Aviatrix Workload Attack Path Assessment Getting Started Guide

Overview

The **Workload Attack Path Assessment** is a free, agentless assessment that shows how attackers could move inside your cloud–without deploying any infrastructure or making any changes to your environment.

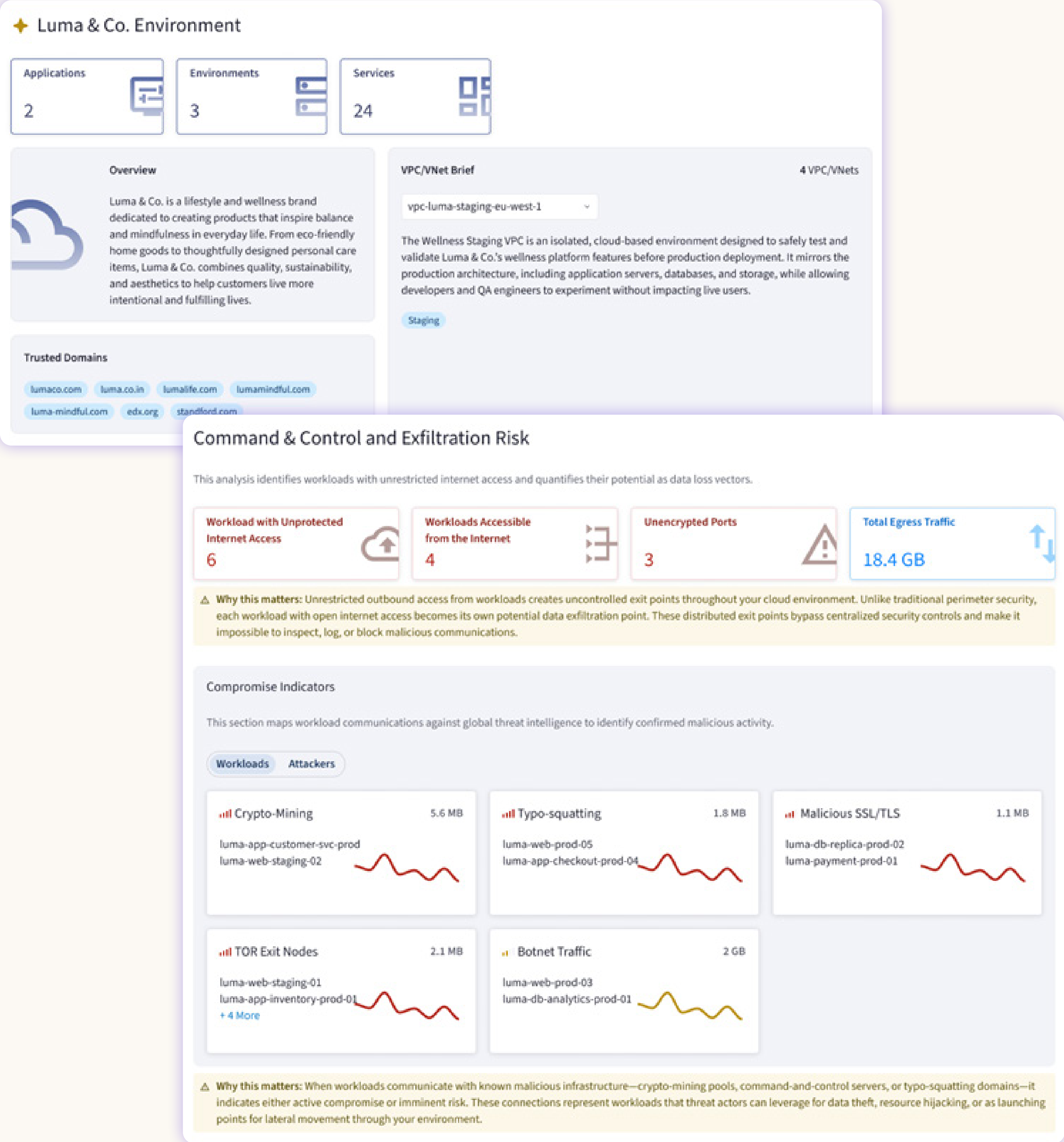
Using only temporary, **read-only access** to your cloud accounts, the assessment analyzes **flow logs, DNS logs, and cloud resource metadata** to automatically discover your applications and map their real runtime behaviors. It reconstructs **workload breach chains**–the multi-stage paths an attacker could take through lateral movement, malicious egress, and command-and-control activity.

Because it runs entirely on **Aviatrix's cloud-hosted platform**, nothing is installed in your environment. You simply grant read-only permissions. The assessment then provides a consolidated report showing:

- ✓ How workloads actually communicate across regions and clouds
- ✓ Risky outbound connections hidden behind NAT gateways
- ✓ Where segmentation, egress, or encryption gaps create exposure
- ✓ The breach chains that represent the most realistic paths from exposure to impact

The result is a clear, actionable understanding of **your workload attack exposure** and where zero trust enforcement is needed.

What's Included



Luma & Co. Environment

Applications 2

Environments 3

Services 24

Overview

Luma & Co. is a lifestyle and wellness brand dedicated to creating products that inspire balance and mindfulness in everyday life. From eco-friendly home goods to thoughtfully designed personal care items, Luma & Co. combines quality, sustainability, and aesthetics to help customers live more intentional and fulfilling lives.

VPC/VNet Brief — 4 VPC/VNets

vpc-luma-staging-eu-west-1

The Wellness Staging VPC is an isolated, cloud-based environment designed to safely test and validate Luma & Co.'s wellness platform features before production deployment. It mirrors the production architecture, including application servers, databases, and storage, while allowing developers and QA engineers to experiment without impacting live users.

Staging

Trusted Domains

lumaco.com luma.co.in lumalife.com lumamindful.com luma-mindful.com edx.org standford.com

Command & Control and Exfiltration Risk

This analysis identifies workloads with unrestricted internet access and quantifies their potential as data loss vectors.

Workload with Unprotected Internet Access 6

Workloads Accessible from the Internet 4

Unencrypted Ports 3

Total Egress Traffic 18.4 GB

⚠ **Why this matters:** Unrestricted outbound access from workloads creates uncontrolled exit points throughout your cloud environment. Unlike traditional perimeter security, each workload with open internet access becomes its own potential data exfiltration point. These distributed exit points bypass centralized security controls and make it impossible to inspect, log, or block malicious communications.

Compromise Indicators

This section maps workload communications against global threat intelligence to identify confirmed malicious activity.

Crypto-Mining 5.6 MB
luma-app-customer-svc-prod
luma-web-staging-02

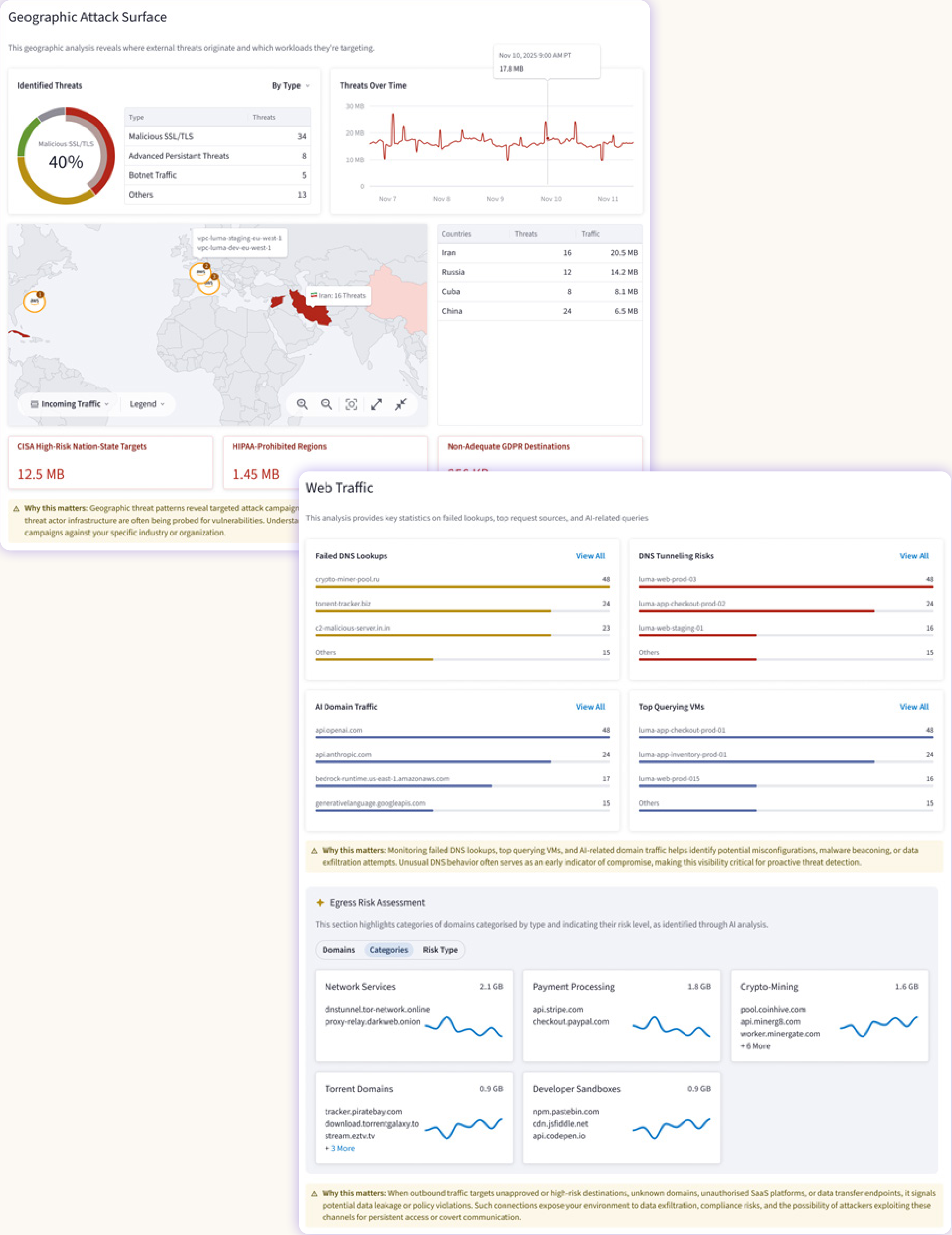
Typo-squatting 1.8 MB
luma-web-prod-05
luma-app-checkout-prod-04

Malicious SSL/TLS 1.1 MB
luma-db-replica-prod-02
luma-payment-prod-01

TOR Exit Nodes 2.1 MB
luma-web-staging-01
luma-app-inventory-prod-01
+ 4 More

Botnet Traffic 2 GB
luma-web-prod-03
luma-db-analytics-prod-01

⚠ **Why this matters:** When workloads communicate with known malicious infrastructure—crypto-mining pools, command-and-control servers, or typo-squatting domains—it indicates either active compromise or imminent risk. These connections represent workloads that threat actors can leverage for data theft, resource hijacking, or as launching points for lateral movement through your environment.



Geographic Attack Surface

This geographic analysis reveals where external threats originate and which workloads they're targeting.

Identified Threats By Type

Type	Threats
Malicious SSL/TLS	34
Advanced Persistant Threats	8
Botnet Traffic	5
Others	13

Threats Over Time

Countries	Threats	Traffic
Iran	16	20.5 MB
Russia	12	14.2 MB
Cuba	8	8.1 MB
China	24	6.5 MB

CISA High-Risk Nation-State Targets

12.5 MB

HIPAA-Prohibited Regions

1.45 MB

Non-Adequate GDPR Destinations

⚠ **Why this matters:** Geographic threat patterns reveal targeted attack campaign
threat actor infrastructure are often being probed for vulnerabilities. Understa
campaigns against your specific industry or organization.

Web Traffic

This analysis provides key statistics on failed lookups, top request sources, and AI-related queries

Failed DNS Lookups View All

crypto-miner-pool.ru	48
torrent-tracker.biz	24
c2-malicious-server.in.in	23
Others	15

DNS Tunneling Risks View All

luma-web-prod-03	48
luma-app-checkout-prod-02	24
luma-web-staging-01	16
Others	15

AI Domain Traffic View All

api.openai.com	48
api.anthropic.com	24
bedrock-runtime.us-east-1.amazonaws.com	17
generativelanguage.googleapis.com	15

Top Querying VMs View All

luma-app-checkout-prod-01	48
luma-app-inventory-prod-01	24
luma-web-prod-015	16
Others	15

⚠ **Why this matters:** Monitoring failed DNS lookups, top querying VMs, and AI-related domain traffic helps identify potential misconfigurations, malware beaconing, or data exfiltration attempts. Unusual DNS behavior often serves as an early indicator of compromise, making this visibility critical for proactive threat detection.

Egress Risk Assessment

This section highlights categories of domains categorised by type and indicating their risk level, as identified through AI analysis.

Domains | **Categories** | Risk Type

Network Services 2.1 GB
dnstunnel.tor-network.online
proxy-relay.darkweb.onion

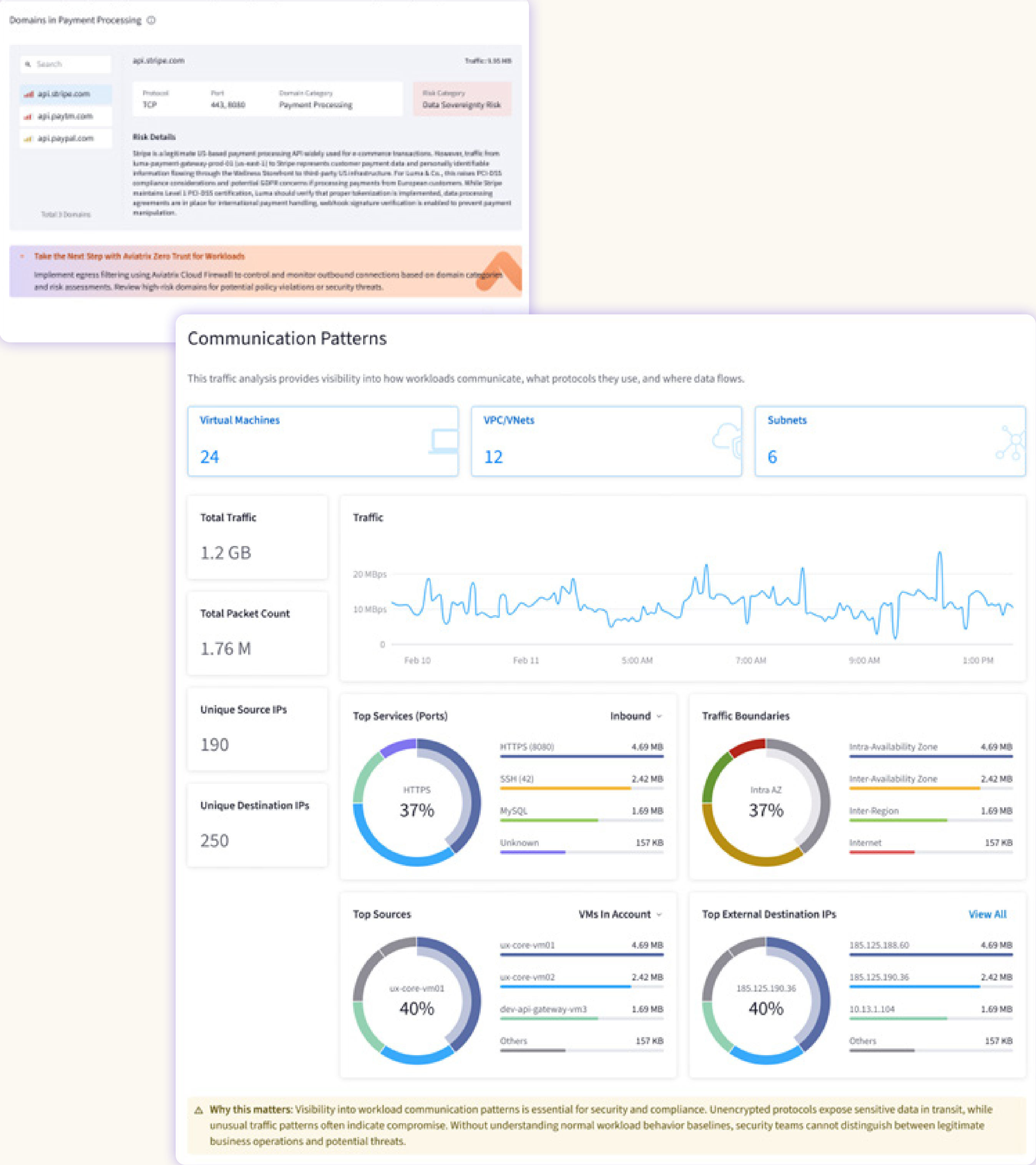
Payment Processing 1.8 GB
api.stripe.com
checkout.paypal.com

Crypto-Mining 1.6 GB
pool.coinhive.com
api.minerg8.com
worker.minergate.com
+ 6 More

Torrent Domains 0.9 GB
tracker.piratebay.com
download.torrentgalaxy.to
stream.eztv.tv
+ 3 More

Developer Sandboxes 0.9 GB
npm.pastebin.com
cdn.jsfiddle.net
api.codepen.io

⚠ **Why this matters:** When outbound traffic targets unapproved or high-risk destinations, unknown domains, unauthorised SaaS platforms, or data transfer endpoints, it signals potential data leakage or policy violations. Such connections expose your environment to data exfiltration, compliance risks, and the possibility of attackers exploiting these channels for persistent access or covert communication.



Domains in Payment Processing ⓘ

Search

- api.stripe.com
- api.paytm.com
- api.paypal.com

Total 3 Domains

api.stripe.com

Traffic: 5.95 MB

Protocol	Port	Domain Category	Risk Category
TCP	443, 8080	Payment Processing	Data Sovereignty Risk

Risk Details

Stripe is a legitimate US-based payment processing API widely used for e-commerce transactions. However, traffic from luma-payment-gateway-prod-01 (us-east-1) to Stripe represents customer payment data and personally identifiable information flowing through the Wellness Storefront to third-party US infrastructure. For Luma & Co., this raises PCI-DSS compliance considerations and potential GDPR concerns if processing payments from European customers. While Stripe maintains Level 1 PCI-DSS certification, Luma should verify that proper tokenization is implemented, data processing agreements are in place for international payment handling, webhook signature verification is enabled to prevent payment manipulation.

Take the Next Step with Aviatrix Zero Trust for Workloads

Implement egress filtering using Aviatrix Cloud Firewall to control and monitor outbound connections based on domain categories and risk assessments. Review high-risk domains for potential policy violations or security threats.

Communication Patterns

This traffic analysis provides visibility into how workloads communicate, what protocols they use, and where data flows.

Virtual Machines	VPC/VNets	Subnets
24	12	6

Metric	Value
Total Traffic	1.2 GB
Total Packet Count	1.76 M
Unique Source IPs	190
Unique Destination IPs	250

Traffic

Top Services (Ports) — Inbound

Service	Traffic
HTTPS (8080)	4.69 MB
SSH (42)	2.42 MB
MySQL	1.69 MB
Unknown	157 KB

Traffic Boundaries

Boundary	Traffic
Intra-Availability Zone	4.69 MB
Inter-Availability Zone	2.42 MB
Inter-Region	1.69 MB
Internet	157 KB

Top Sources — VMs In Account

Source	Traffic
ux-core-vm01	4.69 MB
ux-core-vm02	2.42 MB
dev-api-gateway-vm3	1.69 MB
Others	157 KB

Top External Destination IPs — View All

Destination IP	Traffic
185.125.188.60	4.69 MB
185.125.190.36	2.42 MB
10.13.1.104	1.69 MB
Others	157 KB

⚠ **Why this matters:** Visibility into workload communication patterns is essential for security and compliance. Unencrypted protocols expose sensitive data in transit, while unusual traffic patterns often indicate compromise. Without understanding normal workload behavior baselines, security teams cannot distinguish between legitimate business operations and potential threats.

Pre-Assessment Preparation

Account Access

Ensure you have access to at least one AWS or Azure account/subscription that can grant the necessary IAM or Azure RBAC permissions:

→ For **AWS**, ensure you have permissions to run a Cloud Formation Template that will create **read-only** IAM roles and policies

→ For **Azure**, ensure you have permissions to create a custom role with **read-only/ list** permissions (see Appendix)

Flow Logs

The security assessment analyzes flow log data to provide the traffic and threat analysis.

→ For **AWS**, ensure flow logs are available from an S3 bucket

→ For **Azure**, ensure NSG flow logs are available in Azure Blob storage

Ideally, you would collect ~7 days of flow log data before running the assessment.

Best Practices

→ Run it on AWS (when possible)

- Azure does not have DNS Logs, and some sections would be unavailable

→ Pick a VPC with Egress Traffic

- Most of your analysis is on Egress Traffic

→ Setup longer batching time interval for Flow Logs to Bucket (10 minutes)

- Reduces ingestion time

```
aws ec2 create-flow-logs \
--resource-type VPC \
--resource-ids vpc-xxxxx \
--traffic-type ALL \
--log-destination-type s3 \
--log-destination arn:aws:s3:::your-bucket-name/prefix/ \
--max-aggregation-interval 600
```

Appendix

Enable VPC Flow Logs to send to S3 Bucket using AWS console:

1. **Navigate to VPC Flow Logs**
   a. Open AWS Console → VPC service
   b. Select "Your VPCs" from left menu
   c. Select the VPC you want to monitor
   d. Go to "Flow logs" tab
   e. Click "Create flow log"
2. **Configure Flow Log Settings (Accept All Defaults, except the following)**
   a. **Name**: VPC-FlowLogs-S3
   b. **Filter**: Select "All" (captures both accepted and rejected traffic)
   c. **Destination**: Select "Send to an S3 bucket"
   d. Copy the S3 bucket ARN of existing bucket or create a new S3 bucket.
3. **Create S3 Bucket (Accept all Defaults, except the following)**
   a. **Bucket name**: `my-vpc-flow-logs-bucket` (must be globally unique)
   b. **Region**: Choose your preferred region

Click "Create bucket" **Account Access**

Export VPC Flow Logs from CloudWatch to S3 Bucket using AWS console:

1. Go to CloudWatch → Log groups
2. Select your VPC Flow logs group
3. Click “Actions” → “Export data to Amazon S3”
4. Configure the export settings

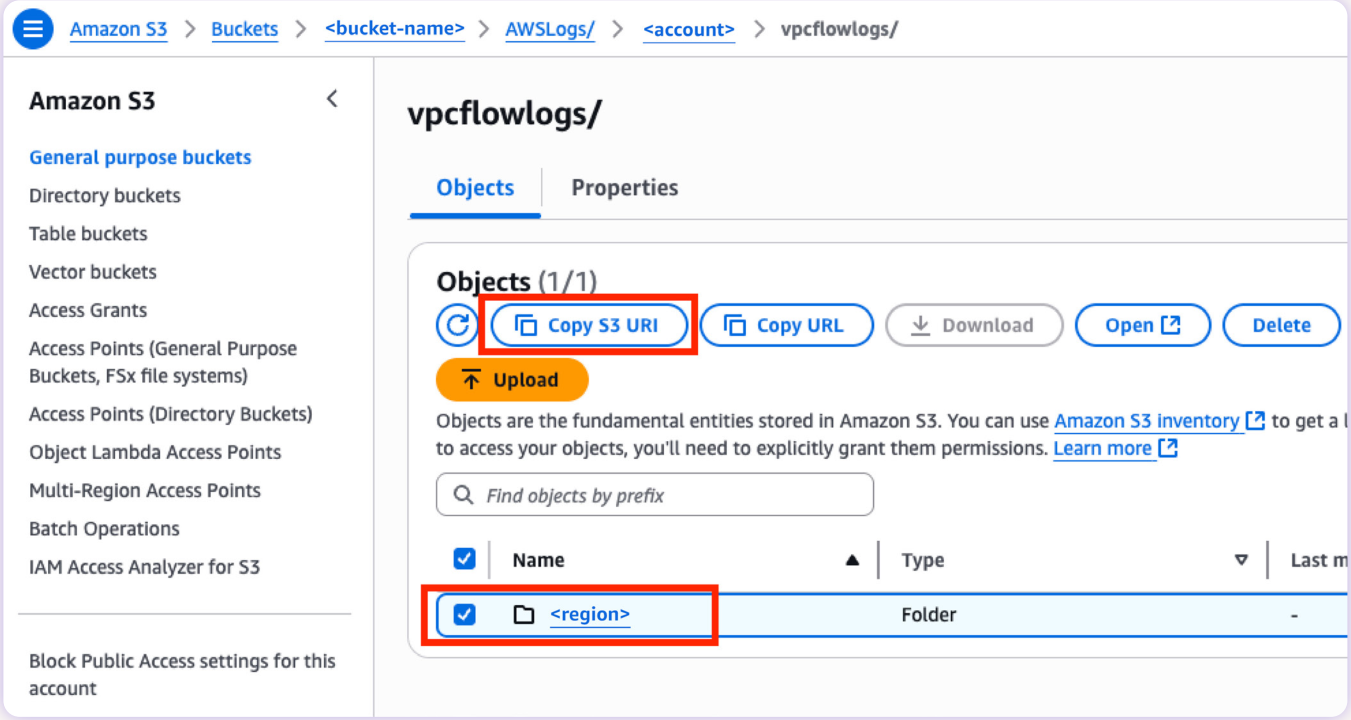
Obtain the URI of the AWS Flow Log S3 bucket.

Go to **Amazon S3 > Buckets > _<bucket-name>_ > AWSLogs > _<account-name>_ > vpcflowlogs,** then select the region for the logs, and click Copy S3 URI.

It should be in the format:

s3://<bucketname>/AWSLogs/<account-number>/vpcflowlogs/<region>

The below example shows where to obtain the VPC flow log information.


Amazon S3 > Buckets > <bucket-name> > AWSLogs/ > <account> > vpcflowlogs/
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Vector buckets
Access Grants
Access Points (General Purpose Buckets, FSx file systems)
Access Points (Directory Buckets)
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
vpcflowlogs/
Objects
Properties
Objects (1/1)
Copy S3 URI
Copy URL
Download
Open
Delete
Upload
Find objects by prefix

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a l
to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name	Type	Last m
☑	<region>	Folder	-

Azure role definition

```
{
  “Name”: “$CUSTOM_ROLE_NAME”,
  “Description”: “Custom read-only role for Aviatrix PaaS with log
access”,
  “Actions”: [
    “Microsoft.Compute/*/read”,
    “Microsoft.Storage/storageAccounts/read”,
    “Microsoft.Storage/storageAccounts/blobServices/containers/read”,
    “Microsoft.Storage/storageAccounts/listServiceSas/action”,
    “Microsoft.Storage/storageAccounts/listAccountSas/action”,
    “Microsoft.Storage/storageAccounts/listkeys/action”,
    “Microsoft.Network/*/read”,
    “Microsoft.Resources/*/read”,
    “Microsoft.ResourceHealth/*/read”,
    “Microsoft.Resources/subscriptions/resourceGroups/read”,
    “Microsoft.Resources/tags/read”,
    “Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/
agreements/read”
  ],
  “NotActions”: [],
  “DataActions”: [
    “Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
read”
  ],
  “NotDataActions”: [],
  “AssignableScopes”: [
    “/subscriptions/$SUB_ID”
  ]
}
```

Steps to Enable DNS Logs to send to S3 Bucket (AWS)

1. Go to the AWS Console and navigate to **Route 53** > **Resolver** > **Query Logging.**
2. Click **Configure query logging.**
   a. Enter a name for the query log configuration, such as **vpc-dns-query-logs.**
   b. For the destination, select **S3 Bucket.**
   c. Choose an existing S3 bucket or create a new one as the destination for the query logs.
3. Click Add VPCs to select the VPCs.
4. Click **Configure query logging** to complete the setup.