



THE AVIGILON HARDENED OPERATING SYSTEM: HOW CAN IT WORK FOR YOU?

Avigilon's secure ES product line and the AI NVR models include a new operating system designed by Avigilon to provide superior performance and simplify the deployment and management of video security systems.

The operating system is designed with three main objectives:

- To simplify management of all system components (e.g. PoE switch, RAID, NIC teaming¹ and VMS services) by converging management tools in a single pane of glass
- To utilize hardware resources most efficiently and achieve unprecedented performance on dedicated appliances
- To build a secure platform with focus on cyber security and data protection

¹ NIC Teaming available in early 2021

² Drive identification available in early 2021

STREAMLINED SYSTEM MANAGEMENT THROUGH A SINGLE PANE OF GLASS

Avigilon is introducing a new streamlined approach to management that allows all system settings to be managed from within Avigilon Control Center (ACC). System Integrators are no longer required to connect a KVM (keyboard, video monitor, mouse) switch to perform initial setup or maintenance. Deploying appliances and NVRs is as simple as unboxing, racking and connecting them to the security network. Any ACC Client on the network will automatically detect the newly installed systems, allowing remote secure deployment and maintenance.

Networking settings such as setting host IP addresses, DNS configuration, and NIC teaming¹ can all be set up via the ACC Client. Additionally, the storage system functions, reviewing RAID health status, identifying drives², ejecting a drive and performing consistency check on the array can also be accessed and performed from an ACC Client on the network.



MANAGING MANY APPLIANCES IN A DATACENTER OR DISTRIBUTED ENVIRONMENTS

AI NVR and ES appliances leverage Avigilon Cloud Services (ACS) to make managing any site easier, including remote and distributed sites. All hardware health status events can be monitored together via ACC and /or ACS Site Health, including CPU usage, drive health, fan health, temperature probes, and much more. Additionally hardware event statuses can be used to trigger rules and alarms within ACC to ensure you never miss a component failure.

The AI NVR dramatically simplifies managing updates for all your cameras, clients, recorders, VMS, and operating system, by packaging them all into a single firmware package. When you update your ES or AI NVR, it automatically pushes updates to your clients and cameras to ensure they get updated to the latest version. Additionally, these updates can be completed remotely from Avigilon Cloud Services allowing the latest update to be pushed directly from the cloud to your AI NVR without the need to connect to the local network.

UNPARALLELED PERFORMANCE

By building a platform intended for video management and analytics applications, we have been able to achieve unparalleled performance. Through a total system approach in design and cohesion between hardware and software development, a higher level of optimized of resources were achieved, allowing ES appliances

and AI NVRs to deliver exceptional performance that can support even the most high bandwidth cameras, while drastically simplifying the deployment process. For example, load balancing the network traffic between NICs is no longer required when using these systems as they are able to ingest much higher throughput per port.

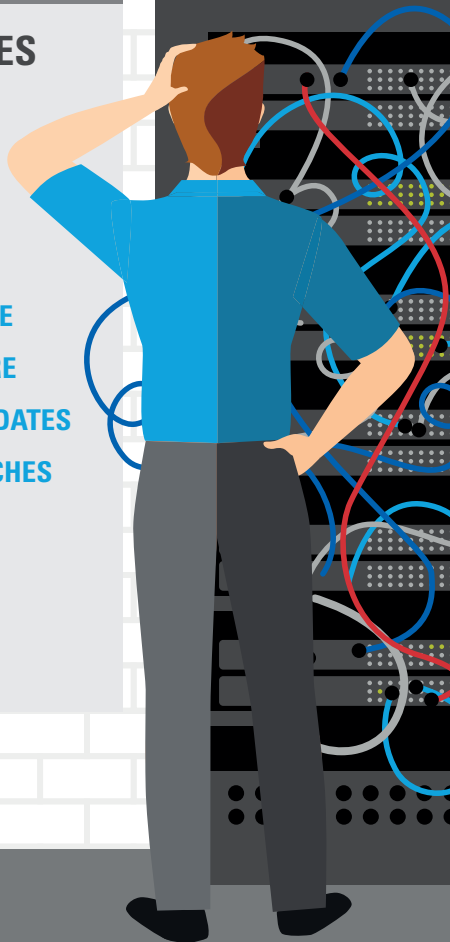
BEFORE: USING TRADITIONAL NETWORK VIDEO RECORDERS



WASTED MAN HOURS ACROSS DIFFERENT DEPARTMENTS

INDIVIDUAL FILES TO MANAGE

- FIRMWARE FOR COMPONENTS (I.E., GRAPHICS CARD)
- VMS UPDATES
- ANALYTICS SERVICE
- CAMERA FIRMWARE
- O/S UPGRADES/UPDATES
- O/S SECURITY PATCHES
- ACC SERVER
- ACC CLIENT
- FIREWALL



AFTER: USING THE AVIGILON HARDENED AI NVR



FAST, EFFICIENT AND MANAGEABLE PROCESS

ONE FILE DOES THE JOB FOR YOU

- SINGLE UPGRADE PACKAGE KEEPS YOUR WHOLE SITE UP TO DATE



SECURE REMOTE ACCESS





BUILDING A CYBER SECURE PLATFORM

Cyber security is built into the foundations of AI NVR and ES Appliances. They are all pre-hardened to ensure network ports required for Avigilon Services are opened, and remote access is disabled and locked. These systems use a signed trust chain during boot and while active, yet ensure no components can be altered while the system is off. Additionally, all USB ports are disabled to ensure no data can be injected or removed from the NVR. Lastly, all systems have an encrypted OS drive and all firmware updates are signed and encrypted by Avigilon before distribution to ensure system integrity. Avigilon puts every release through rigorous penetration testing routines with 3rd party tools before public release.

As a purpose-built video security-hardened NVR, this cost-effective, turnkey appliance bridges high performance with exceptional system deployment and management simplicity. From its hardened embedded OS and cybersecure design foundations to its cloud-ready remote update capabilities using just a singular firmware package to update all system components, this appliance is an IT-friendly solution that is poised to redefine the way security and IT teams approach video security deployments.

To learn more about the Avigilon Hardened Operating System, [get in touch](#).



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](https://www.motorolasolutions.com)

MOTOROLA, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2020 Motorola Solutions, Inc. All rights reserved. Specifications are subject to change without notice 11-2020