# Cloud Enabled Digital Forensics (DFaaS)

## Introduction and Objectives

### TACKLING DIGITAL INVESTIGATIONS.

VMware are looking to help address one of the biggest growing challenges for policing in the UK.

### KEY FACTS

- Utilising existing capabilities and COTS service, VMware will help clients connect to local forensic capabilities and to the Cloud enabled Digital Investigation services.
- The services can be accessed at a station, in a dedicated forensic vehicle, or an approved policing vehicle
- The services need to be available to all but be tailored to the individual's role and access privileges.

With every police investigation having a digital footprint there is a need to rethink how investigators interact with digital evidence. Coupled with a need to assess and share digital evidence quickly and securely there is a growing issue in how police sustain the challenges of exponential growth that digital assets create.

Currently for most officers the process to identify or forensically extract any potential evidence requires moving seized devices physically to locations where the tools, services and processes exist to engage with the device.

**This delays getting to the information they need for their investigation and ultimately affects the time they can spend focusing on the victim.**

With some forces having regional hubs for digital investigations, it can also be quite time consuming to get to the right services, too. With officers sometimes over an hour's journey from the capabilities they need to progress their work.

Technology has demonstrated that taking the office tools into the field is mainstream, the challenge for policing is making use of these capabilities to put the digital forensics capabilities into the hands of officers while they are in the community.

VMware are offering their experience and their capabilities to policing to address these issues.

This paper will set out how we plan to do this.

## Solution Overview

Insight shared, learned and seen by our teams has focused our attention to two scenarios;

- The triage of a volume of seized devices while out in a remote location
- The quick and selective assessment of a device preventing the need to take this device from a victim or a witness.

These scenarios will need to:

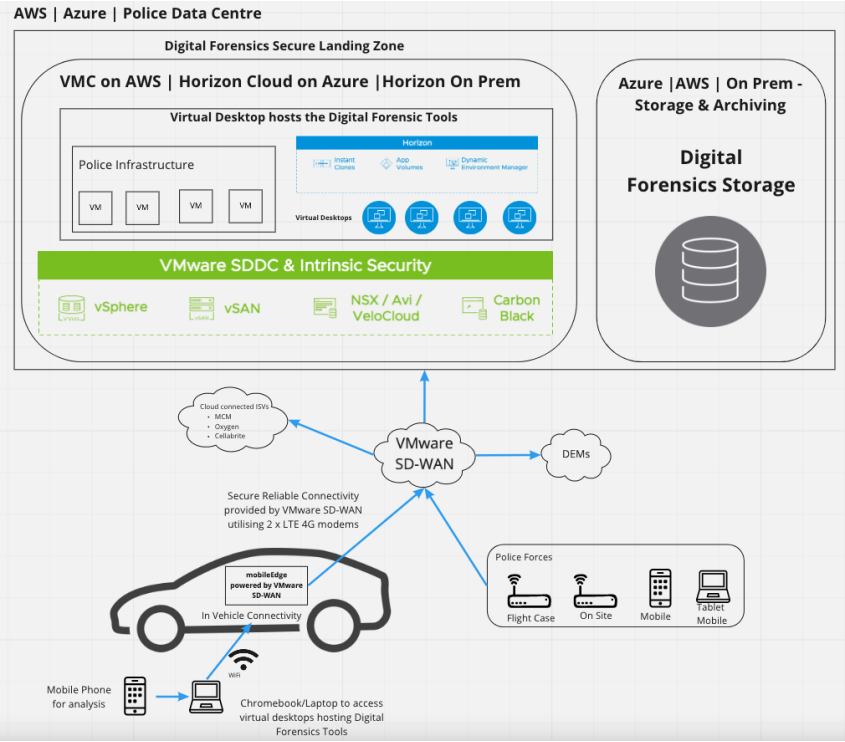
- Offer remote access to policing or cloud enabled forensic tools
- Offer end to end security and monitoring
- Work in the most extreme of environments
- Allow an officer or investigator to start workflows remotely allowing them to process devices while in transit
- Securely store any information and audit any changes to it
- Support Data Collection and transfer to central storage
- Provide secure access to data stored in the cloud
- Provide Role and identity management based on Digital Forensics Tasks
- Secure transfer of large amounts of data

- Provide bandwidth optimization and prioritization to prevent network issues arising from large data transfers
- Provide a secure platform that officers can work from to access Digital Forensics tools remotely
- Protect against malware and potential Anti-Forensics attacks

By placing Digital Forensics data in the cloud, the problems Police Forces face with the exponential growth of data are greatly reduced as storage can be consumed on demand whilst low-cost archiving solutions can be employed that scale and grow organically without the need to procure additional hardware and the real estate to host that hardware.

This brings about its own challenges and opportunities to transform how Digital Forensics is performed to meet the ever-growing demands in this area of policing. By leveraging its partnerships with the Cloud Hyperscalers VMware have come up with the below conceptual design bringing together market leading technologies.

"The Digital Forensics Secure Landing Zone can be accessed securely from anywhere – enabling officers to capture data and transfer securely whilst still in the field"




The solution consists of a Digital Forensics Secure Landing zone built on VMware technology to provide secure remote access to Digital Forensics tooling hosted either in the cloud or within Police Data Centers. The platform benefits from being able to be located adjacent to the Digital Forensics data regardless of which Cloud or Data Centre a Police Force chooses to use.

ANYWHERE WORKSPACE

- Delivers a convergent infrastructure that allows for connected visibility and context across all vectors, ensuring that security coverage is broader and more effective, following users, data, and apps wherever they are.

## Digital Forensics Secure Landing Zone

The Digital Forensics Secure Landing Zone provides a platform which can be accessed securely from anywhere it will;

- Facilitate the data acquisition process by securely redirecting USB connected devices such as a mobile phone enabling secure transmission of data from a laptop or thin client device located within the field.
- Provide a viewing platform to access, view and analyse digital forensics data
- Provide role-based access and identity management
- Prevent unsolicited network traffic from traversing the network
- Provide next generation Antivirus protection scanning for known and unknown threats utilizing Carbon Black

For Police forces to meet the needs of today's distributed workforce, they need a secure Digital Forensics solution that includes key elements of Unified Endpoint Management, Desktop and App Virtualization, Secure Access Service Edge, and Endpoint Security technologies.
VMware Anywhere Workspace delivers a convergent infrastructure that allows for connected visibility and context across all vectors, ensuring that security coverage is broader and more effective, following users, data, and apps wherever they are.

SECURE ACCESS SERVICE EDGE

- Secures and optimizes the network in order to handle bandwidth intensive data transfers whilst maintaining security

## Network & Security

There are a number of challenges that will need to be considered with network and security;

- The need to deal with bandwidth intensive processes when transmitting large amounts of Digital Forensic data to the cloud
- Provide secure access to Cloud resources from anywhere e.g. allowing a Police Officer to begin uploading potential evidence whilst still out in the field
- Prevent and detect malicious code from executing or communicating across the network.

The VMware SASE Platform is cloud-native secure access service edge platform that converges cloud networking and cloud security to deliver flexibility, agility, protection, and scale. The SASE Platform combines the cloud VMware SD-WAN Gateway, VMware Secure Access, VMware Cloud Web Security, and VMware NSX Cloud Firewall into one holistic solution.

The SASE Platform extends the security boundary beyond data center and cloud to applications and users, minimizing the attack surface, and protecting users, networks, applications, and data against threats. This underpins the proposed solution by providing assured connectivity and security for digital forensic assets from device to cloud, in rest and in transit.

VMWARE CLOUD

- Allows the Digital Forensics Platform to be accessed from anywhere and provides access to Digital Forensics tooling with proximity to data stored within any Cloud.

## VMware Cloud

The Digital Forensics Secure Landing Zone can be hosted within VMware Cloud either as an On-Premises instance or within Public Clouds AWS and Azure utilising VMware's partnerships with Amazon and Microsoft. This ensures that the workspace remains close to the Digital forensics data and processes regardless of where they reside. The platform allows for existing Police Digital Forensics toolsets to be hosted in the cloud and made accessible remotely as well as supporting future tooling either located on in the Cloud or with Third-Party providers.

VMware Cloud provides the compute, networking, and storage to host the Digital Forensics Secure Landing Zone alongside any existing supporting Police infrastructure services that can be easily migrated to the Hybrid Cloud platform. It will provide direct access Cloud storage and workflows for processing Digital Forensics data. Virtual Desktops allow for remote access to the Digital Forensics tools.

LEARN MORE

Anywhere Workspace;

*https://www.vmware.com/solutions/anywhere-workspace.html*

VMware Secure Access Service Edge SASE;

*https://www.vmware.com/products/secure-access-service-edge-sase.html*

VMware Cloud on AWS;

*https://www.vmware.com/products/vmc-on-aws.html*

Azure VMware Solutions;

*https://www.vmware.com/uk/partners/strategic-technology-partners/microsoft.html*

Horizon Cloud

*https://www.vmware.com/uk/products/horizon-cloud-virtual-desktops.html*

## Next Steps

VMware provide the building blocks and plumbing using market leading technologies to solve the challenges facing UK Police Forces enabling the critical role of Digital Forensics tools, by dealing with the exponential growth of digital assets and the data attributed to it. The Conceptual Solution described within this paper shows our thought process in how to go about dealing with these challenges.

In doing so we believe that Policing will be able to spend less time collecting and acquiring data from digital assets; allowing them more time to analyse as part of the investigation. Enabling them to focus on the victims of crime and reducing the time to conviction for criminals.

While this paper is positioned as a point of view, VMware has confidence that this will work, technologically. The underpinning capabilities exist today, and it is the insight, experience and appetite of our teams that have been able to put this capability together. With the challenges, policies and needs of policing in mind we feel we have the most comprehensive solution to the challenges police face when there is a need for forensic support for digital devices. Our idea is to reduce the intrusiveness for victims, by cutting down on the time spent in their digital lives and to support the challenges officers have by giving them access to the services that help them investigate incidents efficiently.

As we understand the status and capability of each police service is different, we will offer this as a modular solution to support and augment currently forensic capabilities and operating models.

**Field access:** If the limitation for the organisation is accessibility to the tools outside of the digital forensic locations, we can supply the service to deploy these out to field users.

**Demand Vs capacity:** If the challenge is demand on existing people and services then we can enhance your capabilities by allowing you to extend your local services out into the Cloud, allowing a greater range of storage capabilities, more compute power and flexibility for user locations

**Complexity, automation and innovation:** If you are struggling to keep up with the challenges faced by the pace of technology development and how to engage with the ever-growing range of devices then we can integrate you into a marketplace of capability, that you can draw on to tackle the investigations digital challenges.

If you are interested in how our capabilities could help your organisations needs, please contact one of our team

FOR MORE INFORMATION CONTACT ONE OF OUR TEAM:

*Joseph Langford* – Public Sector Chief Technologist, VMware

*Gavin Lees* – Lead Solutions Engineer, VMware

*Fleur Bamber* – Policing Account Executive, VMware