

+ Netskope SASE/SSE Platforms - Updates

DISA Technical Exchange Meeting (TEM).
Capability Briefing Oct 31, 2024

Netskope: A Leader in SSE. A leader in SASE.

2024 Gartner Magic Quadrant for Security Service Edge



2024 Gartner Magic Quadrant for Single-Vendor SASE



These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Netskope. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

*Gartner, Magic Quadrant for Security Service Edge, Charlie Winckless, Aaron McQuaid, John Watts, Craig Lawson, Thomas Lintemuth, Dale Kooppen, April 15, 2024

*Gartner, Magic Quadrant for Single-Vendor SASE, Andrew Lerner, Neil MacDonald, Jonathan Forest, Charlie Winckless, July 3, 2024.

Gartner and Magic Quadrant are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

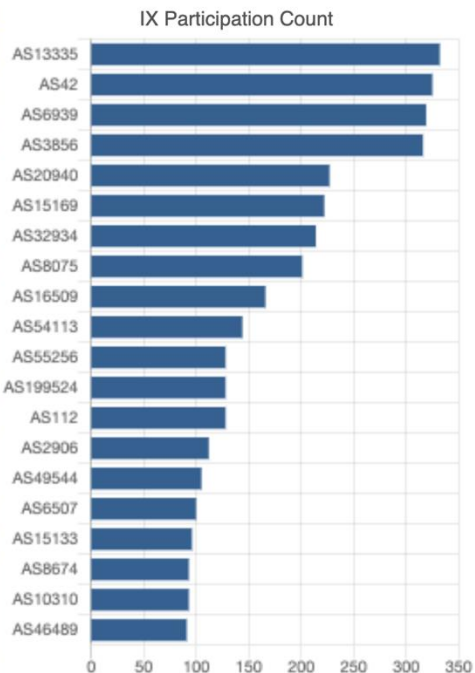
SASE Architectural Framework



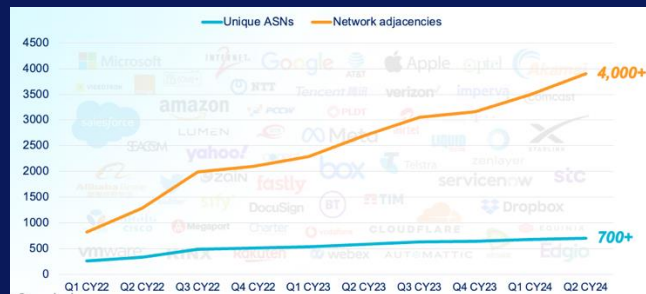
NewEdge - 'top 11' most active global IX participants

IXs translate into better coverage and more paths to achieve best performance/availability

IX Participation Count		
ASN	Name	IXes
AS13335	Cloudflare, Inc.	332
AS42	WoodyNet, Inc.	325
AS6939	Hurricane Electric LLC	319
AS3856	Packet Clearing House, Inc.	316
AS20940	Akamai International B.V.	227
AS15169	Google LLC	222
AS32934	Facebook, Inc.	214
AS8075	Microsoft Corporation	201
AS16509	Amazon.com, Inc.	166
AS54113	Fastly, Inc.	144
AS55256	Netskope Inc	128
AS199524	G-Core Labs S.A.	128
AS112	DNS-OARC	128
AS2906	Netflix Streaming Services Inc.	112
AS49544	i3D.net B.V	105
AS6507	Riot Games, Inc	100
AS15133	Edgecast Inc.	96
AS8674	Netnod AB	93
AS10310	Oath Holdings Inc.	93
AS46489	Twitch Interactive Inc.	91



- **IX / PX Peering**
- **Route Control**
- **Path optimization**
- **Localization Zones**
- **Decrypted traffic <50MS**
- **Non-Decrypted traffic < 10ms**
- **Real user monitoring**
- **Periodic GSLB / RTT calculation**
- **L3 - L7; Server initiated, VOIP / Video**

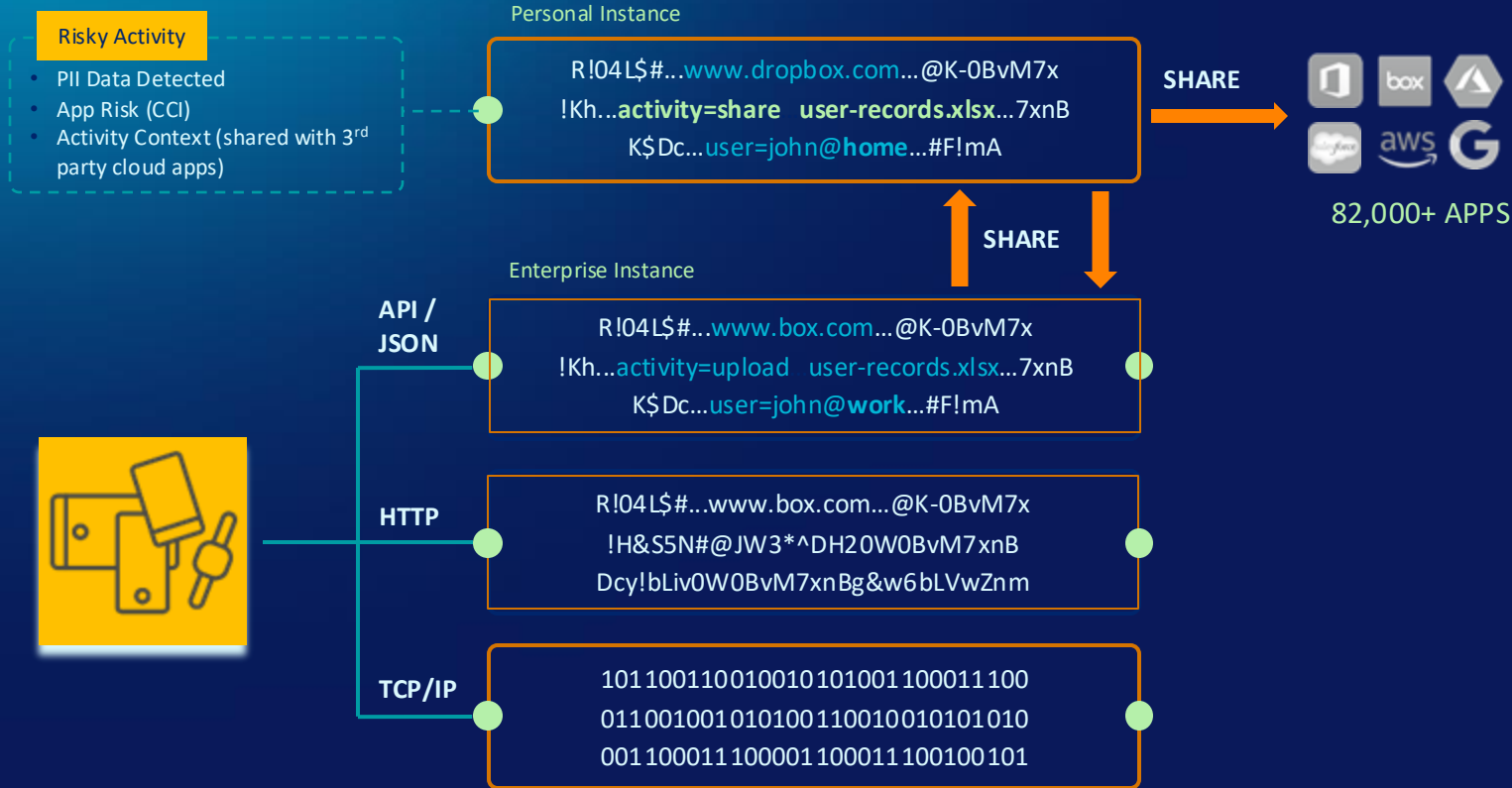


Traffic steering control



- Any user, any device (including SD-WAN), from anywhere, to any app...
 - zone-specific steering for traffic to ensure compliance

Netskope Inline Security



Without the Netskope Zero Trust Engine

You would lose the ability to make risk-based decisions on the important parts of the transaction

**IDENTITY
TRUST**

Should the
Identity
be Trusted?

**DEVICE
TRUST**

Should the
Device
be Trusted?

**LOCATION
TRUST**

Should the
Location
be Trusted?

**APP
TRUST**

Should the
App
be Trusted?

**INSTANCE
TRUST**

Should the
App Instance
be Trusted?

**ACTIVITY
TRUST**

Should the
App Activity
be Allowed?

**BEHAVIOR
TRUST**

Should the
Behavior
be Allowed?

**DATA
TRUST**

Should the
Data
be Allowed?









ALLOW
BLOCK
COACH
AUTH
JUSTIFY
ISOLATE

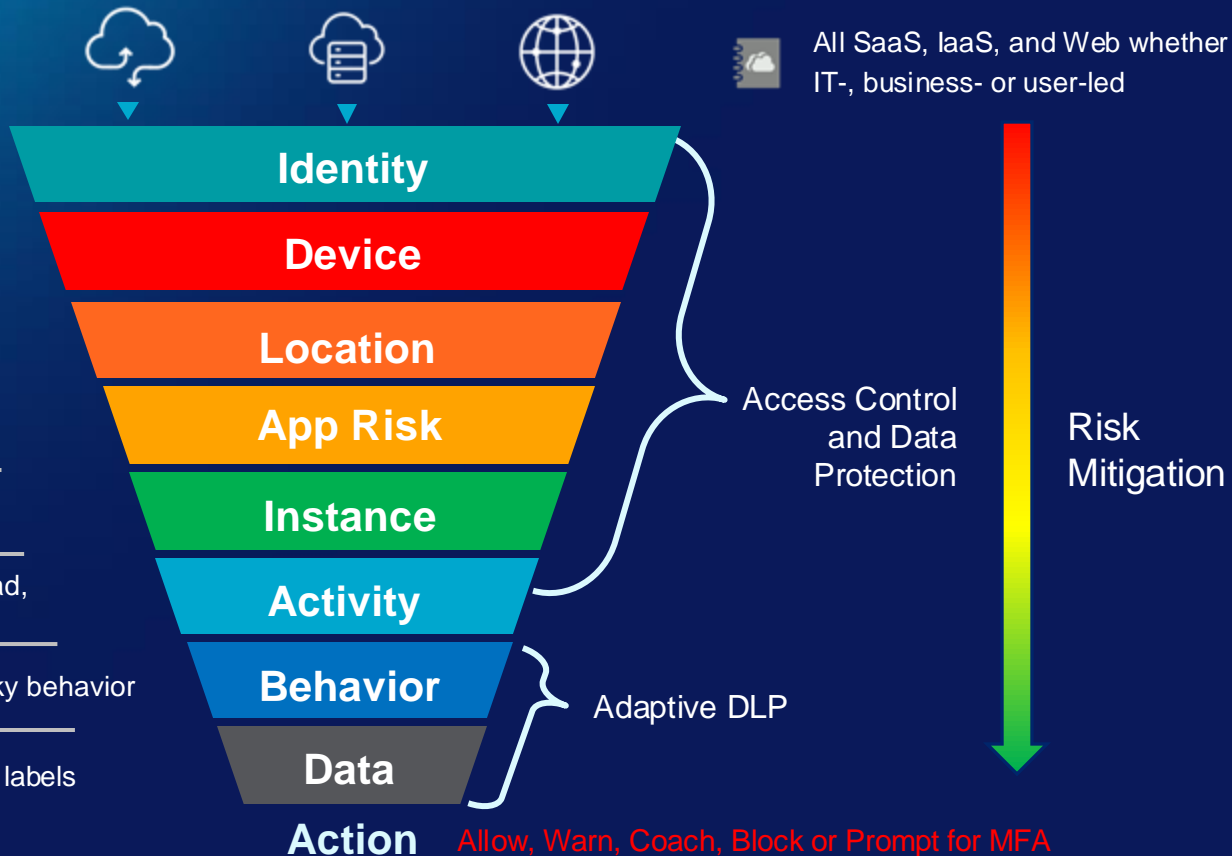
What **Action**
Should Be
Taken?

Netskope Native TLS 1.3 Decryption
Context based data protection
Netskope Inline Granular Policy Enforcement
Dynamic Assessment of Risk
User Entity Behaviour Analytics
Bi-directional Risk and threat exchange
Adaptive Access Controls

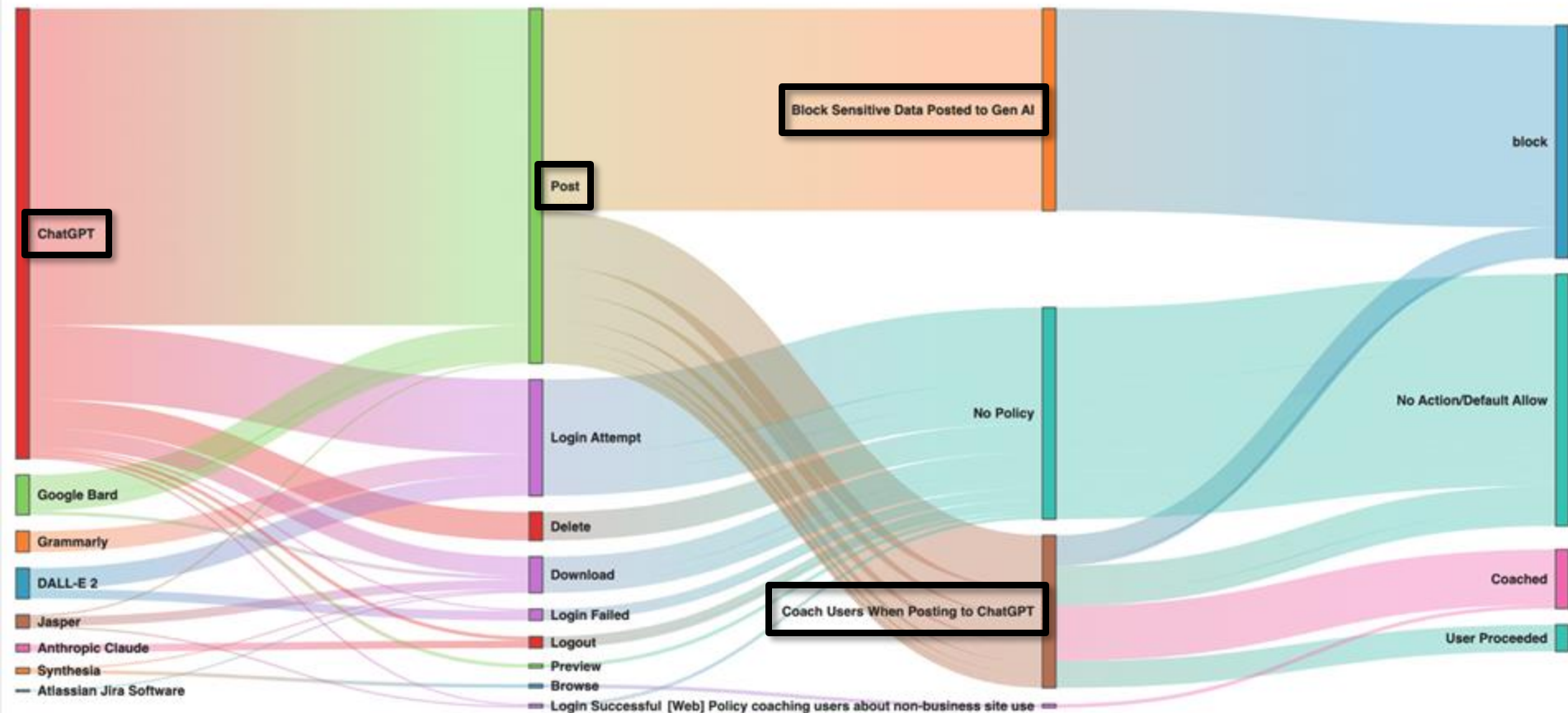
Netskope Zero Trust Policy In Practice

Zero trust in Practice

-  Restrict access based on identity
-  Restrict access based on device
-  Restrict access based on location/network
-  Block high risk cloud services
-  Restrict access to third party instances of allowed applications
-  Block high risk activities such as upload, edit and share
-  Restrict access based on previous risky behavior
-  Identify sensitive data or classification labels



Policies and Actions Controlling AI Usage



Next TEM

- ZTNA – L3 to L7
- Digital Experience Monitoring (REM)
- Enterprise Browser
- Web based E2E Applications SSLi
- Web based E2E Applications with RBI
- Cloud TAP – Full PCAP with Keylog File.
- Cloud log streaming
- Cloud Exchange
- Data Security Posture management (RDBMS + Unstructured data including file shares)

Skope AI



Netskope SkopeAI

Security and Performance Updates

Skope AI- AI Across the Portfolio



SkopeAI Data Protection

- Automatically protect unstructured data with high reliability and speed with pre-trained ML classifiers
- Protect novel data with Train Your Own Classifiers (TYOC)



SkopeAI Threat Protection

- Prevent evasive attacks, polymorphic malware, new phishing, zero-day
- Faster detection and categorization of malware, web domains, URLs, and web content



Generative AI and SaaS

- Discover and govern the use of generative AI and novel SaaS apps
- Protect sensitive data across apps like ChatGPT and coach employees in real-time



User & Entity Behavior

- Detect users' unpredictable risky behavior
- Identify insiders' anomalous behavior, compromised accounts, data exfiltration



SD-WAN Optimization

- Optimal network access through enterprise-wide predictive insights
- WAN access anomaly detection, app performance flow analytics



Device Access Intelligence

- Discover newly connected devices and gain deeper device context, activities and behavior
- Real-time detection of behavioral anomalies, threats and vulnerabilities

Data Protection that Mimics the Human Brain



Conventional DLP → Not a credit card

Text-only methods applied:

- Optical Character Recognition (OCR)
- Regular Expressions Matching
- Text Matching



SkopeAI DLP → It is a credit card

Text + AI/ML Imaging methods applied:

- ML Classifiers with computer vision and statistical modeling
- Natural language processing (NLP)
- Optical Character Recognition (OCR)
- Regular Expressions Matching
- Text Matching
- Document Matching

Skope AI Data Protection - DLP ML Classifiers

• ML Image Classification



Passports



Driver's Licenses



Social Security Cards



Credit/Debit Cards



Pay Check



Insurance Cards

Whiteboards

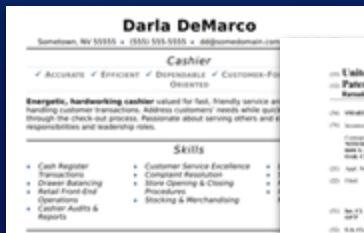


Screenshots



AI/ML: Deep Learning, Convolutional Neural Network (CNN), YOLO v5 object detection algorithms

• ML Document Classification



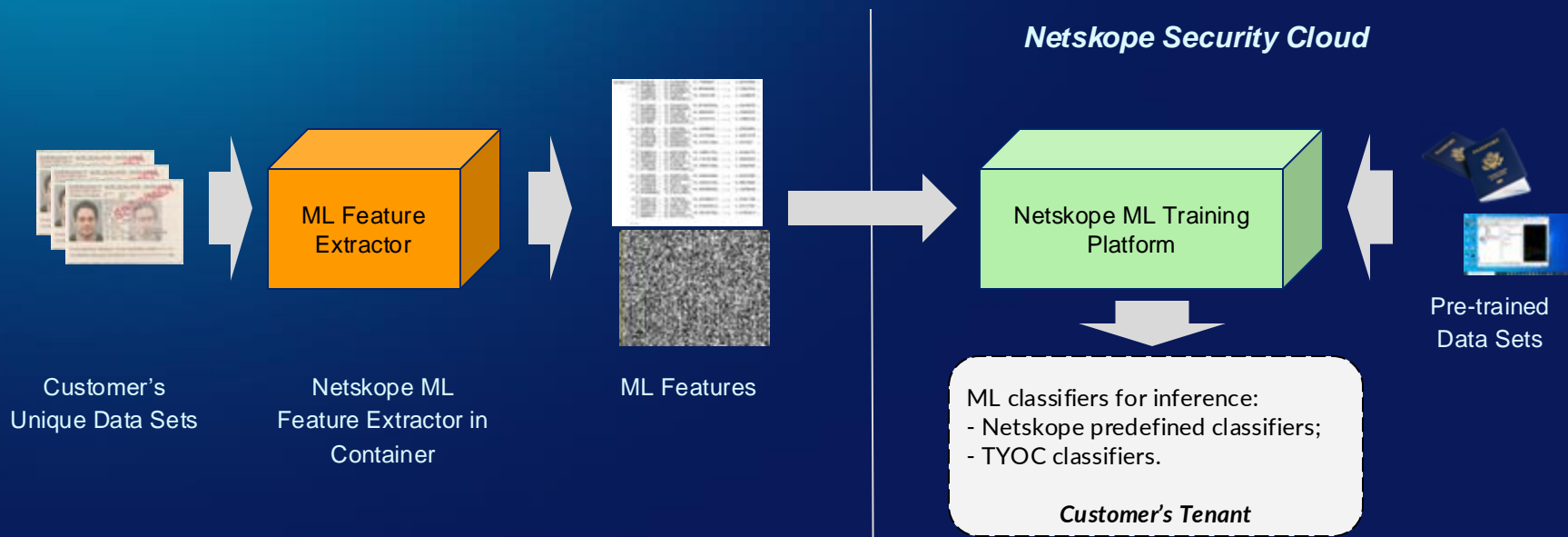
Bank Statement
Consulting Agreement
M&A document
NDAs
Offer Letter
Partner Agreement

Patents
Power of Attorney
Resume
Source code
Stock Agreement
Tax document



AI/ML: Advanced Natural Language Processing (NLP)

Skope AI Data Protection - DLP Train Your Own Classifier



TYOC: Customers train ML with their unique data sets to complement predefined ML classifiers

Skope AI Threat Protection

- ML Detection of New and Existing Phishing Websites



AI/ML: Deep learning of both URLs and page content, natural language processing and image classification, to detect both existing and newly registered phishing websites

- Dynamic URL Categorization Based on Web Content

"... Find singles looking to date. 40,000,000 singles worldwide and 3,000,000 messages sent daily ..."

"... BetOnline.ag is more than just an online betting platform. We boast a 'focus on the player' ..."

"... Welcome to Impact Guns, the nation's top online gun dealer. With our unbeatable prices and ..."



Dating
Gambling
Weapons



AI/ML: Natural language processing (NLP) enables the dynamic categorization of new and uncategorized web pages

2024 © Netskope Confidential. All rights reserved.

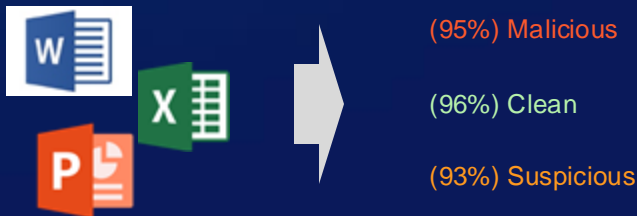
Skope AI Threat Protection

- Detection of Portable Executable (PE) Malware in FastScan



AI/ML: Raw file features, LightGBM and LSTM classifiers, reduced false negative rate with <60 ms inline latency

- Detection of Malware Infected Microsoft Office Files

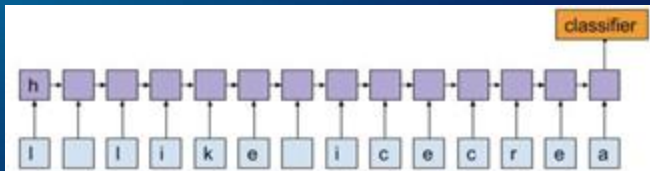


AI/ML: Boosted Tree supervised machine learning (ML) with heuristics detect infected Microsoft Office files

2024 © Netskope Confidential. All rights reserved.

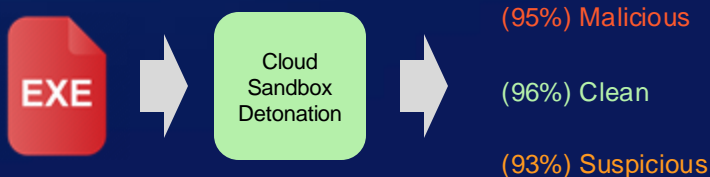
Skope AI Threat Protection

- Domain Generation Algorithm (DGA) Detection



AI/ML: Deep neural network to accurately detect and classify DGA domains frequently used by modern malware

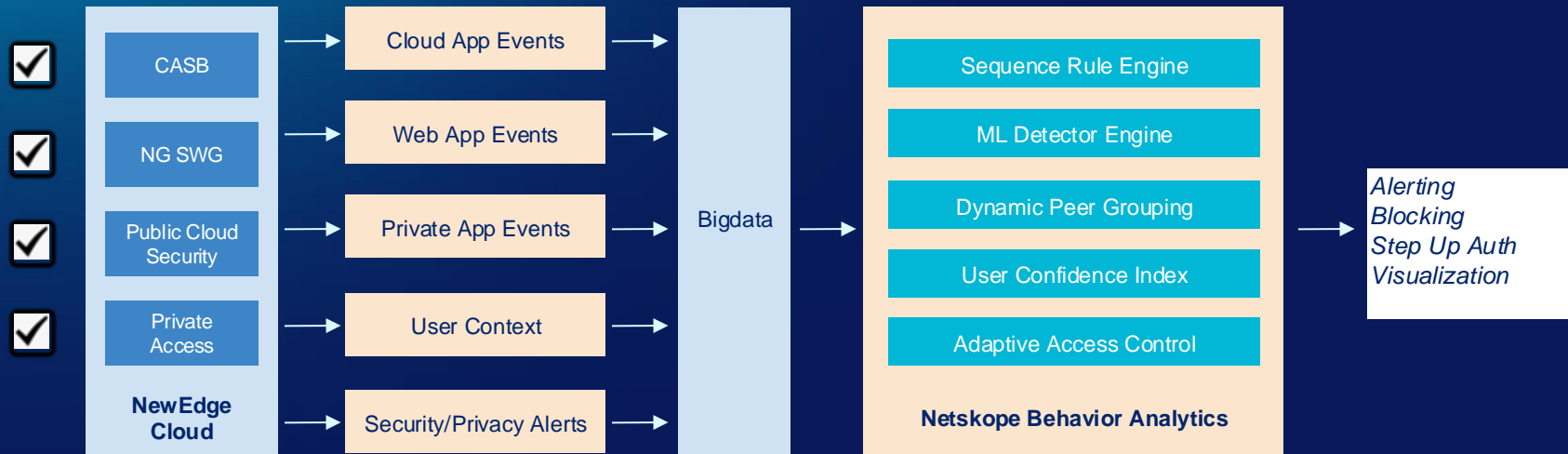
- AI-boosted Cloud Sandbox



AI/ML: Machine learning deep analysis with sandboxing automatically detects unknown threats, anomalies, and behaviors without manually defined rules

Skope AI User and Entity Behavior Analytics

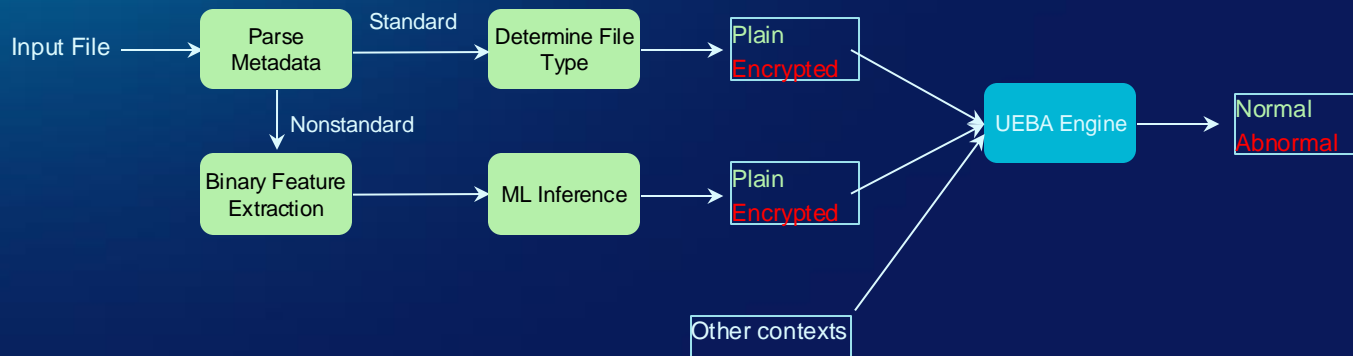
AI/ML user behavior anomaly detection



AI/ML UEBA: Discern normal behavior versus anomalies, discovering malicious insiders, compromised accounts, data exfiltration, brute force attacks and user-defined anomalies

Skope AI User and Entity Behavior Analytics

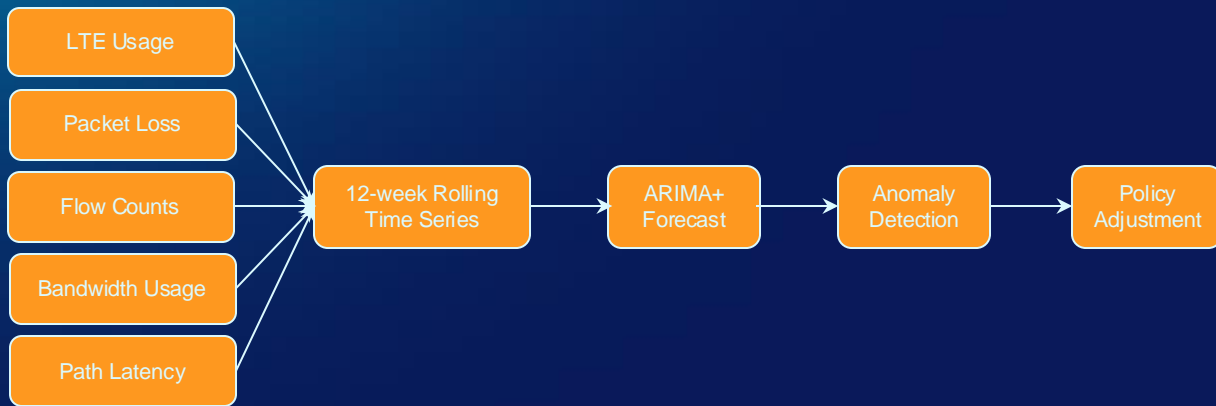
Ransomware attack detection based on encrypted file detection and anomalous behavior



AI/ML UEBA: Trained ML model differentiates plain and encrypted content. UEBA generates user-level alerts when an anomalous amount of encrypted data movements occur

Skope AI SD-WAN Optimization

AI/ML SD-WAN access anomaly detection



AI/ML: Use statistical modeling to detect WAN access performance metric anomalies and adjust policies accordingly

SkopeAI Device Access Intelligence

- Automatic Device Classification



AI/ML: Extract layer 2-7 protocol features from network traffic to build ML model to classify new devices. Combine it with rules generated from knowledge-base to improve coverage and accuracy

- Automatic Device Identification



AI/ML: Use RF, location, layer 2-7 network traffic metadata, device classification result and deep neural networks to fingerprint new devices

Thank you

John Schroder
jschroder@netskope.com