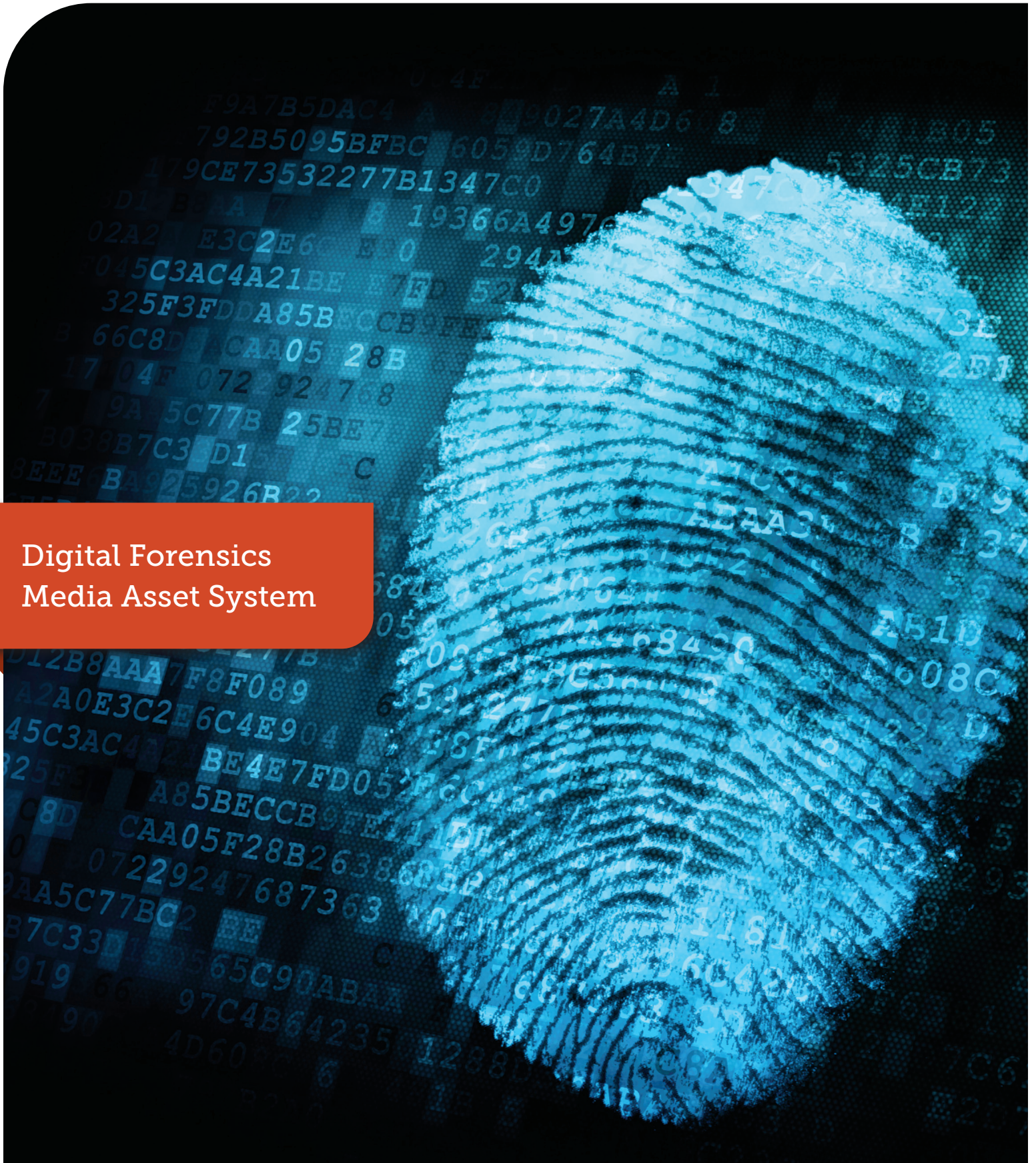


Digital Forensics
Media Asset System



Highlights

KEY ADVANTAGES:

- High performance configuration allows direct access to data sets
- Scale-out architecture meets future needs and next generation exploitation
- Greatly improves workflows while supporting multiple analysis tools
- Data assets are protected and available
- Fully supported by Expert level services

SOLUTION HIGHLIGHTS:

- Full scope architected solution designed by Keeper Tech Experts
- Incorporates Quantum StorNext software with High Performance Storage
- Allows natively participating clients
- Preserves existing applications and compute infrastructure
- Pairs with virtual/sandbox environments
- Offers integrated continuous data protection to on-premises or cloud storage

Keeper Technology simplifies ingesting, sharing, and archiving data across experts and teams to boost productivity and accelerate time to insight.

We live in a digital world. Social media, email, cloud storage, local storage, personal computers, iPhones, etc. all contribute to the way we interact with our business associates, friends, and family. Criminals use these same capabilities but leverage them to skirt detection and break laws. As more criminals adopt a digital lifestyle, law enforcement needs mechanisms to stay ahead of them. This involves the creation of digital forensic laboratories where an ever-expanding cadre of forensic software tools

examine, correlate, and exploit vast troves of digital information in the possession of suspected terrorists or criminals. Keeping up with the voracious appetite of forensic software in terms of processing, memory, storage, and performance is a key architectural concern of forensic labs, both small and large. Finding the best technology solutions that also address concerns for access, management and protection of forensic media assets is also of paramount importance.

Key Challenges

As storage architects look to implement or expand existing NAS infrastructure, several potential problems become evident.

PROTECTION: After the original media is imaged into an operational system, these digital images must be secured from alteration as well as protected in the event of a system failure.

RECOVERY: If an image is somehow lost, creating a new digital image from the original physical device can be time consuming, expensive, and call into question any processing that occurred on the first digital image.

PREVENTION: Malware is always a threat when ingesting media. A virus breakout threatens all the investigations within a forensics lab, not just the one that introduced the virus. Intelligent use of sandboxing and virtual environments that can be thrown away and rebuilt instantaneously is critical.

COST EFFECTIVE CONFIGURATIONS: As the sophistication of forensic software programs increases, so does the need for cost-effective storage and processing architectures to match the needs of forensic software. Increased exploitation techniques require a combination of capability that are difficult to achieve within budget.

EFFICIENT SCALABILITY: High performance streaming combined with random access can strain storage systems. Machine Learning and Artificial Intelligence (AI/ML) tools often require specialized GPU or DPU systems to quickly analyze data sets. Creating an efficient architecture without simply throwing significant hardware at the problem is a challenge.



Solution Bundles

Each forensic use case has its own challenges with unique requirements driving the handling, processing, exploitation, and preservation of digital evidence. Keeper Technology provides scalable storage and processing architectures for forensic laboratories from a handful of analysts to hundreds of analysts.

Solution Bundle Featuring Quantum StorNext

Keeper knows that one size does not fit all, so we have created scalable solution bundles to support a wide range of unique environments. Built around StorNext, Keeper's forensic architecture solutions provide a consolidated, high-performance solution which securely optimizes the forensic workflow. Forensic workstations simultaneously access the same captured media images to perform unique analytics operations, from natural language programs to sophisticated ETL processes. Solution bundles start with Keeper Ingenuity combined with StorNext capability and proven, commodity hardware delivered in a turnkey bundle and then are scaled and optimized to meet your unique environment.

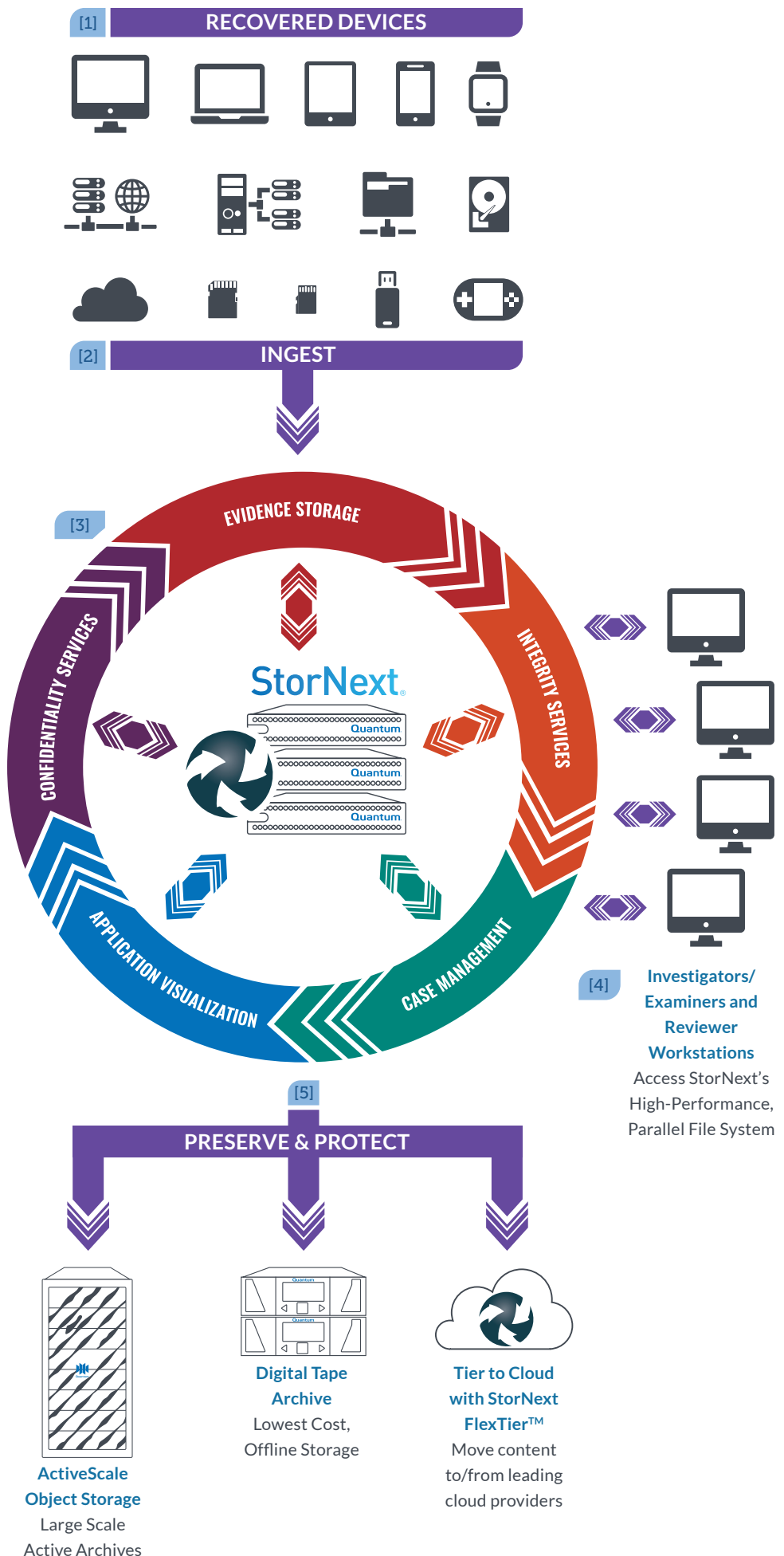
[1] A wide variety of devices are acquired to aid in an investigative process. Anything that stores digital information can be of interest to investigators and analysts.

[2] The original digital storage media is forensically imaged and stored into the high-performance shared storage environment utilizing hardware and software that is often unique to the device being imaged.

[3] StorNext provides a robust, shared data management environment for media images, scratch space, and analyst results.

[4] High performance storage is utilized by existing and future analyst software running on connected workstations and servers.

[5] StorNext ensures that case files are properly protected and archived to a variety of cost-effective local devices or to the cloud.



[4] **Investigators/Examiners and Reviewer Workstations**
 Access StorNext's High-Performance, Parallel File System



Scalable Core Hardware

Today's storage hardware does not have to be expensive to be capable and performant. Thanks to the commoditization of flash storage devices enabled by software defined storage, KeeperTech has created a core architecture that can start small (or large!) and grow with changing requirements and current technologies.

Access Considerations

The digital media assets are at the core of any forensic architecture, this solution evolves around the performant delivery of data to a variety of applications. Both open-source and commercial forensic applications run primarily in Windows and Linux operating system environments. Having a mix of operating systems typically drives the architecture towards a Network Attached Storage (NAS) solution using NAS protocols such as NFS or SMB/CIFS. NAS protocols are not well suited to high performance, mixed workload environments, causing forensic scientists to copy data back and forth from the NAS server, wasting time and effort.

The KeeperTech architecture leverages Quantum's StorNext File System (SNFS) to provide native, high-performance access to Windows, Linux, and Apple operating system environments. SNFS provides local-system performance over a high-speed Ethernet (or Infiniband) Network at data rates from 10 Gbit/s to 100's Gbit/s.

Protection

The StorNext software suite provides an optional add-on for ensuring that files stored in the file system are automatically protected according to customizable policies. Protecting individual files can happen as soon as they are stored, ensuring that your data loss exposure is at a minimum. StorNext also provides the widest array of support for secondary storage targets including on-premises NAS, object, and tape as well as cloud-based object.

Scaling Up and Out

There is a lot of marketing effort around trying to explain and promote scale-up and scale-out architectures. The bottom-line for customers, however, is a need to grow an existing environment easily, quickly, and cost-effectively without a lot of hassle. This is accomplished with KeeperTech's careful architecture at the core enabled by adaptable software to grow capacity and performance as well as add new client systems and dynamically insert innovative technologies.

Bring Your Own Clients

Odds are, there are existing forensic workstations that operate independently and are specially configured to perform certain tasks very well. There is no need to change or eliminate them – simply attach them to the high-performance network and mount the StorNext File System locally to gain all of the advantages of the core storage.

Optimizing Workflows

Often, an investigation requires many tools, multiple analysts with specialized skills, and a workflow of moving, copying, and sharing of data and information from one stage to the next. As target media grow from gigabytes to terabytes, the resulting delays of excess data movement can cause an unacceptable time to solution. The KeeperTech solutions optimize data workflows and ensure even the most complex investigation achieves the highest efficiency possible.

About Keeper Technology

For the past 17 years, Keeper Technology has been architecting, deploying, and supporting some of the largest forensic architectures for use in the US intelligence community. This vast experience working with high-velocity data analytics, ETL processing and workflow, and open-source architectures has led us to create a variety of turnkey, scalable solution bundles that are easy to deploy and support for the full range of requirements from a few forensic scientists to hundreds. As systems integrators, we bring together the best of commodity hardware, open-source projects, and commercial software to create uniquely repeatable capabilities for dynamic forensic systems.

21740 Beaumeade Circle
Suite 150, Ashburn, VA 20147

P [571] 333 2725 | F [703] 738 7231
solutions@keepertech.com

www.keepertech.com

Quantum[®]
EXPERT PARTNER