BADDAS

VIDEO SURVEILLANCE SYSTEMS ARE SUPPOSED TO PROTECT YOU FROM SERIOUS RISK, NOT EXPOSE YOU TO IT.

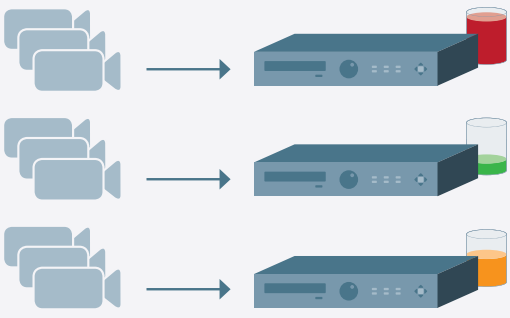
Are you still recording video like it's 1999?

Remember your very first cell phone with a camera? Today, with the proliferation of smart phone technology, would you bring this obsolete device to snap and send photos and videos of your latest vacation to your family and friends? Certainly not, so why use an outdated, highly ineffective, underperforming and unreliable technology to capture, protect and enable performance for your video surveillance system?

IT departments stopped using direct attached storage (DAS) in the 1990s, and moved to virtualized servers and shared storage solutions (SAN). Yet many organizations in the security industry continue to rely on DAS-based NVRs to host increasingly sophisticated video surveillance implementations.

This is your wake up call. Here are the five reasons why systems that continue to leverage DAS are putting your entire organization at risk.

LIMITATIONS OF DAS



Storage capacity is fixed and limited to each physical NVR, resulting in inconsistent retention times and unreliable data protection

5 REASONS WHY DAS IS BAD

5 POOR MANAGEABILITY

All NVRs must be managed as individual systems, a very manual and time consuming process. IT departments require that all systems are managed and monitored in one simple, centralized manner. NVRs do not comply with this approach, leading IT departments to often ignore them and prevent them from getting necessary maintenance and administration. This leads to the all-too-familiar and common problem of systems that underperform and fail without the end users' knowledge – until it's too late.

4 POOR EFFICIENCY AND SCALABILITY

Video needs change constantly, but NVRs are fixed and unable to scale to meet those needs. They are limited to the resources inside the physical box, leading to highly inefficient utilization – stranded islands of compute, storage and bandwidth capacity. As technology and budgets change, systems must scale ALL resources simultaneously. Adding another NVR simply inserts another stand-alone system, which does nothing to help existing systems and requires disruptive, time consuming administration and rebalancing.

3 POOR PERFORMANCE

Video surveillance is a very challenging write-intensive workload, and despite claims to the contrary NVRs are NOT designed or optimized to capture video without loss. NVR hardware is fundamentally designed for read-intensive applications. Because video data is so highly variable and unpredictable, NVRs must be wildly overprovisioned to plan for the worst case. They can perform adequately in small systems during ideal conditions, but performance will suffer greatly during spikes of video data and degraded system operations (disk or appliance failures and rebuilds). This makes them highly prone to dropped video frames, leading to video loss and image degradation.

2 POOR FAULT TOLERANCE

The amount of data generated by IP video systems doubles roughly every 18 months, and hard disks storing that data are 3x more likely to fail than those used in non-video applications. RAID technology developed in the 1970's is no longer sufficient for protecting against the increased likelihood of multiple simultaneous failures, exposing systems to permanent data loss and severely limited performance during extremely long disk rebuilds.

1 SINGLE POINTS OF FAILURE

Appliance or component failures prevent access to live and recorded video, halt recording and often result in permanent data loss. VMS failover only partially solves these problems, offering no protection for previously recorded video or integrated applications and requiring costly redundant hardware, software and licensing.

The days of NVR are numbered.

Click here to find out how you can avoid the pitfalls of a badDAS.

Pivot3