MAGNET FORENSICS®

Dig Deeper: Acquisition and Analysis of AWS Cloud Data

//Trey Amick & Curtis Mutter

Trey Amick

Manager, Forensic Consultants
Magnet Forensics, Inc.
trey.amick@magnetforensics.com

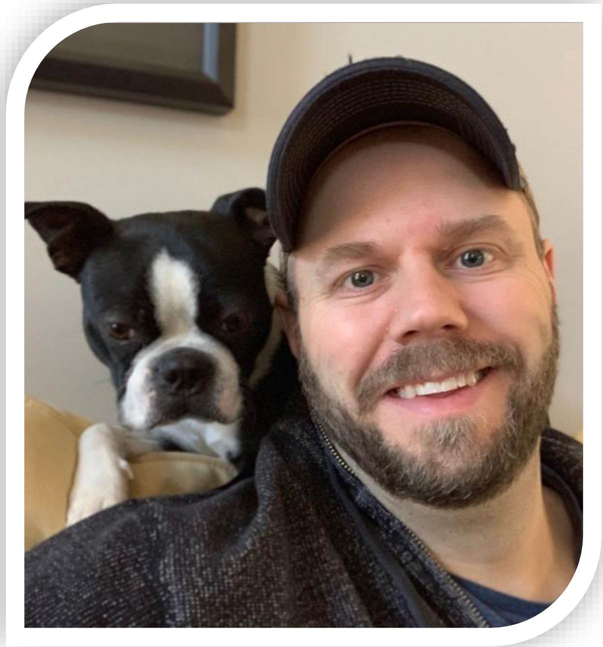
@amick_trey

Supervisor Sammy

- Joined Magnet in 2018
- Special Deputy US Marshal | USSS Electronic Crimes Task Force
- Detective Rock Hill Police Department | Professional Standards
- Capital One Technical Investigations | Education & Awareness Team
- Intelligence Contractor: Iraq
- Apple
- Photographer: Sr. Staff Writer Fstoppers.com

Curtis Mutter

- Senior Product Manager
  Magnet AXIOM Cloud and Mobile
  curtis.mutter@magnetforensics.com



- Joined Magnet in 2018
- 10+ years of Product Management experience across a variety of industries including Enterprise content management, and professional A/V

Agenda

- Using Cloud Data in modern investigations
- AWS: S3 / EC2
- Introduction to Magnet AXIOM Cyber
- Automation & Orchestration in the Cloud

MAGNET FORENSICS

Cyber Crime Trends

- Cyber attacks are the fastest growing crime. They’re increasing in frequency, size, complexity, and cost to the victim organization.

1 in 5 organizations lose more $1 million a year to fraud

70%

People who are bullied end up leaving their employer. Costs include retraining, and potential Wrongful Termination lawsuits

= +80%

IP can be +80% of a company’s total value and it’s at risk from outsiders and insiders alike

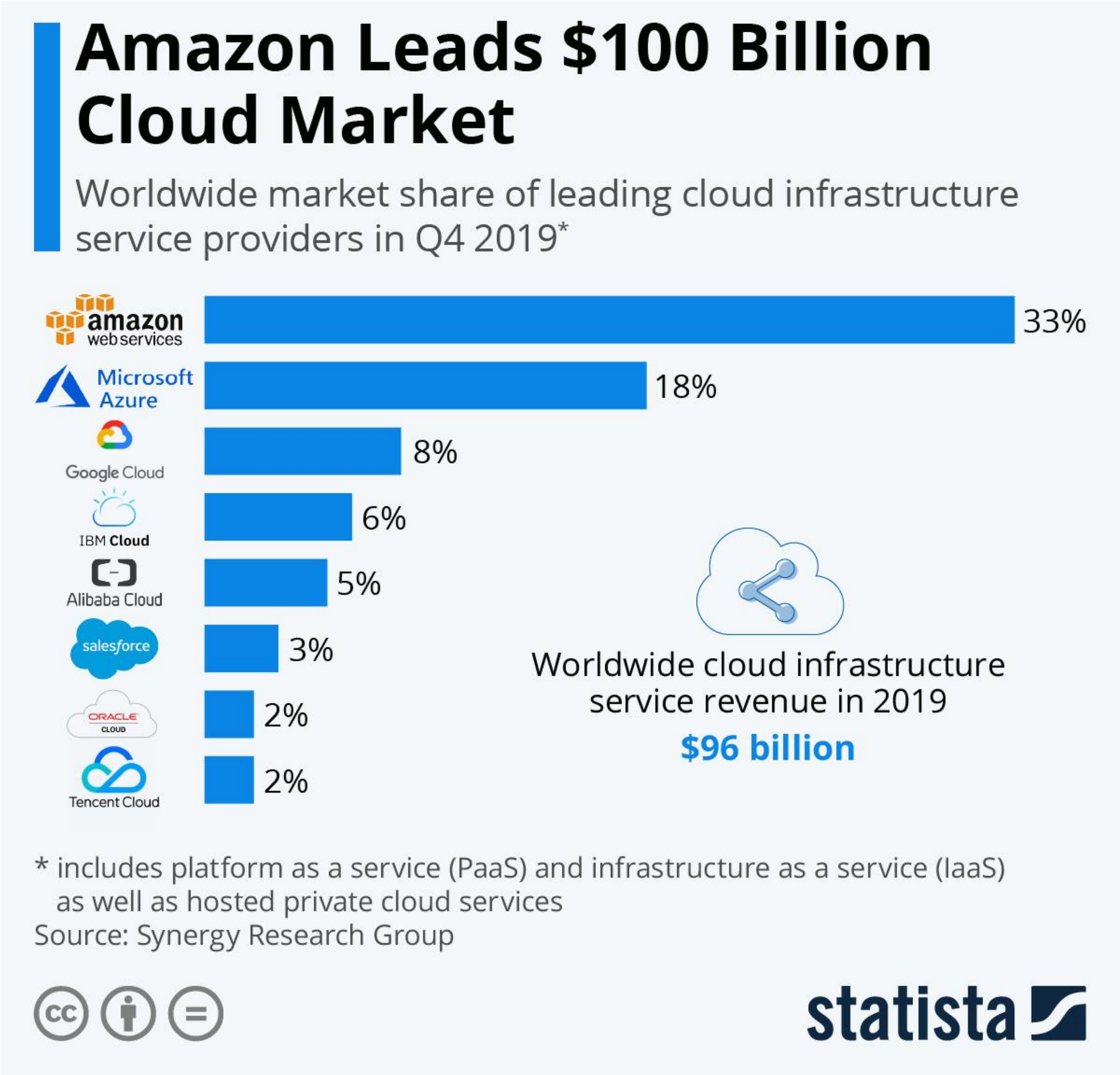
$3.92M

Average cost of a data breach in 2019

An average of +25k records are compromised at a cost of $150 each

Cloud Market Share

- Amazon Web Services and Microsoft Azure make up more than 50% of the Cloud IaaS / PaaS market
- Revenue set to far exceed $100 billion in 2020
- The 2019 market was more than double the size of 2017



Amazon Leads $100 Billion Cloud Market

Worldwide market share of leading cloud infrastructure service providers in Q4 2019*

Worldwide cloud infrastructure service revenue in 2019

$96 billion

* includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group

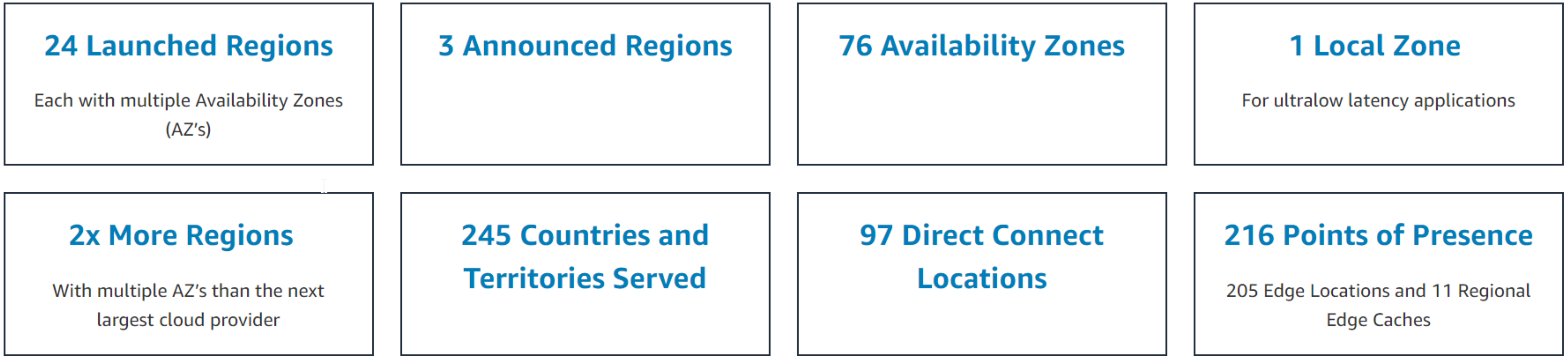
Amazon Web Services (AWS)

MAGNET FORENSICS®

AWS Infrastructure

Amazon has a vast and always growing infrastructure that is available around the world.

AWS Regions - a physical location around the world where data centers are clustered.
AWS Availability Zones – a group of logical data centers.
Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area.
Edge Locations - where end users access services **located** at **AWS**, the cloud computing division of US-headquartered Amazon. They are **located** in most of the major cities around the world and are specifically used by CloudFront (CDN) to distribute content to end users to reduce latency.



24 Launched Regions

Each with multiple Availability Zones (AZ's)

3 Announced Regions

76 Availability Zones

1 Local Zone

For ultralow latency applications

2x More Regions

With multiple AZ's than the next largest cloud provider

245 Countries and Territories Served

97 Direct Connect Locations

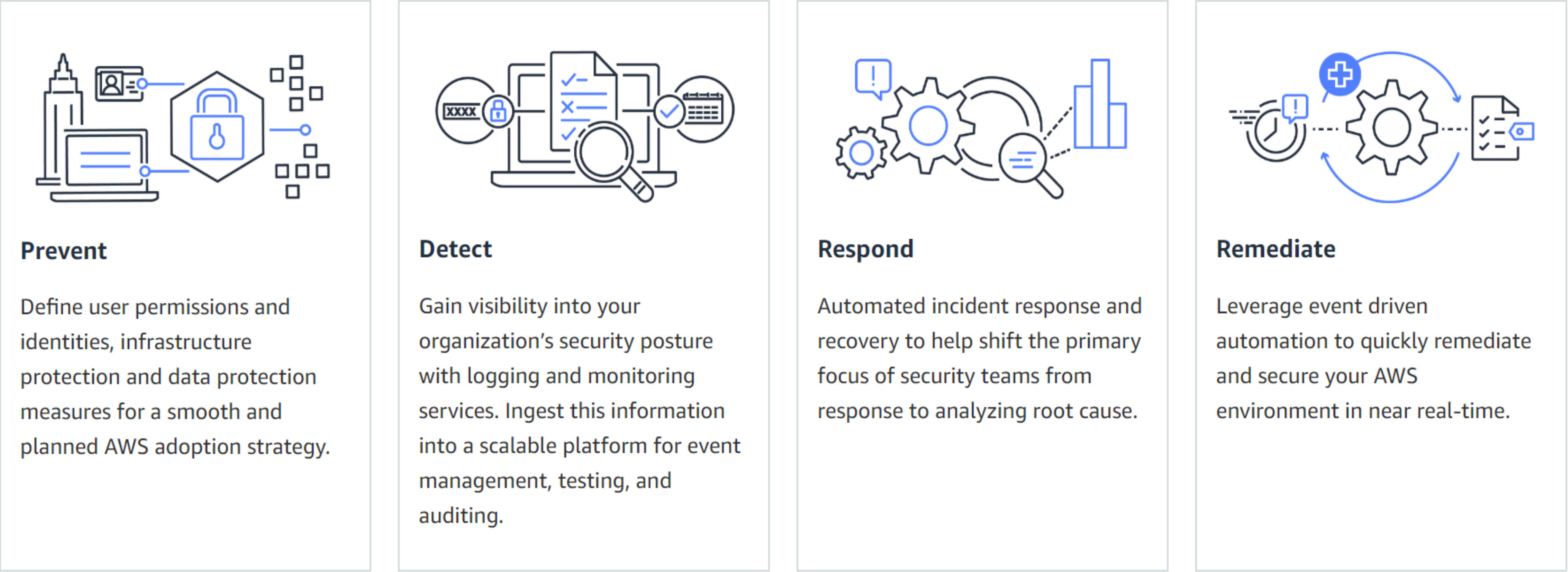
216 Points of Presence

205 Edge Locations and 11 Regional Edge Caches

AWS Security

Amazon offers a large variety of security focused services that allow all practitioners to ensure that whatever they create in AWS will be secure.

AWS provides services that help protect the data, accounts, and workloads created by its users, from unauthorized access. AWS data protection services provide encryption and key management and threat detection that continuously monitors and protects accounts and workloads.



Prevent

Define user permissions and identities, infrastructure protection and data protection measures for a smooth and planned AWS adoption strategy.

Detect

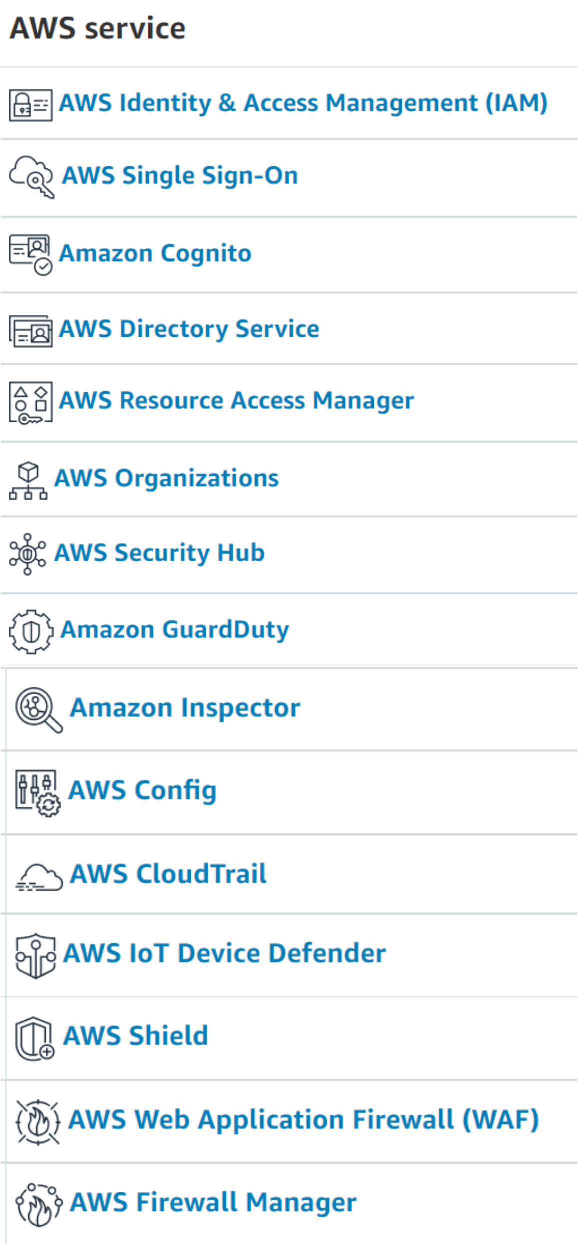
Gain visibility into your organization's security posture with logging and monitoring services. Ingest this information into a scalable platform for event management, testing, and auditing.

Respond

Automated incident response and recovery to help shift the primary focus of security teams from response to analyzing root cause.

Remediate

Leverage event driven automation to quickly remediate and secure your AWS environment in near real-time.



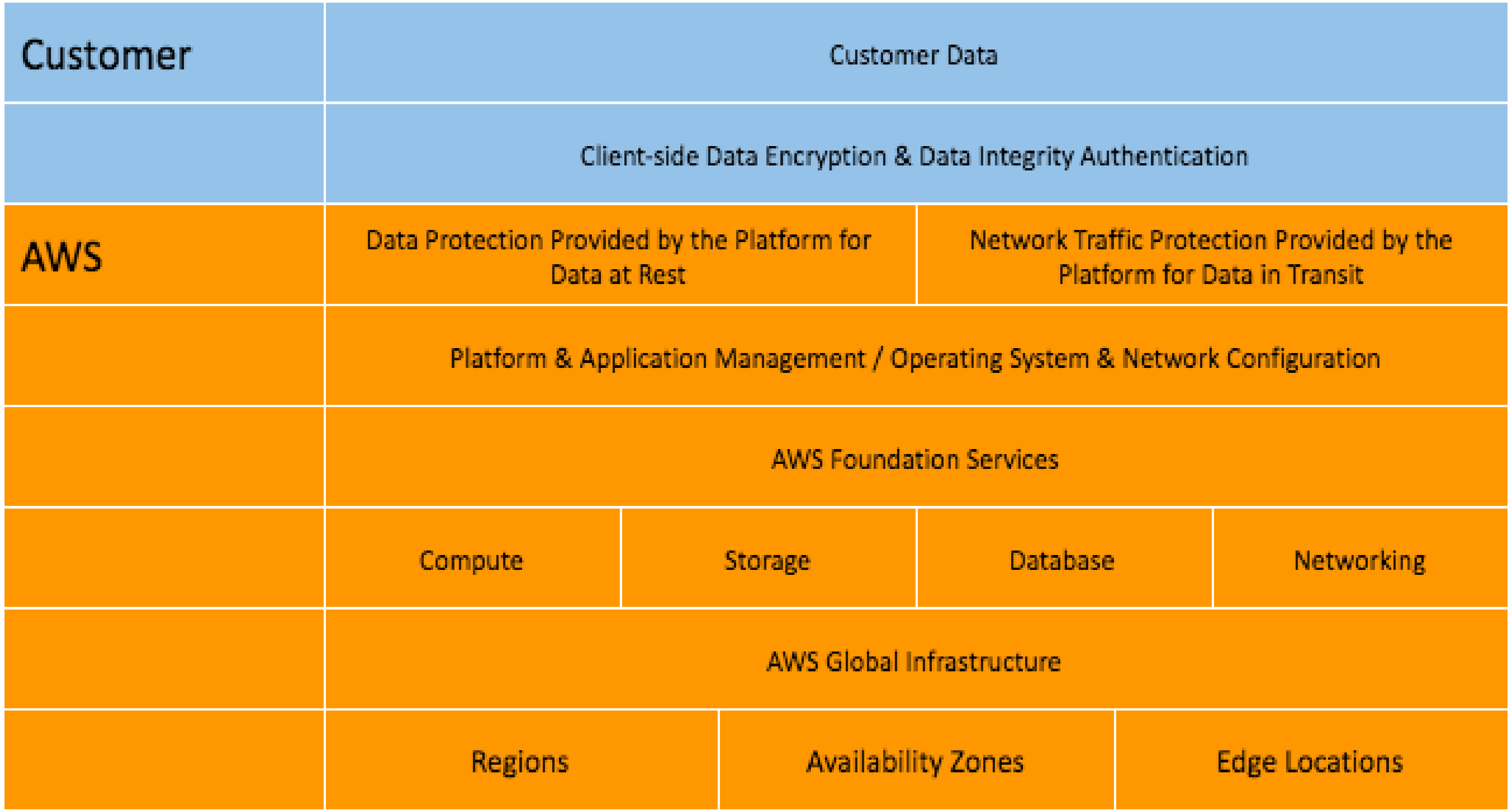
AWS service

- AWS Identity & Access Management (IAM)
- AWS Single Sign-On
- Amazon Cognito
- AWS Directory Service
- AWS Resource Access Manager
- AWS Organizations
- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- AWS Config
- AWS CloudTrail
- AWS IoT Device Defender
- AWS Shield
- AWS Web Application Firewall (WAF)
- AWS Firewall Manager

AWS Shared Responsibility Model

Customer responsibility *“Security in the Cloud”*

AWS responsibility *“Security of the Cloud”*



Customer

Customer Data

Client-side Data Encryption & Data Integrity Authentication

AWS

Data Protection Provided by the Platform for Data at Rest

Network Traffic Protection Provided by the Platform for Data in Transit

Platform & Application Management / Operating System & Network Configuration

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Regions

Availability Zones

Edge Locations

AWS S3 Bucket Overview

- Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.
- Amazon S3 offers a range of storage classes designed for different use cases. These include:
- *S3 Standard* for general-purpose storage of frequently accessed data
- *S3 Intelligent-Tiering* for data with unknown or changing access patterns
- *S3 Standard-Infrequent Access* and *S3 One Zone-Infrequent Access* for long-lived, but less frequently accessed data
- Amazon *S3 Glacier* and Amazon *S3 Glacier Deep Archive* for long-term archive and digital preservation.
- Every S3 Storage Class supports a specific data access level at corresponding costs.
- https://aws.amazon.com/s3/storage-classes/?nc=sn&loc=3

AWS EC2 Instance Overview

- Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud.
- **General purpose** instances provide a balance of compute, memory and networking resources, and can be used for a variety of diverse workloads. These instances are ideal for applications that use these resources in equal proportions such as web servers and code repositories.
- **Compute Optimized** instances are ideal for compute bound applications that benefit from high performance processors.
- **Memory optimized** instances are designed to deliver fast performance for workloads that process large data sets in memory.
- **Storage optimized** instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage.

MAGNET AXIOM™ CYBER

Simplify your remote forensic investigations by focusing on the evidence that matters.

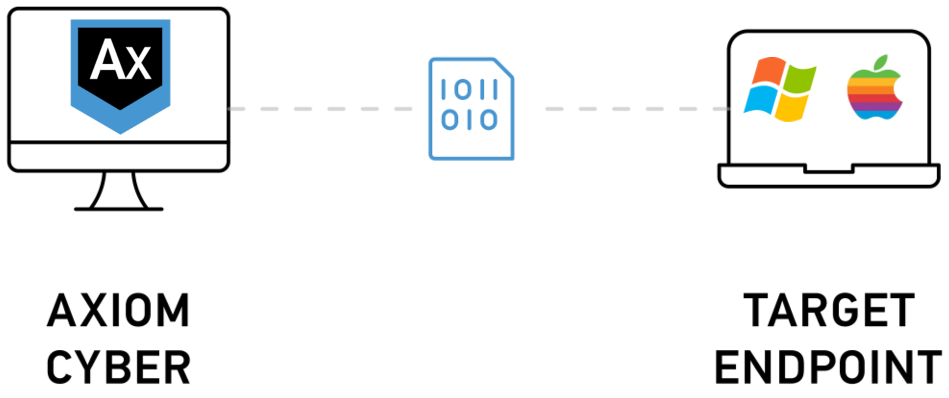
AXIOM Cyber is a digital forensics solution that allows organizations to perform remote acquisitions while collecting and analyzing evidence from cloud services, computers, and mobile devices.

Advanced Cloud Collection

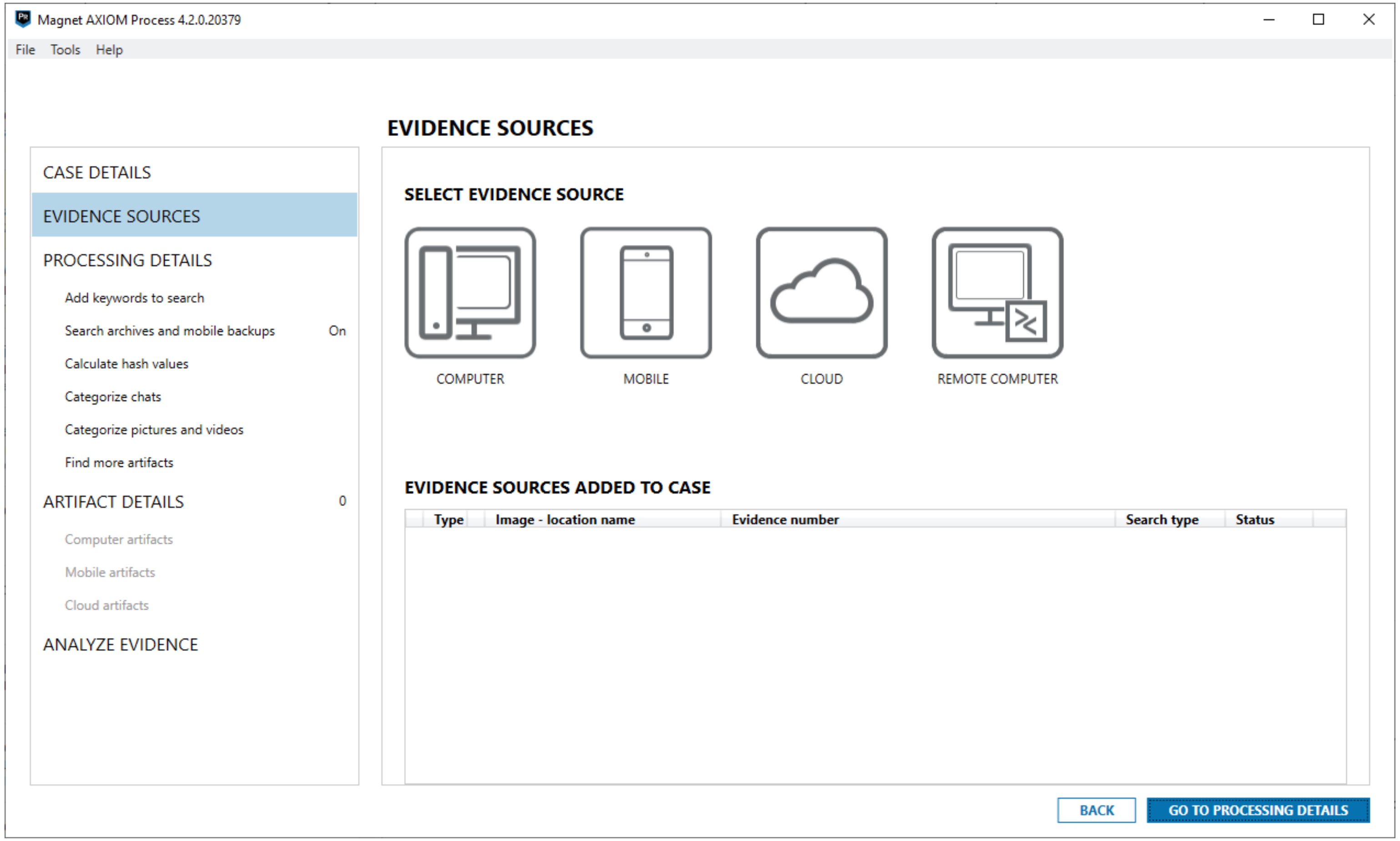
- Leverage admin credentials to acquire from Office 365, G Suite, and Box.com
- Collect data from corporate cloud services like AWS S3 and EC2,
- Investigate top corporate communication tools like MS Teams, and Slack
- Acquire from social media and other cloud services with user credentials

Covert Remote Collection

- Remotely collect individual files, targeted locations, or the full disk, and memory from Windows devices
- Remotely collect files from Macs including those with T2 security chips and SIP enabled
- Automatically reconnect to target endpoint if it goes offline and resume collections from where it left off
- Configurable, on-demand remote agent



MAGNET AXIOM CYBER



Add keywords to search

Search archives and mobile backups On

Calculate hash values

Categorize chats

Categorize pictures and videos

Find more artifacts

ARTIFACT DETAILS 0

EVIDENCE SOURCES

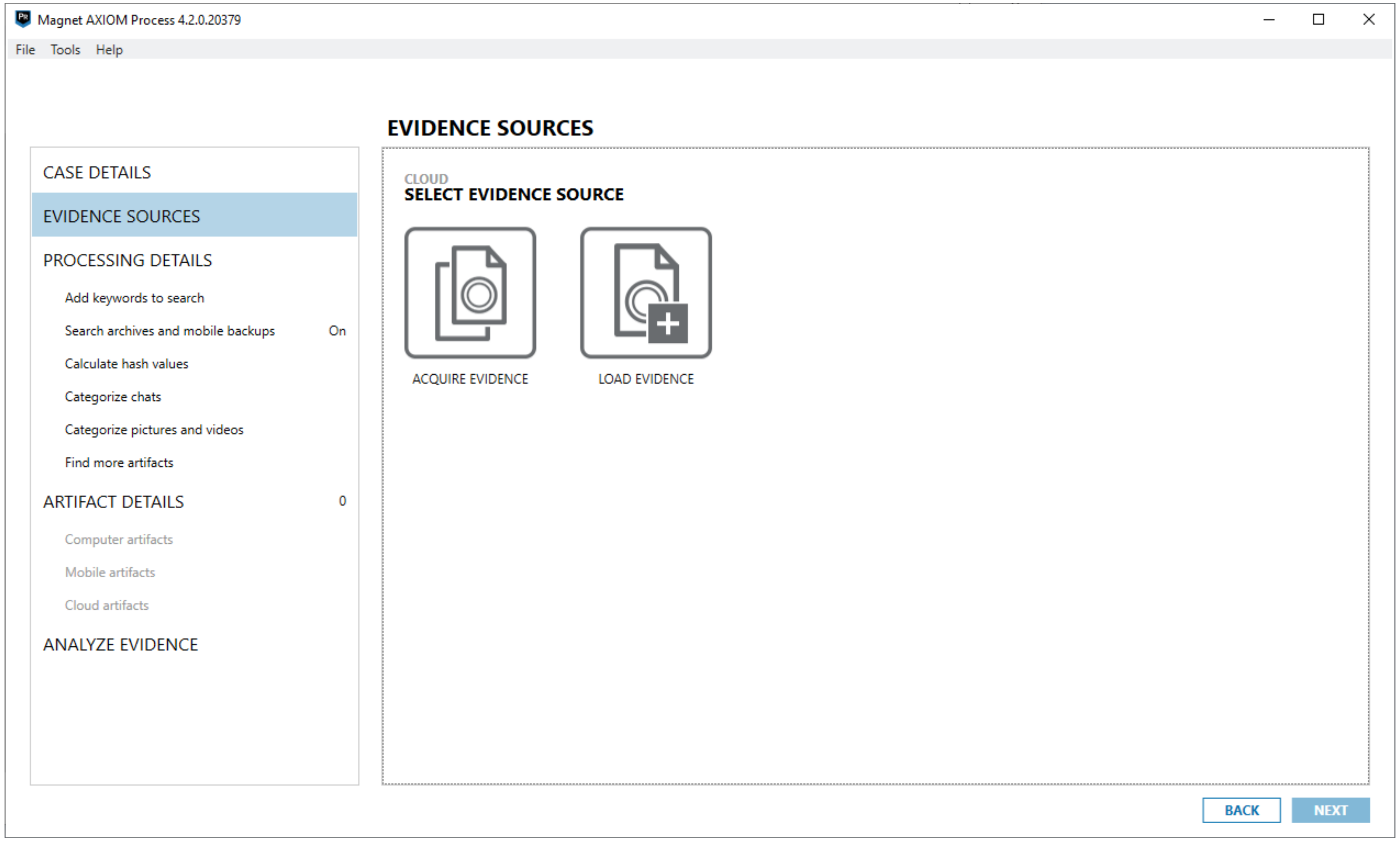
SELECT EVIDENCE SOURCE

EVIDENCE SOURCES ADDED TO CASE

Type	Image - location name	Evidence number	Search type	Status

AXIOM Cyber supports multiple evidence sources including the analysis of computer and mobile devices, remote collection of systems, and Cloud based sources.

MAGNET AXIOM CYBER



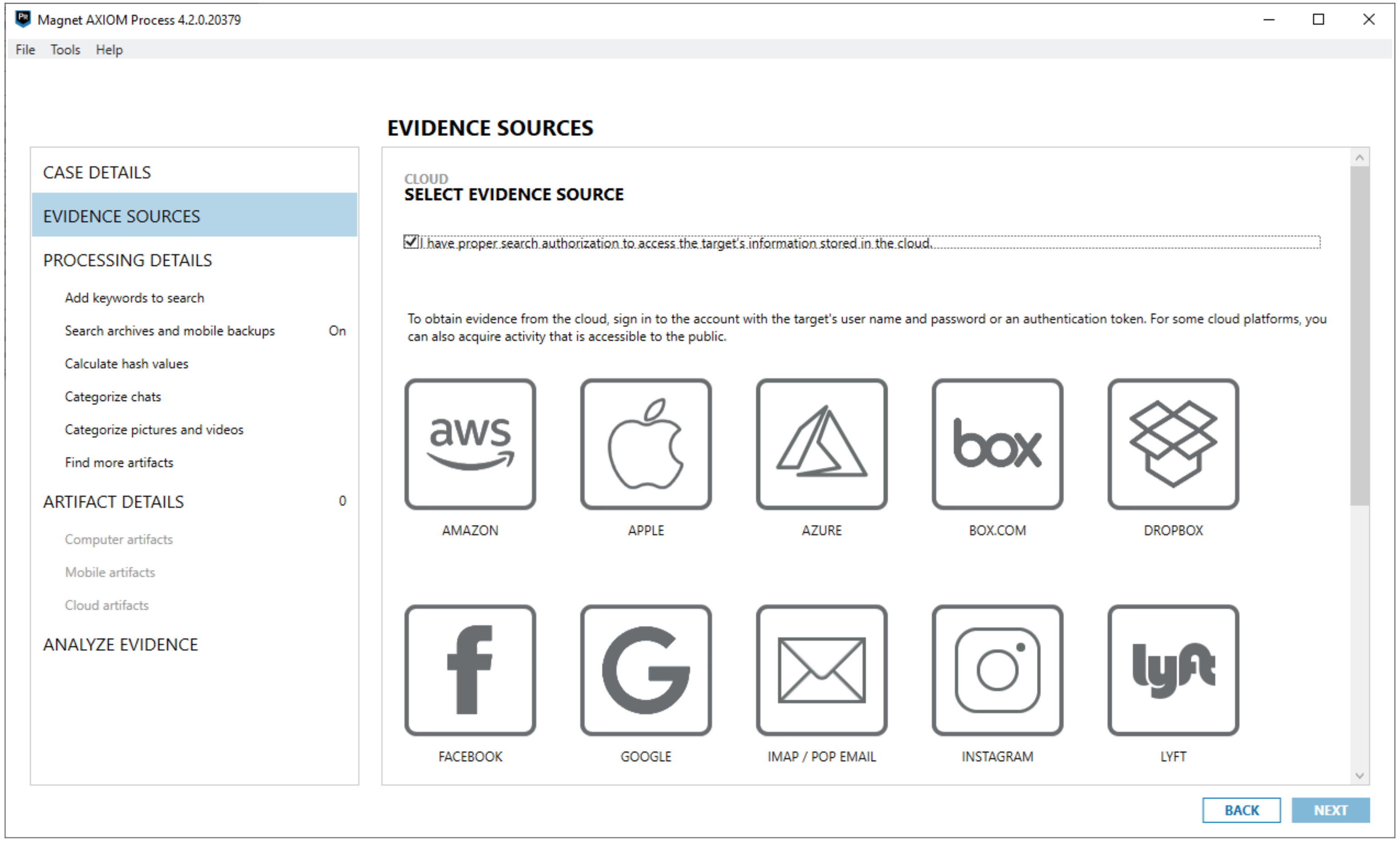
EVIDENCE SOURCES

- CASE DETAILS
- EVIDENCE SOURCES
- PROCESSING DETAILS
  - Add keywords to search
  - Search archives and mobile backups On
  - Calculate hash values
  - Categorize chats
  - Categorize pictures and videos
  - Find more artifacts
- ARTIFACT DETAILS 0
  - Computer artifacts
  - Mobile artifacts
  - Cloud artifacts
- ANALYZE EVIDENCE

CLOUD
SELECT EVIDENCE SOURCE

Cloud evidence can be acquired directly from service providers or loaded as evidence packages downloaded externally using services such as Google Takeout or Facebook’s Download My Data Feature

MAGNET AXIOM CYBER



Search archives and mobile backups On

ARTIFACT DETAILS 0

EVIDENCE SOURCES

CLOUD

SELECT EVIDENCE SOURCE

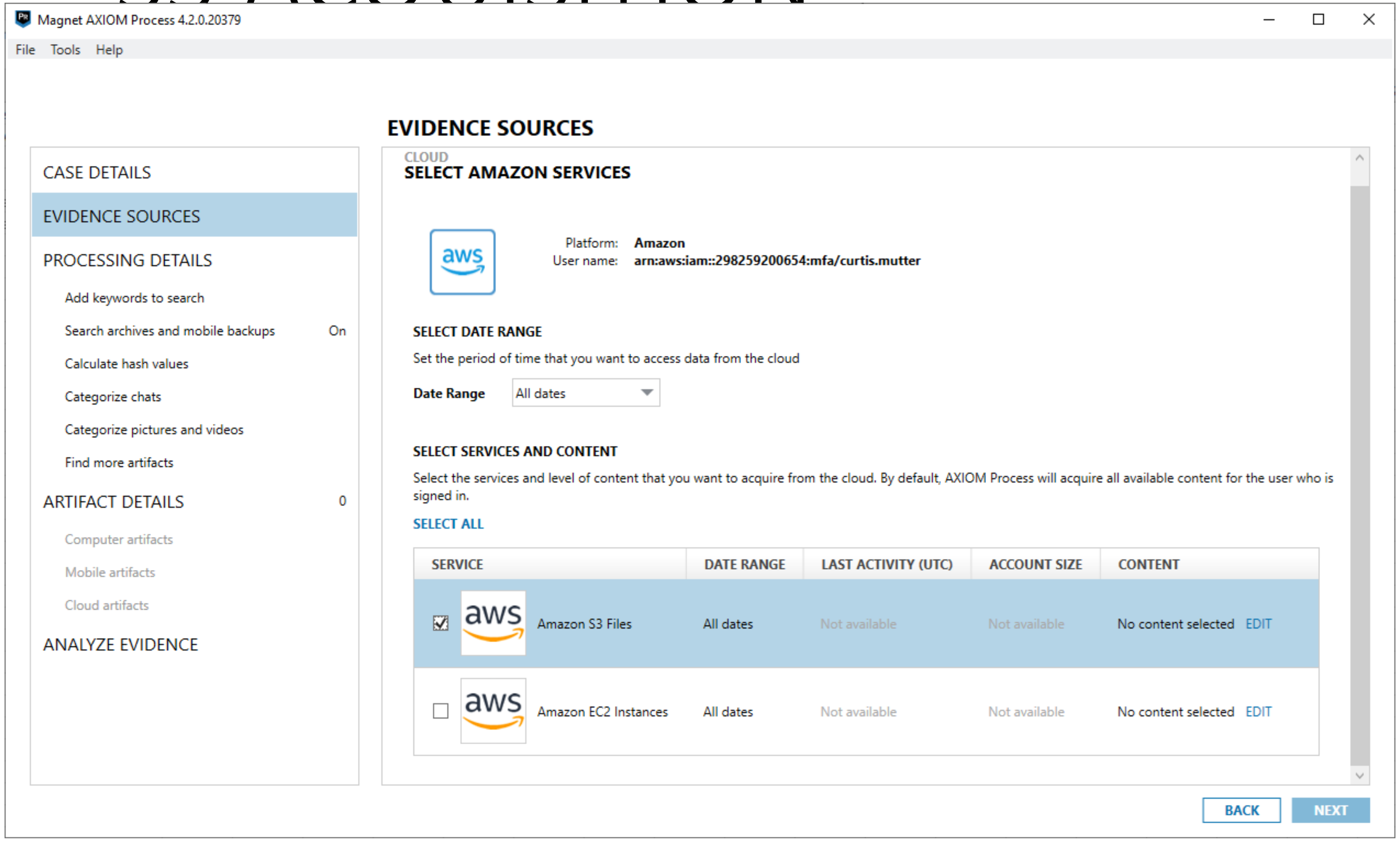
☑ I have proper search authorization to access the target's information stored in the cloud.

To obtain evidence from the cloud, sign in to the account with the target's user name and password or an authentication token. For some cloud platforms, you can also acquire activity that is accessible to the public.

AXIOM Cyber supports many different platforms for live acquisition including:

- Amazon Web Services
- Microsoft Azure
- O365
- MS Teams
- Box.com
- Dropbox
- Google Gsuite
- …and more

MAGNET AXIOM CYBER S3 ACQUISITION



EVIDENCE SOURCES

CLOUD

SELECT AMAZON SERVICES

Platform: Amazon
User name: arn:aws:iam::298259200654:mfa/curtis.mutter

SELECT DATE RANGE

Set the period of time that you want to access data from the cloud

Date Range: All dates

SELECT SERVICES AND CONTENT

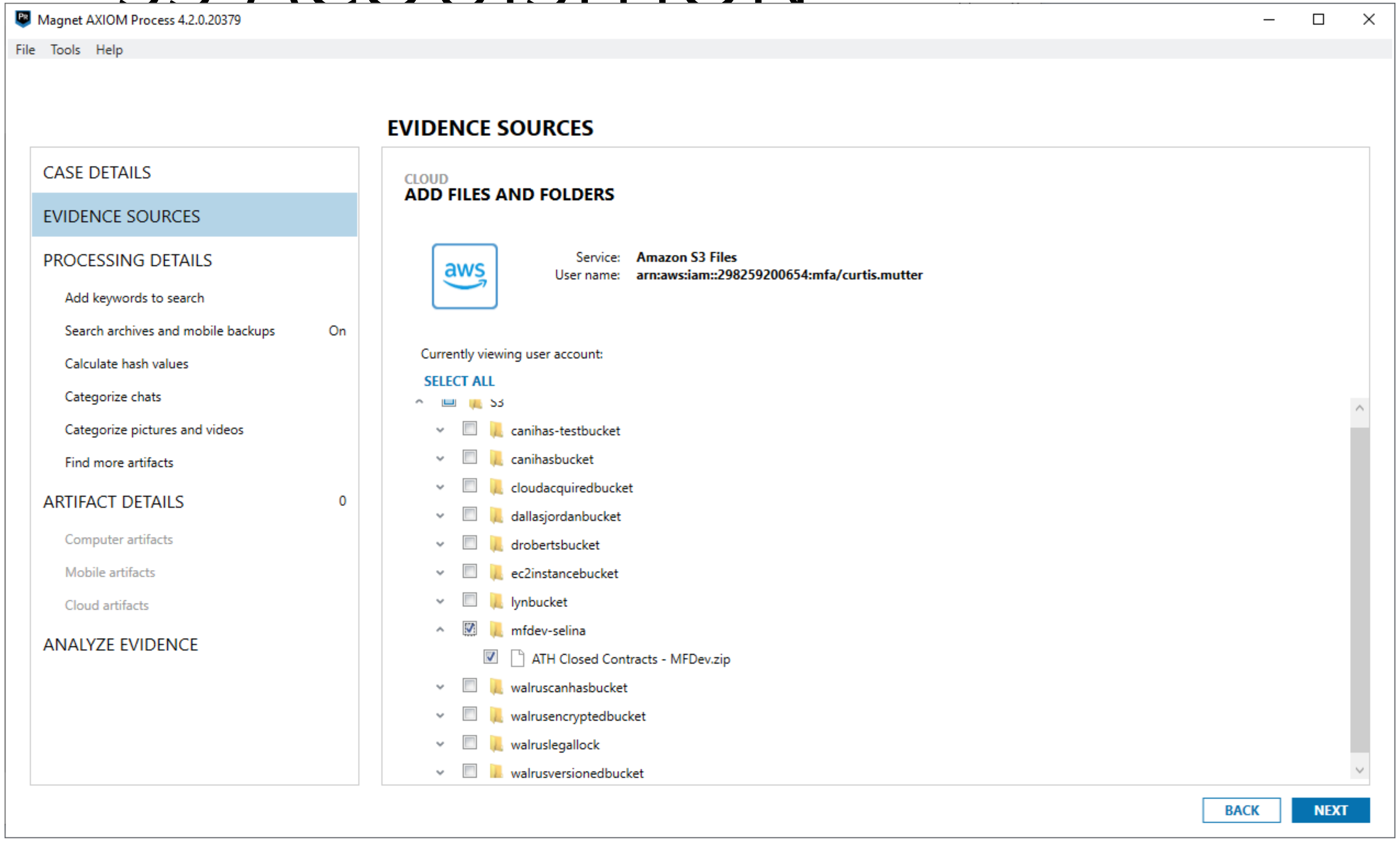
Select the services and level of content that you want to acquire from the cloud. By default, AXIOM Process will acquire all available content for the user who is signed in.

SELECT ALL

	SERVICE	DATE RANGE	LAST ACTIVITY (UTC)	ACCOUNT SIZE	CONTENT
☑	Amazon S3 Files	All dates	Not available	Not available	No content selected EDIT
□	Amazon EC2 Instances	All dates	Not available	Not available	No content selected EDIT

S3 buckets are presented similar to other file storage applications.

MAGNET AXIOM CYBER S3 ACQUISITION



Magnet AXIOM Process 4.2.0.20379

EVIDENCE SOURCES

- CASE DETAILS
- EVIDENCE SOURCES
- PROCESSING DETAILS
  - Add keywords to search
  - Search archives and mobile backups: On
  - Calculate hash values
  - Categorize chats
  - Categorize pictures and videos
  - Find more artifacts
- ARTIFACT DETAILS: 0
  - Computer artifacts
  - Mobile artifacts
  - Cloud artifacts
- ANALYZE EVIDENCE

CLOUD

ADD FILES AND FOLDERS

Service: **Amazon S3 Files**

User name: **arn:aws:iam::298259200654:mfa/curtis.mutter**

Currently viewing user account:

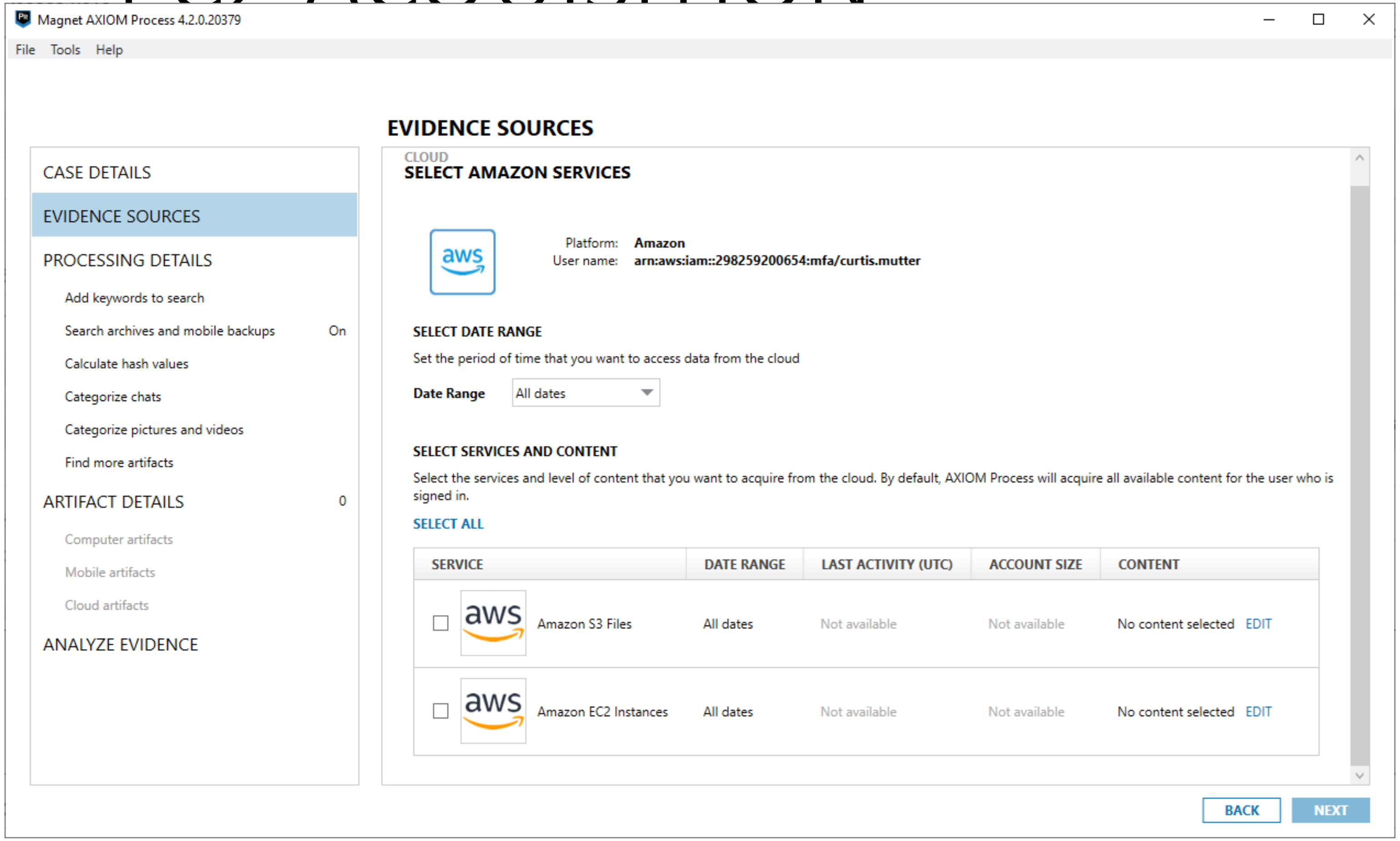
SELECT ALL

- S3
  - □ canihas-testbucket
  - □ canihasbucket
  - □ cloudacquiredbucket
  - □ dallasjordanbucket
  - □ drobertsbucket
  - □ ec2instancebucket
  - □ lynbucket
  - ☑ mfdev-selina
    - ☑ ATH Closed Contracts - MFDev.zip
  - □ walruscanhasbucket
  - □ walrusencryptedbucket
  - □ walruslegallock
  - □ walrusversionedbucket

AXIOM will provide the examiner to choose the bucket they wish to acquire.

The examiner can explore the contents of the buckets and only acquire the files of interest as well.

MAGNET AXIOM CYBER EC2 ACQUISITION



CASE DETAILS

EVIDENCE SOURCES

PROCESSING DETAILS

- Add keywords to search
- Search archives and mobile backups: On
- Calculate hash values
- Categorize chats
- Categorize pictures and videos
- Find more artifacts

ARTIFACT DETAILS: 0

- Computer artifacts
- Mobile artifacts
- Cloud artifacts

ANALYZE EVIDENCE

EVIDENCE SOURCES

CLOUD

SELECT AMAZON SERVICES

Platform: **Amazon**
User name: **arn:aws:iam::298259200654:mfa/curtis.mutter**

SELECT DATE RANGE

Set the period of time that you want to access data from the cloud

Date Range: All dates

SELECT SERVICES AND CONTENT

Select the services and level of content that you want to acquire from the cloud. By default, AXIOM Process will acquire all available content for the user who is signed in.

SELECT ALL

SERVICE	DATE RANGE	LAST ACTIVITY (UTC)	ACCOUNT SIZE	CONTENT
□ Amazon S3 Files	All dates	Not available	Not available	No content selected EDIT
□ Amazon EC2 Instances	All dates	Not available	Not available	No content selected EDIT

AWS users who have been granted appropriate permissions within their environment, can acquire both virtual machine snapshots from EC2, as well as the contents of S3 buckets.

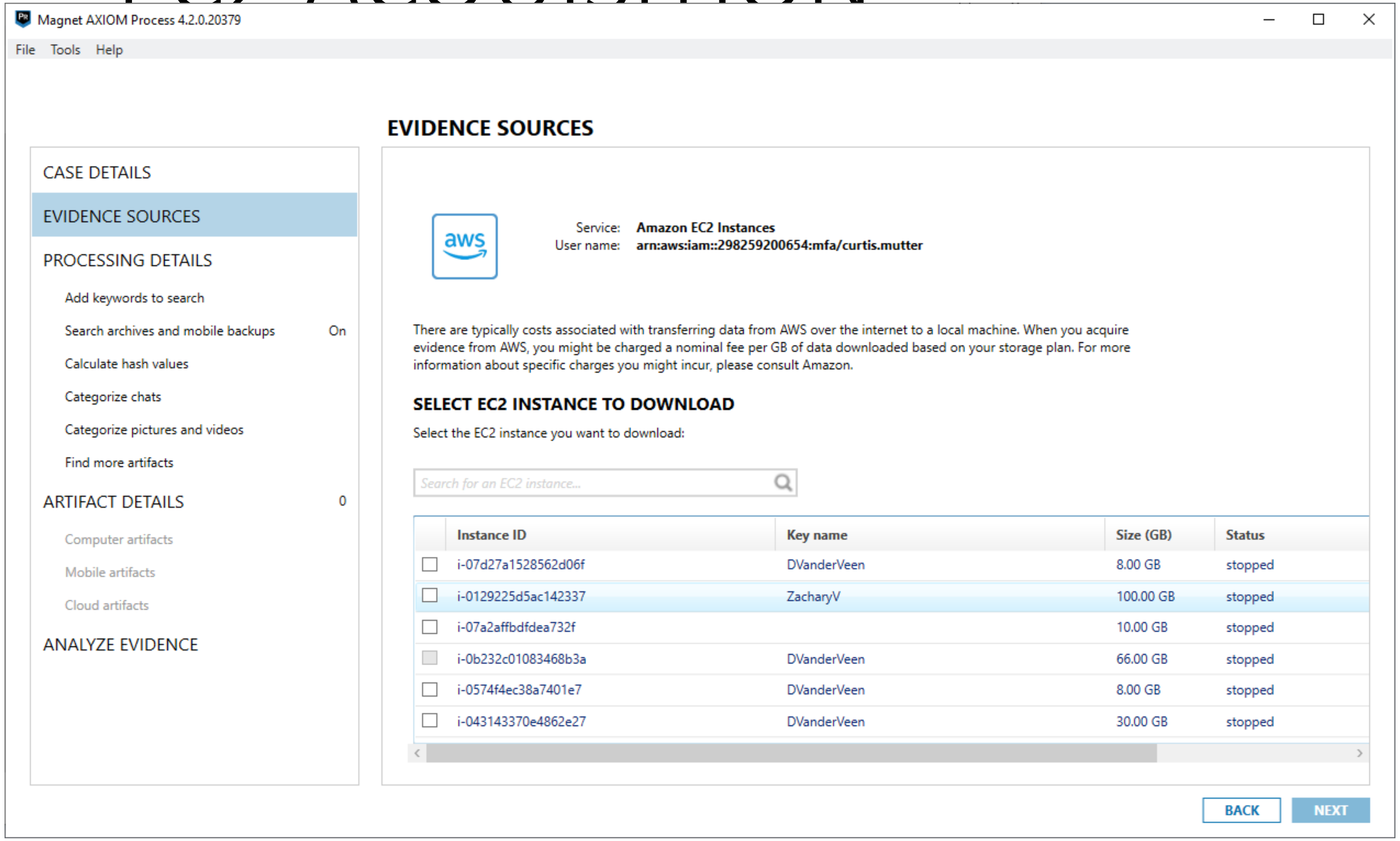
For information on configuring AWS to support acquisition, see the following articles from the Magnet Forensics Knowledge Center

Find AWS authentication details to acquire AWS S3 buckets or EC2 instances

Prerequisites for acquiring an EC2 instance

To learn more about AWS Access and Identity Management see https://aws.amazon.com/iam/

MAGNET AXIOM CYBER EC2 ACQUISITION



EVIDENCE SOURCES

Service: **Amazon EC2 Instances**
User name: **arn:aws:iam::298259200654:mfa/curtis.mutter**

There are typically costs associated with transferring data from AWS over the internet to a local machine. When you acquire evidence from AWS, you might be charged a nominal fee per GB of data downloaded based on your storage plan. For more information about specific charges you might incur, please consult Amazon.

SELECT EC2 INSTANCE TO DOWNLOAD

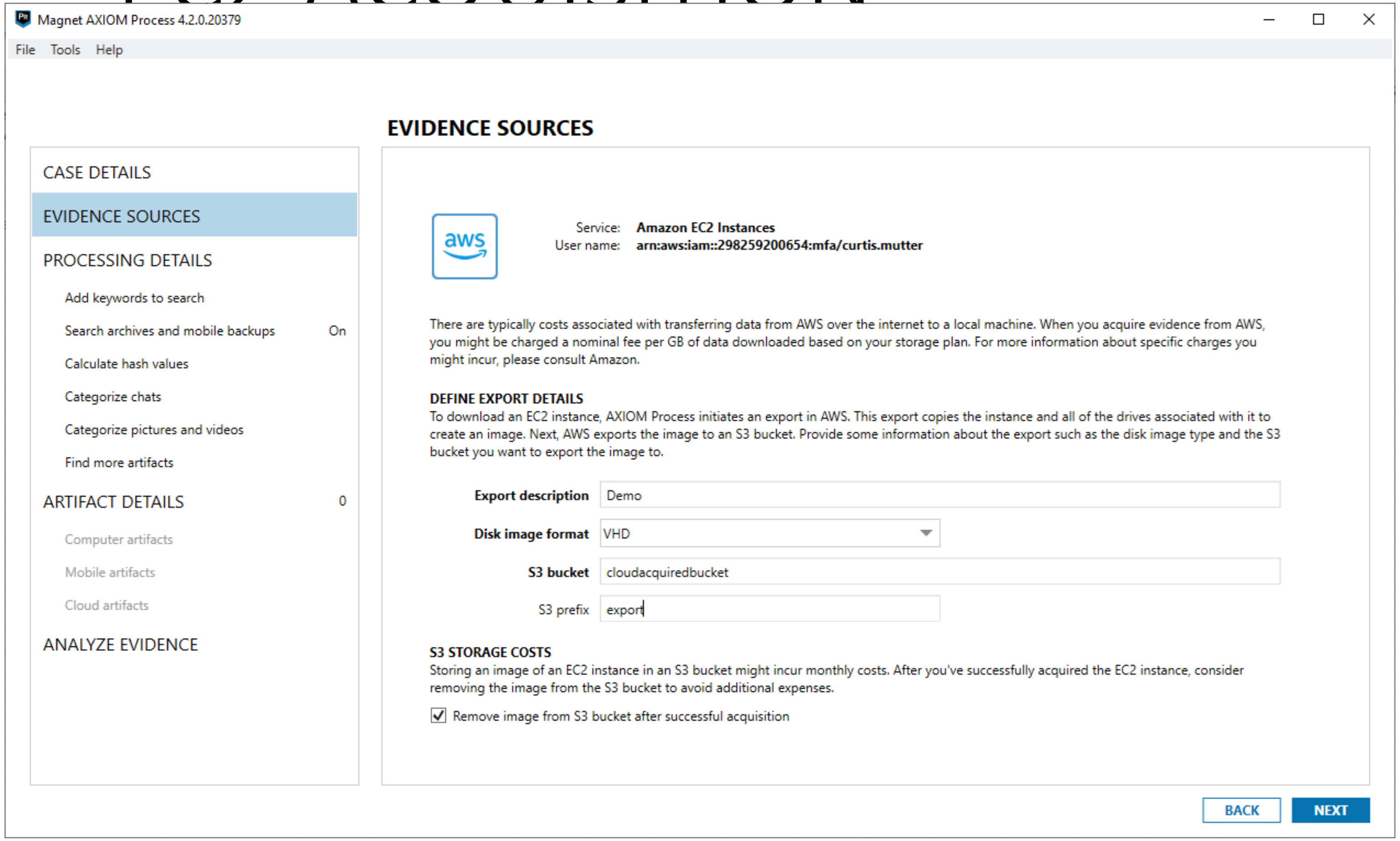
Select the EC2 instance you want to download:

	Instance ID	Key name	Size (GB)	Status
□	i-07d27a1528562d06f	DVanderVeen	8.00 GB	stopped
□	i-0129225d5ac142337	ZacharyV	100.00 GB	stopped
□	i-07a2affbdfdea732f		10.00 GB	stopped
□	i-0b232c01083468b3a	DVanderVeen	66.00 GB	stopped
□	i-0574f4ec38a7401e7	DVanderVeen	8.00 GB	stopped
□	i-043143370e4862e27	DVanderVeen	30.00 GB	stopped

To acquire EC2 instances, users can search for the end point system they wish to acquire.

If available, the user can select the image for download.

MAGNET AXIOM CYBER EC2 ACQUISITION



EVIDENCE SOURCES

Service: **Amazon EC2 Instances**
User name: **arn:aws:iam::298259200654:mfa/curtis.mutter**

There are typically costs associated with transferring data from AWS over the internet to a local machine. When you acquire evidence from AWS, you might be charged a nominal fee per GB of data downloaded based on your storage plan. For more information about specific charges you might incur, please consult Amazon.

DEFINE EXPORT DETAILS

To download an EC2 instance, AXIOM Process initiates an export in AWS. This export copies the instance and all of the drives associated with it to create an image. Next, AWS exports the image to an S3 bucket. Provide some information about the export such as the disk image type and the S3 bucket you want to export the image to.

Export description: Demo
Disk image format: VHD
S3 bucket: cloudacquiredbucket
S3 prefix: export

S3 STORAGE COSTS

Storing an image of an EC2 instance in an S3 bucket might incur monthly costs. After you've successfully acquired the EC2 instance, consider removing the image from the S3 bucket to avoid additional expenses.

☑ Remove image from S3 bucket after successful acquisition

AWS requires that the image be copied to a S3 bucket prior to acquisition.

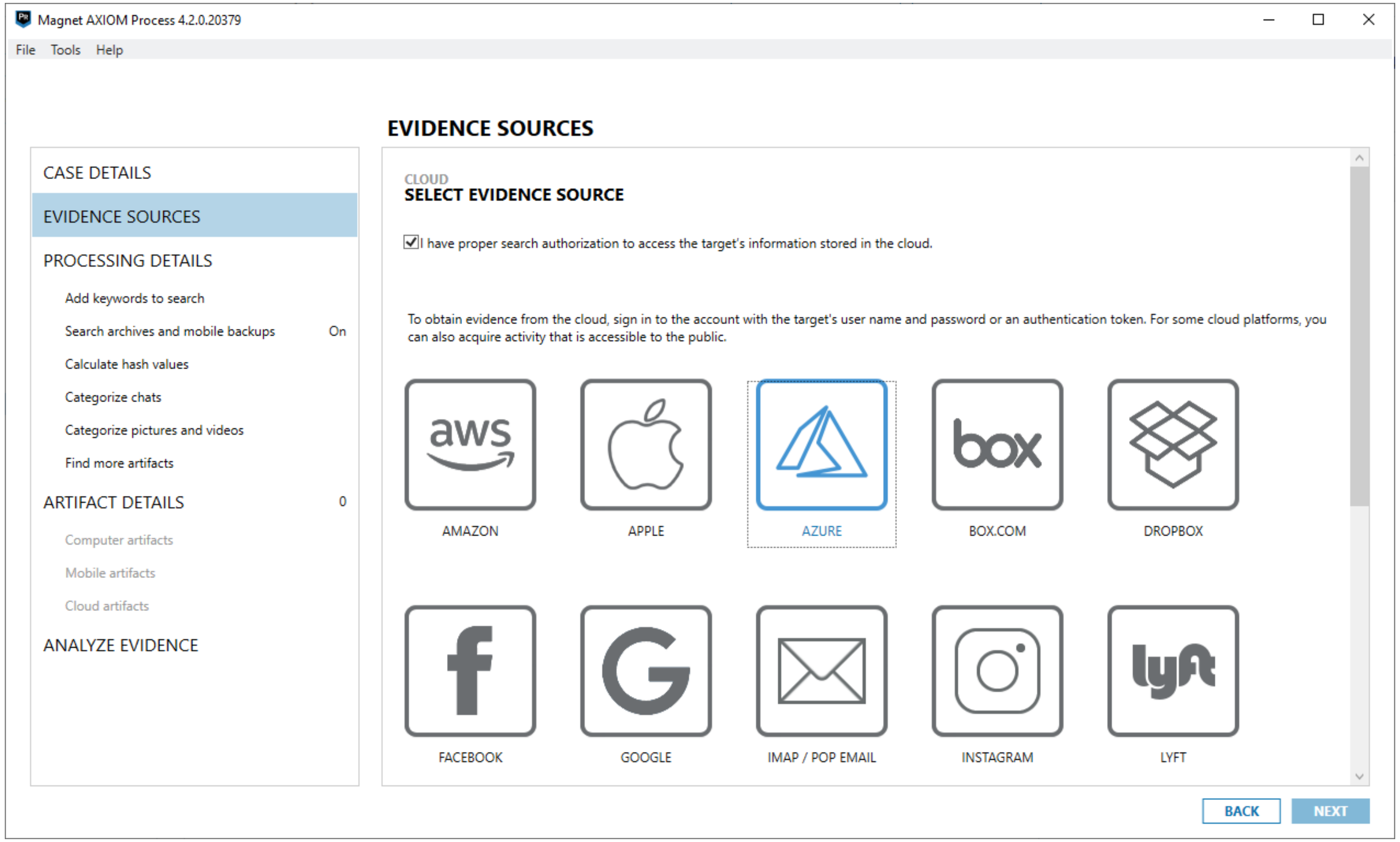
Users can choose to acquire the image as a VHD or VMDK image.

Users can optionally remove the image upon completion of the acquisition to reduce storage costs.

MAGNET AXIOM CYBER
EC2 AND S3 CONSIDERATIONS

- S3 Acquisition supports the following bucket types for acquisition.
  - *S3 Standard* for general-purpose storage of frequently accessed data
  - *S3 Intelligent-Tiering* for data with unknown or changing access patterns
  - *S3 Standard-Infrequent Access* and *S3 One Zone-Infrequent Access* for long-lived, but less frequently accessed data
  - *S3 Glacier* and *S3 Glacier Deep Archive* are not currently supported
- EC2 acquisition requires at least one accessible S3 bucket, which will be used to store the image snapshot prior to downloading.
- AXIOM Process supports acquiring EC2 instances for Amazon Linux and Ubuntu Server SSD volume types
- For additional limitations on supported acquisition types see https://docs.aws.amazon.com/vm-import/latest/userguide/vmexport.html
- There are roles in IAM that allow other AWS resources to be utilized in conjunction with other AWS resources. This can include collection of data from S3 or EC2 via S3. One such role is the *ExportEC2ToS3Role*. Associated with this role is a policy called *AmazonS3FullAccess*. This policy allows access to S3. For more info on IAM see: https://aws.amazon.com/iam/

MAGNET AXIOM CYBER AZURE ACQUISITION



EVIDENCE SOURCES

CASE DETAILS

EVIDENCE SOURCES

PROCESSING DETAILS

Add keywords to search

Search archives and mobile backups On

Calculate hash values

Categorize chats

Categorize pictures and videos

Find more artifacts

ARTIFACT DETAILS 0

Computer artifacts

Mobile artifacts

Cloud artifacts

ANALYZE EVIDENCE

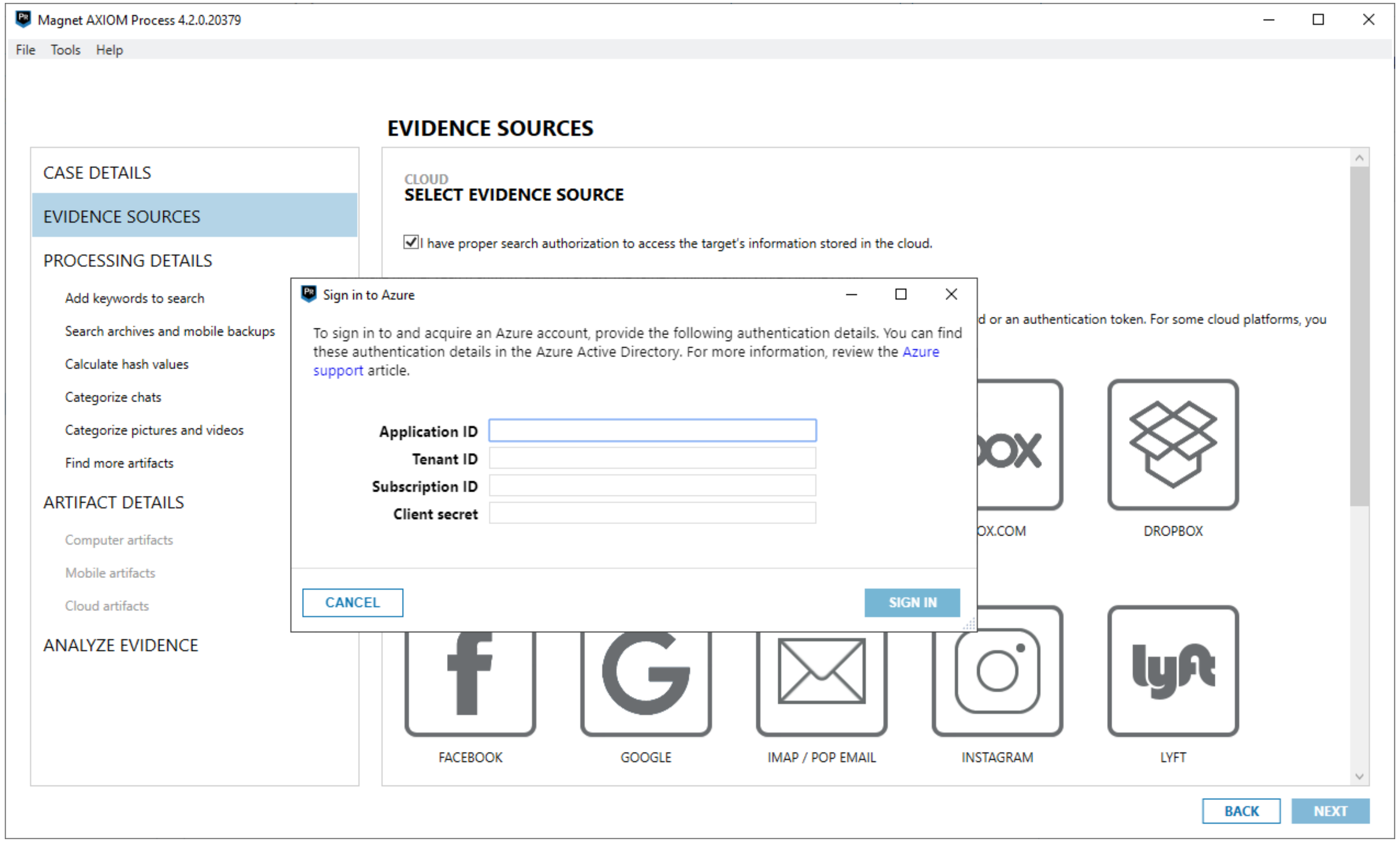
CLOUD
SELECT EVIDENCE SOURCE

☑ I have proper search authorization to access the target's information stored in the cloud.

To obtain evidence from the cloud, sign in to the account with the target's user name and password or an authentication token. For some cloud platforms, you can also acquire activity that is accessible to the public.

Magnet AXIOM Cyber has recently added the ability to acquire virtual machine images from Microsoft Azure.

MAGNET AXIOM CYBER AZURE ACQUISITION



☑ I have proper search authorization to access the target's information stored in the cloud.

d or an authentication token. For some cloud platforms, you

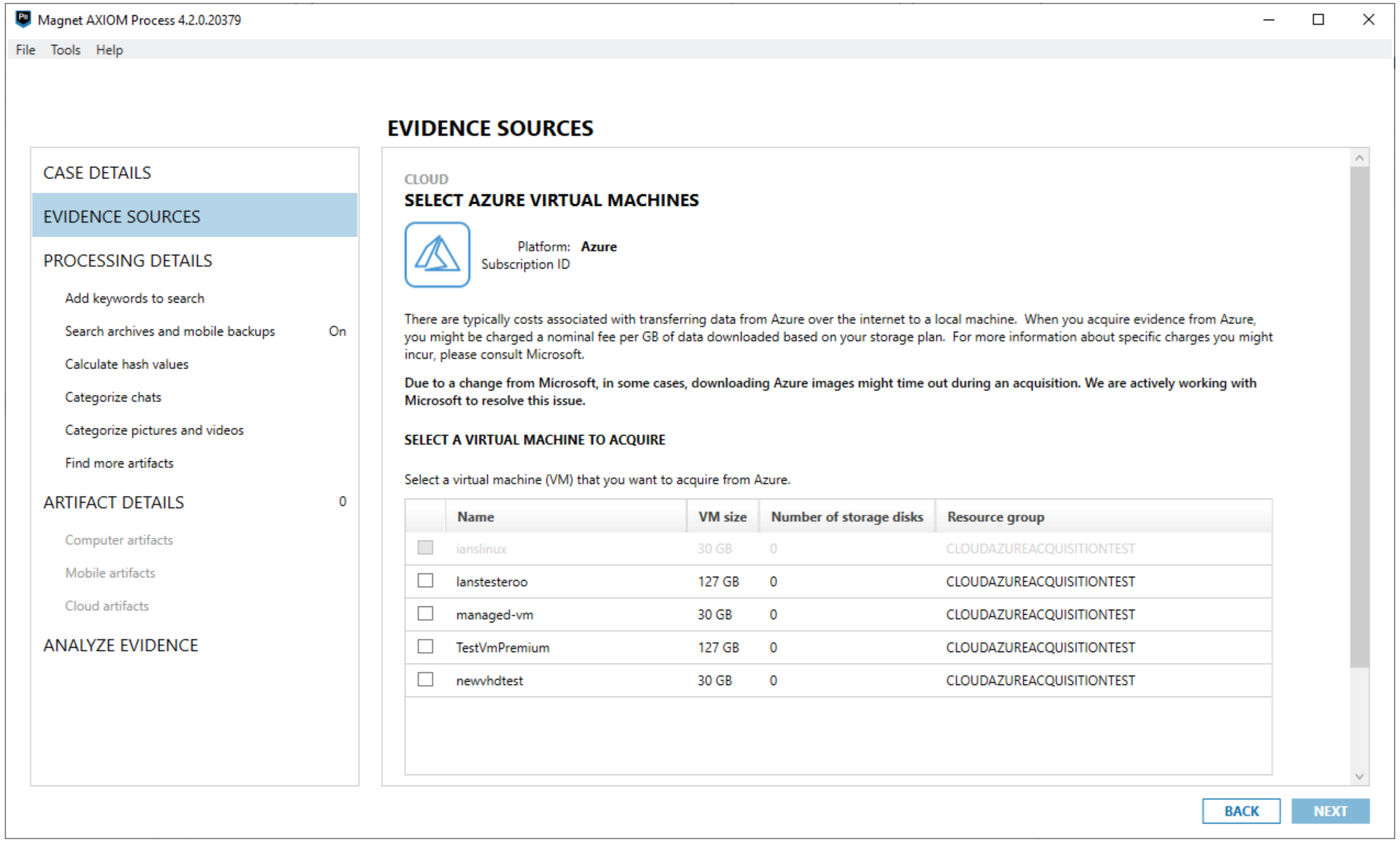
To sign in to and acquire an Azure account, provide the following authentication details. You can find these authentication details in the Azure Active Directory. For more information, review the Azure support article.

Application ID	
Tenant ID	
Subscription ID	
Client secret	

For information on configuring access to Azure, see the following Knowledge Base Article:

Find Azure authentication details

MAGNET AXIOM CYBER AZURE ACQUISITION



EVIDENCE SOURCES

CLOUD

SELECT AZURE VIRTUAL MACHINES

Platform: **Azure**
Subscription ID

There are typically costs associated with transferring data from Azure over the internet to a local machine. When you acquire evidence from Azure, you might be charged a nominal fee per GB of data downloaded based on your storage plan. For more information about specific charges you might incur, please consult Microsoft.

Due to a change from Microsoft, in some cases, downloading Azure images might time out during an acquisition. We are actively working with Microsoft to resolve this issue.

SELECT A VIRTUAL MACHINE TO ACQUIRE

Select a virtual machine (VM) that you want to acquire from Azure.

	Name	VM size	Number of storage disks	Resource group
□	ianslinux	30 GB	0	CLOUDAZUREACQUISITIONTEST
□	lanstesteroo	127 GB	0	CLOUDAZUREACQUISITIONTEST
□	managed-vm	30 GB	0	CLOUDAZUREACQUISITIONTEST
□	TestVmPremium	127 GB	0	CLOUDAZUREACQUISITIONTEST
□	newvhdtest	30 GB	0	CLOUDAZUREACQUISITIONTEST

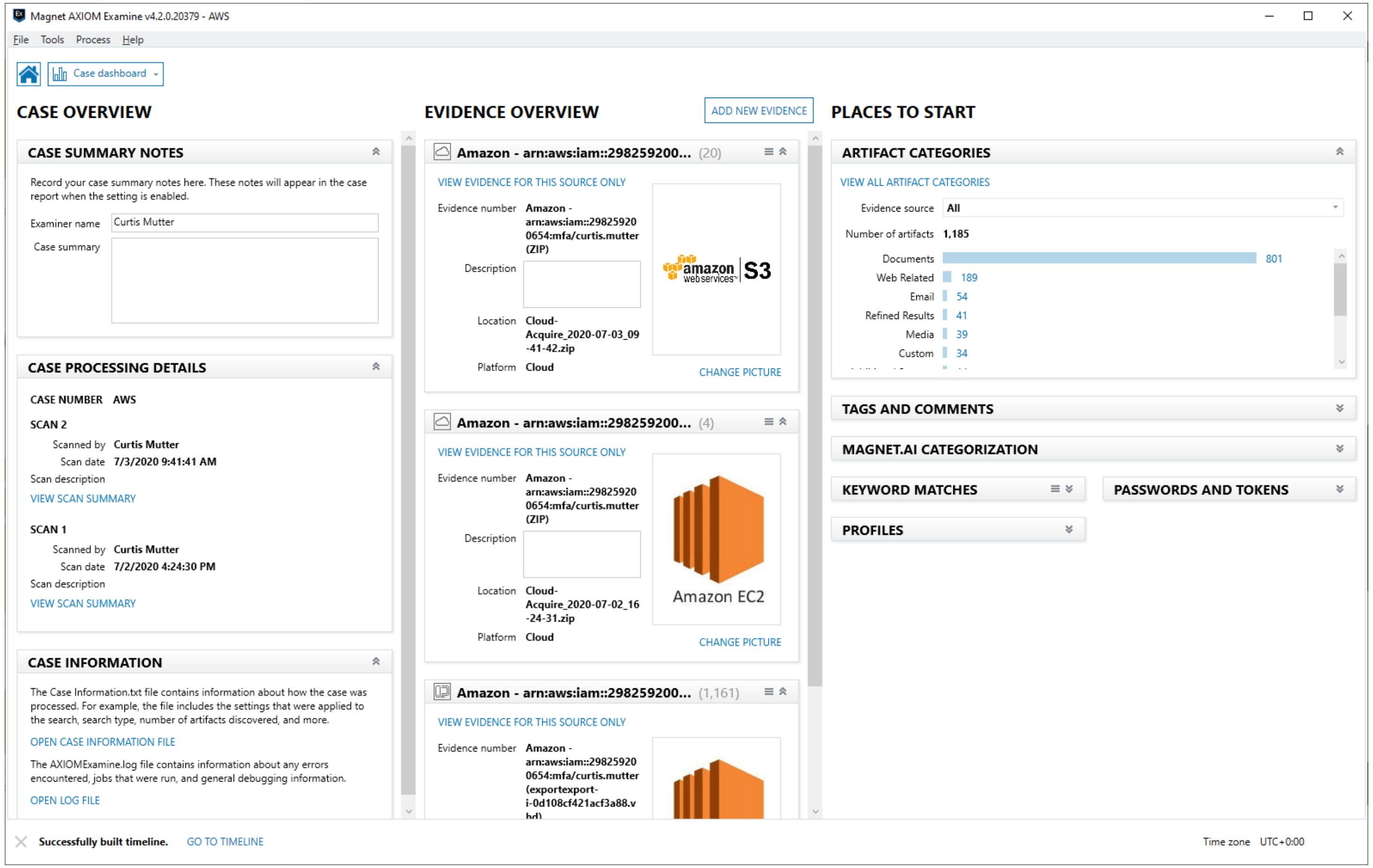
Once authenticated, the user can choose from the available instances for acquisition.

Note that only one image can be acquired at a time, however multiple evidence items can be added to the same case file by adding additional evidence.

MAGNET AXIOM CYBER
AZURE ACQUISITION - CONSIDERATIONS

- Available VMs can be selected for download.
- Only one image can be acquired at a time.
- Users can choose to discard the image snapshot once it has been downloaded
- The image will be downloaded as a Virtual Hard Drive (VHD)
- Artifacts will be carved after acquisition
- Only VMs using Azure Managed Disks can be acquired (for more information see link)

MAGNET AXIOM CYBER – ANALYSIS



CASE OVERVIEW

CASE SUMMARY NOTES

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name: Curtis Mutter

Case summary:

CASE PROCESSING DETAILS

CASE NUMBER AWS

SCAN 2

Scanned by Curtis Mutter
Scan date 7/3/2020 9:41:41 AM
Scan description
VIEW SCAN SUMMARY

SCAN 1

Scanned by Curtis Mutter
Scan date 7/2/2020 4:24:30 PM
Scan description
VIEW SCAN SUMMARY

CASE INFORMATION

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

OPEN CASE INFORMATION FILE

The AXIOMExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

OPEN LOG FILE

EVIDENCE OVERVIEW

Amazon - arn:aws:iam::298259200... (20)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number: Amazon - arn:aws:iam::298259200654:mfa/curtis.mutter (ZIP)
Description:
Location: Cloud-Acquire_2020-07-03_09-41-42.zip
Platform: Cloud

Amazon - arn:aws:iam::298259200... (4)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number: Amazon - arn:aws:iam::298259200654:mfa/curtis.mutter (ZIP)
Description:
Location: Cloud-Acquire_2020-07-02_16-24-31.zip
Platform: Cloud

Amazon - arn:aws:iam::298259200... (1,161)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number: Amazon - arn:aws:iam::298259200654:mfa/curtis.mutter (exportexport-i-0d108cf421acf3a88.vhd)

PLACES TO START

ARTIFACT CATEGORIES

VIEW ALL ARTIFACT CATEGORIES

Evidence source: All
Number of artifacts: 1,185

Documents	801
Web Related	189
Email	54
Refined Results	41
Media	39
Custom	34

TAGS AND COMMENTS

MAGNET.AI CATEGORIZATION

KEYWORD MATCHES

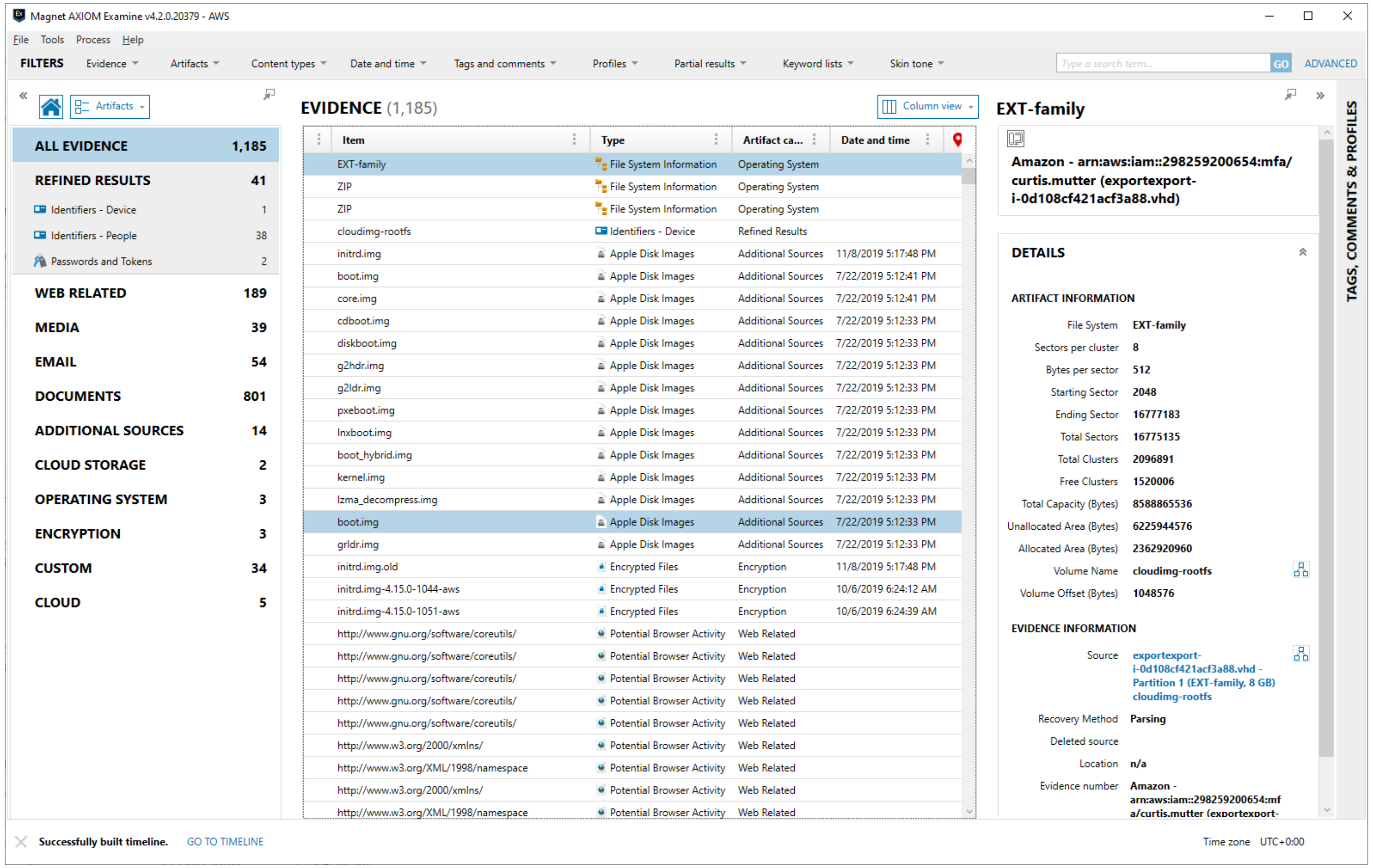
PASSWORDS AND TOKENS

PROFILES

Successfully built timeline. GO TO TIMELINE

Acquired evidence will be loaded into the case file and can be combined with evidence from any other service.

MAGNET AXIOM CYBER – ANALYSIS



ALL EVIDENCE	1,185
REFINED RESULTS	41
Identifiers - Device	1
Identifiers - People	38
Passwords and Tokens	2
WEB RELATED	189
MEDIA	39
EMAIL	54
DOCUMENTS	801
ADDITIONAL SOURCES	14
CLOUD STORAGE	2
OPERATING SYSTEM	3
ENCRYPTION	3
CUSTOM	34
CLOUD	5

EVIDENCE (1,185)

Item	Type	Artifact ca...	Date and time
EXT-family	File System Information	Operating System	
ZIP	File System Information	Operating System	
ZIP	File System Information	Operating System	
cloudimg-rootfs	Identifiers - Device	Refined Results	
initrd.img	Apple Disk Images	Additional Sources	11/8/2019 5:17:48 PM
boot.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:41 PM
core.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:41 PM
cdboot.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
diskboot.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
g2hdr.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
g2ldr.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
pxeboot.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
lnxboot.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
boot_hybrid.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
kernel.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
lzma_decompress.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
boot.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
grldr.img	Apple Disk Images	Additional Sources	7/22/2019 5:12:33 PM
initrd.img.old	Encrypted Files	Encryption	11/8/2019 5:17:48 PM
initrd.img-4.15.0-1044-aws	Encrypted Files	Encryption	10/6/2019 6:24:12 AM
initrd.img-4.15.0-1051-aws	Encrypted Files	Encryption	10/6/2019 6:24:39 AM
http://www.gnu.org/software/coreutils/	Potential Browser Activity	Web Related	
http://www.gnu.org/software/coreutils/	Potential Browser Activity	Web Related	
http://www.gnu.org/software/coreutils/	Potential Browser Activity	Web Related	
http://www.gnu.org/software/coreutils/	Potential Browser Activity	Web Related	
http://www.gnu.org/software/coreutils/	Potential Browser Activity	Web Related	
http://www.w3.org/2000/xmlns/	Potential Browser Activity	Web Related	
http://www.w3.org/XML/1998/namespace	Potential Browser Activity	Web Related	
http://www.w3.org/2000/xmlns/	Potential Browser Activity	Web Related	
http://www.w3.org/XML/1998/namespace	Potential Browser Activity	Web Related	

EXT-family

Amazon - arn:aws:iam::298259200654:mfa/curtis.mutter (exportexport-i-0d108cf421acf3a88.vhd)

DETAILS

ARTIFACT INFORMATION

File System	EXT-family
Sectors per cluster	8
Bytes per sector	512
Starting Sector	2048
Ending Sector	16777183
Total Sectors	16775135
Total Clusters	2096891
Free Clusters	1520006
Total Capacity (Bytes)	8588865536
Unallocated Area (Bytes)	6225944576
Allocated Area (Bytes)	2362920960
Volume Name	cloudimg-rootfs
Volume Offset (Bytes)	1048576

EVIDENCE INFORMATION

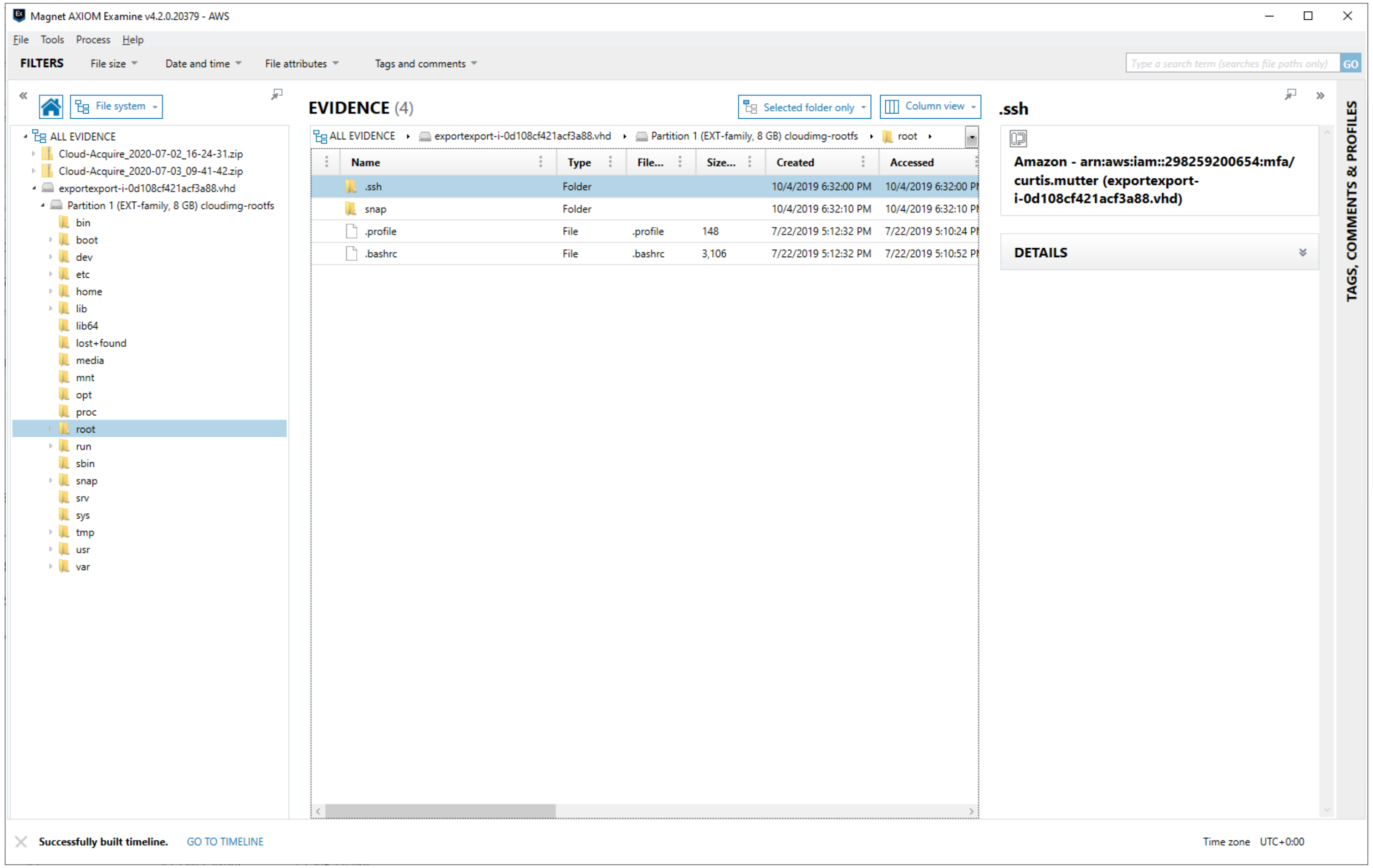
Source	exportexport-i-0d108cf421acf3a88.vhd - Partition 1 (EXT-family, 8 GB) cloudimg-rootfs
Recovery Method	Parsing
Deleted source	
Location	n/a
Evidence number	Amazon - arn:aws:iam::298259200654:mfa/curtis.mutter (exportexport-

Successfully built timeline.

Time zone UTC+0:00

Magnet AXIOM Cyber is an artifact based forensic platform providing examiners with instant access to critical evidence including documents, media, and operating system artifacts.

MAGNET AXIOM CYBER – ANALYSIS


Magnet AXIOM Examine v4.2.0.20379 - AWS
File
Tools
Process
Help
FILTERS
File size
Date and time
File attributes
Tags and comments
Type a search term (searches file paths only)
GO
File system
ALL EVIDENCE
Cloud-Acquire_2020-07-02_16-24-31.zip
Cloud-Acquire_2020-07-03_09-41-42.zip
exportexport-i-0d108cf421acf3a88.vhd
Partition 1 (EXT-family, 8 GB) cloudimg-rootfs
bin
boot
dev
etc
home
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
EVIDENCE (4)
Selected folder only
Column view
ALL EVIDENCE ▸ exportexport-i-0d108cf421acf3a88.vhd ▸ Partition 1 (EXT-family, 8 GB) cloudimg-rootfs ▸ root ▸
.ssh
DETAILS
TAGS, COMMENTS & PROFILES
GO TO TIMELINE
Time zone UTC+0:00

Name	Type	File...	Size...	Created	Accessed
.ssh	Folder			10/4/2019 6:32:00 PM	10/4/2019 6:32:00 PI
snap	Folder			10/4/2019 6:32:10 PM	10/4/2019 6:32:10 PI
.profile	File	.profile	148	7/22/2019 5:12:32 PM	7/22/2019 5:10:24 PI
.bashrc	File	.bashrc	3,106	7/22/2019 5:12:32 PM	7/22/2019 5:10:52 PI

Amazon - arn:aws:iam::298259200654:mfa/curtis.mutter (exportexport-i-0d108cf421acf3a88.vhd)

Successfully built timeline.

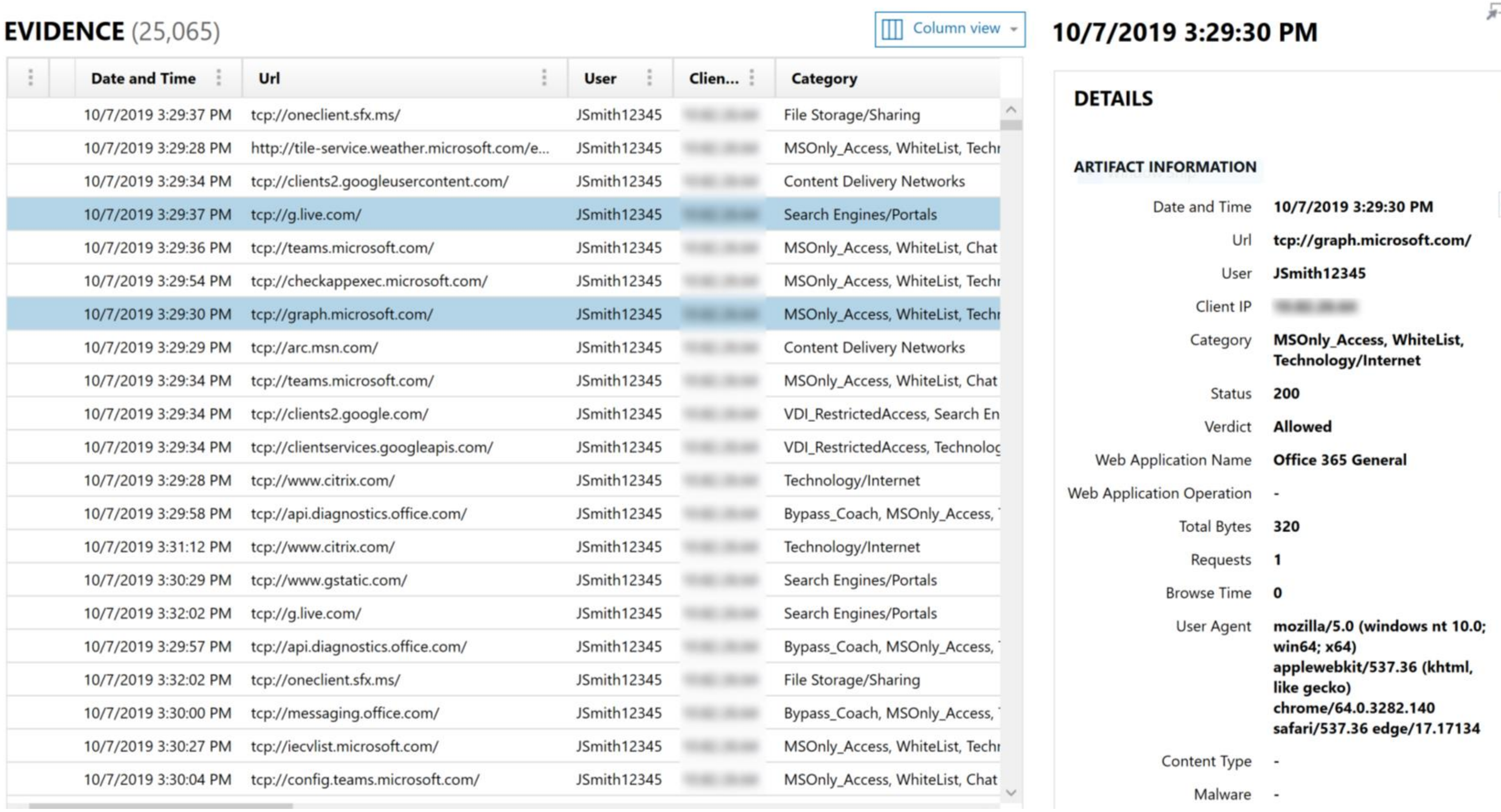
Magnet AXIOM Cyber also includes a full file system analysis tool for browsing or searching the file system of acquired virtual machines.

Evidence can easily be tagged and exported as a part of a report in multiple formats.

Loading Log Files into AXIOM Cyber

BlueCoat

- Magnet Free Tools
  - Magnet Custom Artifact Generator (*MCAG*)
- Load CSV / delimited files or SQLite DB of logs into MCAG
- Customize Fields
- Open AXIOM Cyber Process!



EVIDENCE (25,065)

Date and Time	Url	User	Clien...	Category
10/7/2019 3:29:37 PM	tcp://oneclient.sfx.ms/	JSmith12345	[redacted]	File Storage/Sharing
10/7/2019 3:29:28 PM	http://tile-service.weather.microsoft.com/e...	JSmith12345	[redacted]	MSOnly_Access, WhiteList, Techr
10/7/2019 3:29:34 PM	tcp://clients2.googleusercontent.com/	JSmith12345	[redacted]	Content Delivery Networks
10/7/2019 3:29:37 PM	tcp://g.live.com/	JSmith12345	[redacted]	Search Engines/Portals
10/7/2019 3:29:36 PM	tcp://teams.microsoft.com/	JSmith12345	[redacted]	MSOnly_Access, WhiteList, Chat
10/7/2019 3:29:54 PM	tcp://checkappexec.microsoft.com/	JSmith12345	[redacted]	MSOnly_Access, WhiteList, Techr
10/7/2019 3:29:30 PM	tcp://graph.microsoft.com/	JSmith12345	[redacted]	MSOnly_Access, WhiteList, Techr
10/7/2019 3:29:29 PM	tcp://arc.msn.com/	JSmith12345	[redacted]	Content Delivery Networks
10/7/2019 3:29:34 PM	tcp://teams.microsoft.com/	JSmith12345	[redacted]	MSOnly_Access, WhiteList, Chat
10/7/2019 3:29:34 PM	tcp://clients2.google.com/	JSmith12345	[redacted]	VDI_RestrictedAccess, Search En
10/7/2019 3:29:34 PM	tcp://clientservices.googleapis.com/	JSmith12345	[redacted]	VDI_RestrictedAccess, Technolog
10/7/2019 3:29:28 PM	tcp://www.citrix.com/	JSmith12345	[redacted]	Technology/Internet
10/7/2019 3:29:58 PM	tcp://api.diagnostics.office.com/	JSmith12345	[redacted]	Bypass_Coach, MSOnly_Access,
10/7/2019 3:31:12 PM	tcp://www.citrix.com/	JSmith12345	[redacted]	Technology/Internet
10/7/2019 3:30:29 PM	tcp://www.gstatic.com/	JSmith12345	[redacted]	Search Engines/Portals
10/7/2019 3:32:02 PM	tcp://g.live.com/	JSmith12345	[redacted]	Search Engines/Portals
10/7/2019 3:29:57 PM	tcp://api.diagnostics.office.com/	JSmith12345	[redacted]	Bypass_Coach, MSOnly_Access,
10/7/2019 3:32:02 PM	tcp://oneclient.sfx.ms/	JSmith12345	[redacted]	File Storage/Sharing
10/7/2019 3:30:00 PM	tcp://messaging.office.com/	JSmith12345	[redacted]	Bypass_Coach, MSOnly_Access,
10/7/2019 3:30:27 PM	tcp://iecvlist.microsoft.com/	JSmith12345	[redacted]	MSOnly_Access, WhiteList, Techr
10/7/2019 3:30:04 PM	tcp://config.teams.microsoft.com/	JSmith12345	[redacted]	MSOnly_Access, WhiteList, Chat

10/7/2019 3:29:30 PM

DETAILS

ARTIFACT INFORMATION

Date and Time	10/7/2019 3:29:30 PM
Url	tcp://graph.microsoft.com/
User	JSmith12345
Client IP	[redacted]
Category	MSOnly_Access, WhiteList, Technology/Internet
Status	200
Verdict	Allowed
Web Application Name	Office 365 General
Web Application Operation	-
Total Bytes	320
Requests	1
Browse Time	0
User Agent	mozilla/5.0 (windows nt 10.0; win64; x64) applewebkit/537.36 (khtml, like gecko) chrome/64.0.3282.140 safari/537.36 edge/17.17134
Content Type	-
Malware	-

Automation & Orchestration with AWS

MAGNET FORENSICS®

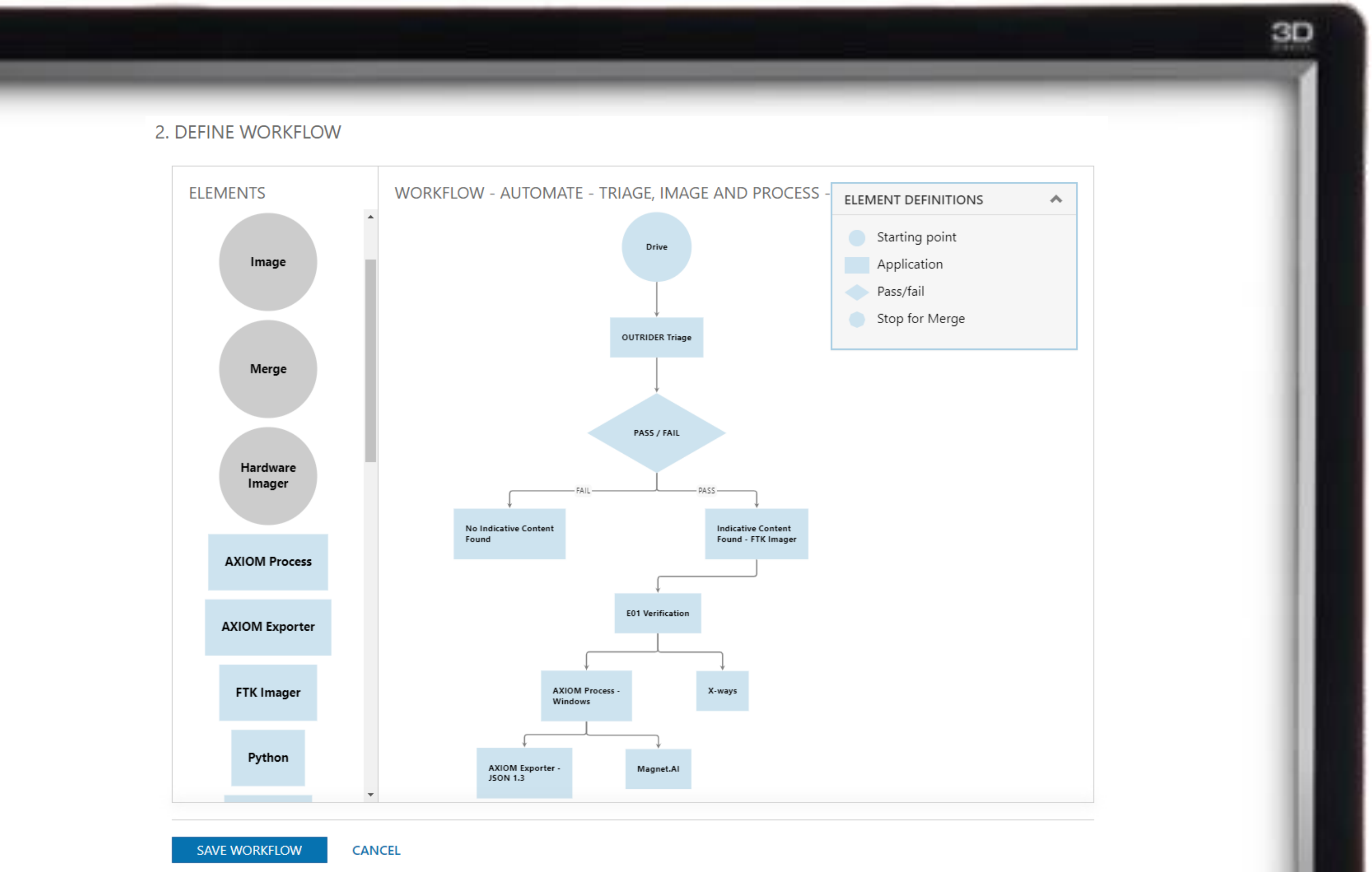
MAGNET AUTOMATE™

Improve service to your agency by scaling up existing resources and processes with the power of orchestration and automation.

Magnet AUTOMATE is an orchestration and automation platform that uses your lab’s existing hardware and software tools to create standardized workflows, to image and process data without examiner intervention.

Simplified Workflows

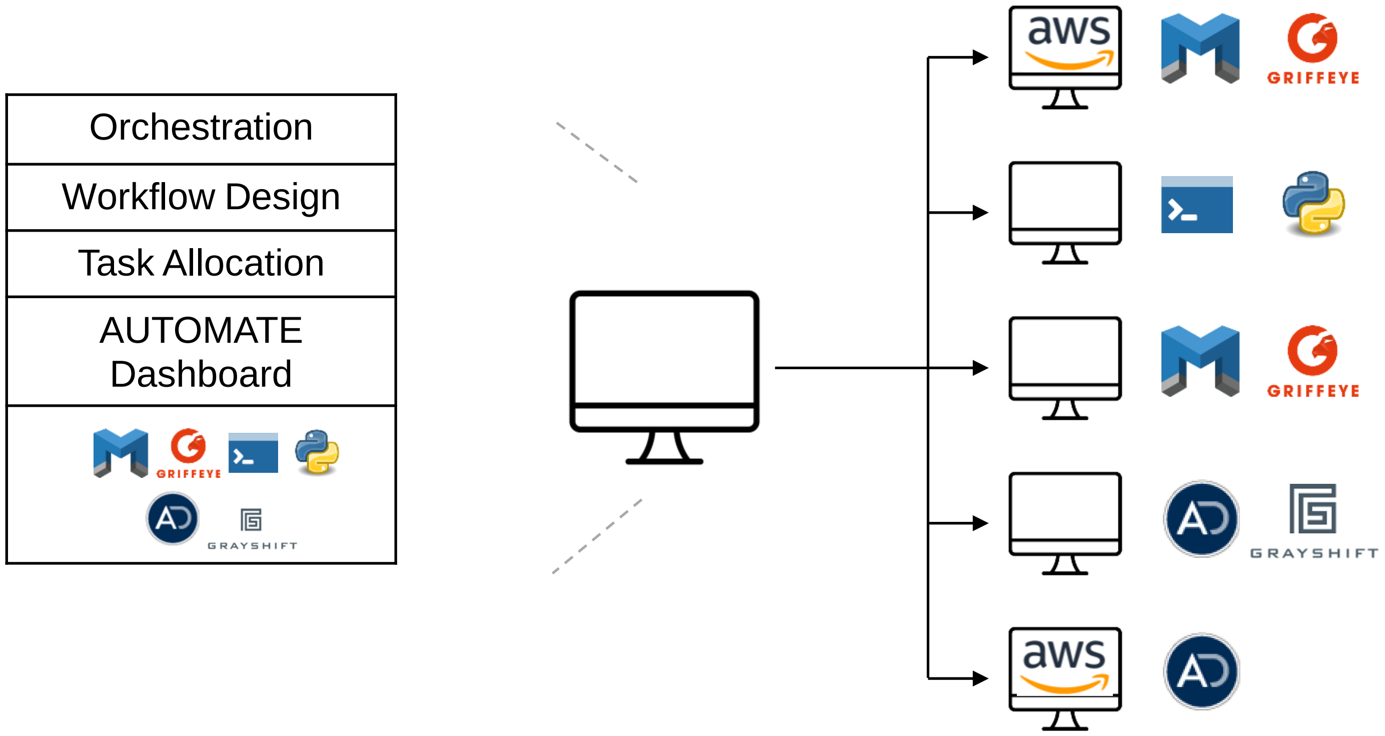
Consistent and easy-to-use



- Visual workflows designed using an easy drag-and-drop interface.
- Consistent workflows ensure the right workflow is used for each investigation.

Parallel Processing

Get more with existing hardware



Orchestration

Workflow Design

Task Allocation

AUTOMATE Dashboard

- Leverage the full power of your IT investments by processing cases using two or more workstations.

- Utilize assets on-prem, virtual, cloud or hybrid environments.

Watch Folders

AUTOMATE 2.2

Accelerate mobile investigations with AUTOMATE

- Integrate *any acquisition tool* within workflows, including mobile, even if they don’t have a command line interface
- Cases seamlessly flow from post-image acquisition through to processing with no downtime, improving the efficiency of computer and mobile workflows.

Thank you!

Questions?

trey.amick@magnetforensics.com
curtis.mutter@MagnetForensics.com

http://www.magnetforensics.com