systems very often operate on an isolated network, such as a network in a different vLAN, subnet, or IP range.

However, there will be circumstances where a surveillance system operates directly on the corporate network.

Visualizing network topology and generating a complete network device register list will be the first steps of the review process.



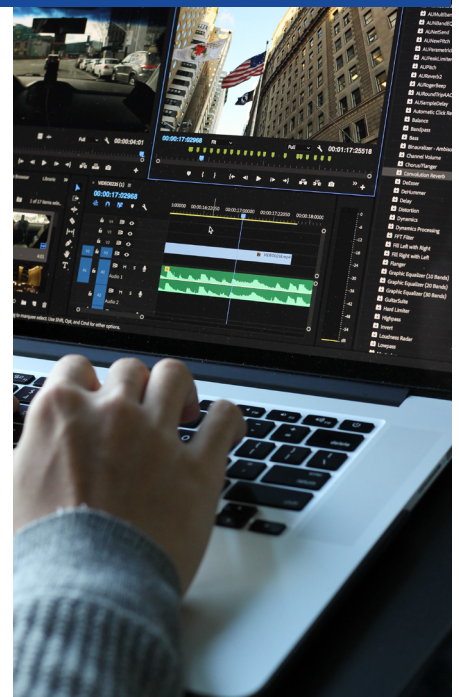
## “In The List” Is Different From Operational

From the headlines above, we learned that downtime of CCTV cameras is often not immediately noticed, often for days.

Not every business has at least one guard watching the screens 24/7, if they are on duty.

The next challenge we face is SLA reporting. Marking downtime manually for each camera simply does not sound practical in most cases.

For public venues, such as stadiums, galleries, and exhibition centers, assurance for public safety is not negotiable and thus full visibility and functioning surveillance system is mandatory.





## In Depth Surveillance System Review And Log Archiving

**Sophisticated surveillance systems typically support system log for critical events such as:**

Hard Disk Failure  
Administrative Logon  
Failed Logons  
Offline endpoints

Repeated failed logons are just as alarming as an early warning on hardware failure.

Unfortunately, the events typically are “First-In-First-Out,” meaning the oldest event is deleted when the newest event is added.

Therefore, establishing a regular review routine on the system log provides valuable insight, **and maintains the information before it is lost.**





## The Financial Cost of Surveillance And GDPR

While some attacks to CCTV cameras were done just for laughs (such as the Canon headline event in 2018), such events can be very costly when, for example, they result failure to comply with government regulations, such as GDPR – The General Data Protection Regulation.

**Thursday, 25 November 2021 – IT Pro Portal**

*“In accordance with GDPR, all data forms capable of identifying specific individuals are required to be handled in a secure, transparent, ethical and lawful manner.”*

*“A lack of compliance can leave unsuspecting organizations open to severe punishments from data protection authorities responsible for enforcing regulatory data protection laws. For example, earlier this year, German computer electronics retailer Notebooksbilliger was handed a €10.4m GDPR fine over non-compliant video monitoring of its employees.”*



Read the full article here: [Source Link](#)





## A Successful Strategy Requires Proper Execution And Repeatable Processes

**In the IT industry, repeated manual routines can waste a valuable resource - your highly-skilled IT people.**

A modern and common approach is automation. The benefits are obvious and include:

Always On-time

Identical Execution

Programmatical For Scenario-Based Reaction

Instant Action



A major government agency that operates CCTV cameras for a state police department shared with us their successful story using Argent.

Argent Software - All Rights Protected

**We can automate this critical task for you**  
at no cost - in under four hours, just email us at:

**[MonitorMyCCTVs@Argent.com](mailto:MonitorMyCCTVs@Argent.com)**

