

Versatility 2025



AI/ML for security use cases

Agenda

- Pain points in cybersecurity
- Key components
- AI/ML for Advanced Threat Prevention (ATP)
- AI/ML for Data Loss Prevention (DLP)
- AIOps for cybersecurity
- Questions

Today's Pain Points - Threat Prevention(ATP)

SaaS/IaaS/PaaS sprawl –
Increasing Attack surface

- *Security teams overwhelmed by alert volume.*
- *Difficult to identify genuine threats amidst the noise.*

Financial impact - TTRR

- *Average cost of a data breach crossed \$4.5m in 2023, a 15% YoY increase.*
- *277 days to Respond and Remediate breaches (204 to Respond, 73 to Remediate) in 2023.*
- *Loss of brand confidence.*

Multiple point products -
Integration complexity

- *On average there are 76 different security solutions which creates problem of interworking the disparate security solutions*
- *54% of SoC teams feel burnt out fielding security events, 45% of which were false positives.*

Attack sophistication

- *AI-created malware, zero-day exploits used by attackers to launch sophisticated and faster attacks.*
- *Ransomware attacks increased 24% YoY costing around \$5.3m to Respond and Remediate.*

Today's Pain Points - Data Loss Prevention(DLP)

Data Visibility & Classification

- *Identifying sensitive data across complex environments (on-prem, cloud, SaaS) is challenging.*
- *Complexities in data classification is a primary barrier to effective DLP implementation*

Balancing Security & Productivity

- *Strict DLP rules can block legitimate business activities.*
- *Employees/Users could potentially use insecure workarounds ("shadow IT").*
- *Tuning DLP policies to be effective without hindering productivity is difficult.*

Data Protection in hybrid work environments

- *Data sprawl across cloud services (IaaS, PaaS, SaaS) and accessed by remote workers.*
- *Data breaches cost about USD 1 million more on average at organizations.*

Insider Threats

- *Threats originating from within the Org (malicious or accidental) are harder to detect.*
- *Internal "privilege misuse" and "error" patterns remain significant factors in breaches.*

Versa AI for file/stream-based Security – Key Components

Threat Protection

AI/ML Based Malware Detection

What is it?

Multi-stage AI/ML for real-time processing of files to identify malware



Key benefits

- ✓ Eliminates zero-day attacks covering 90 % of file types used to transmit malware while reducing sandbox load by 75%


Data Protection

AI/ML Based Data Loss Prevention

For dynamic, adaptive protection from data loss (unintentional or malicious)



- ✓ Detection of sensitive data in text documents and image – enabling more accurate and dynamic data security.



AI/ML – Advanced Threat Prevention (ATP)

Versatility 2025

© 2025 Versa and/or its affiliates. All rights reserved.



AI/ML based Malware Detection – 1,000 ft view

Reduce reliance on static signatures:

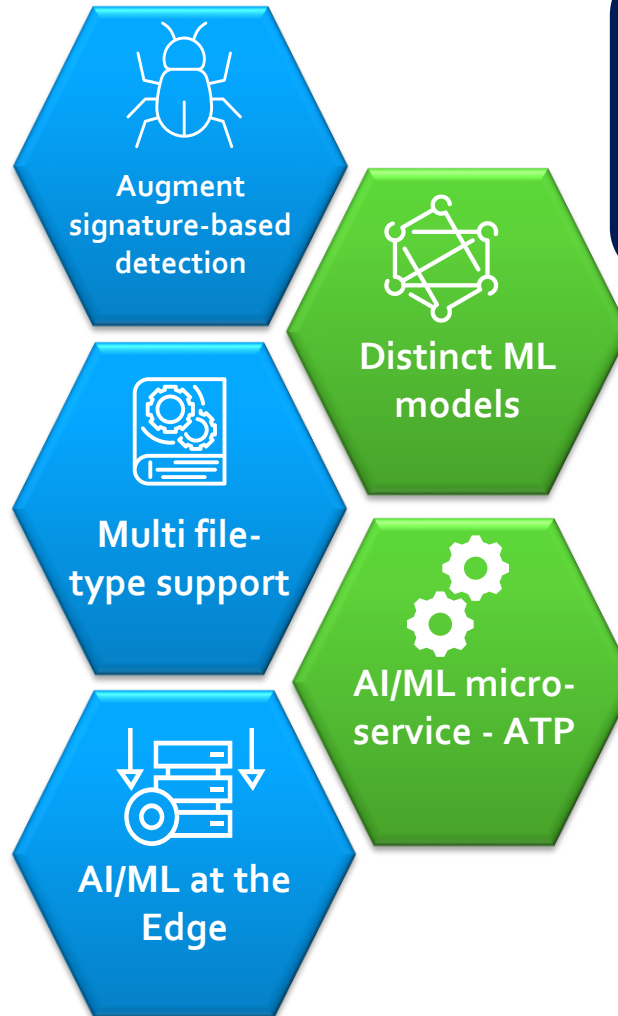
- AI/ML-based malware detection systems can identify patterns and characteristics common to malware behaviors.
- Extract the way malware interacts with the system, such as auto-execution, data encryption, C&C communication etc.

AI/ML-based malware detection for common file-types:

- PE (Portable Executable)
- PDF
- Docx, Pptx, Xlsx, RTF
- HTML/JS (JavaScript).

AI/ML-based lightweight inference at the Edge:

- Subset of file-types.
- Down-select files.
- Sent to cloud ATP for analysis beyond certain confidence score.



Distinct ML models trained for each file-type

- Gradient-boosted trees.
- Deep Neural Networks.
- Multi-model Ensembles.
- Fine-tuned State-Of-The-Art transformer models.

AI/ML microservice – Integral part of ATP

- Receive file analysis request -> launch inference for file-type.
- Return results, [Clean, Suspicious, Malicious] with appropriate metadata.
- Depending on the result and confidence score one of the following actions:
 - ✓ Subsequent multi-vendor AV or sandboxing is triggered within ATP.
 - ✓ The result is returned instantly, and rest of the analysis is skipped.

Traditional Malware Detection

- Reactive Detection

Traditional methods run regex/pcr on known signatures, yara rules etc. to identify malware which are error prone.

- Static Analysis

Examine and evaluate the code of a software program without executing

Signature based, Heuristic analysis, File hashing, Resource analysis, Static code analysis tools

- “Point in Time” Remediation

Detection and remediation based on known attacks at a specific point of time (e.g. signatures) which may become outdated

Traditional Malware Detection: Unable to detect Zero-Day Exploits, Polymorphic and Metamorphic Malware and Advanced Persistent Threats (APT) Identification

VERSA AI/ML BASED MALWARE DETECTION

- Proactive Detection

- ✓ *AI can identify threats based on behavior, catching zero-day and polymorphic malware.*
- ✓ *Eliminates zero-day attacks covering 90% of file used to transmit malware while reducing sandbox load by 75% (e.g PE, PDF, docx, pptx, xlsx, JS etc.)*

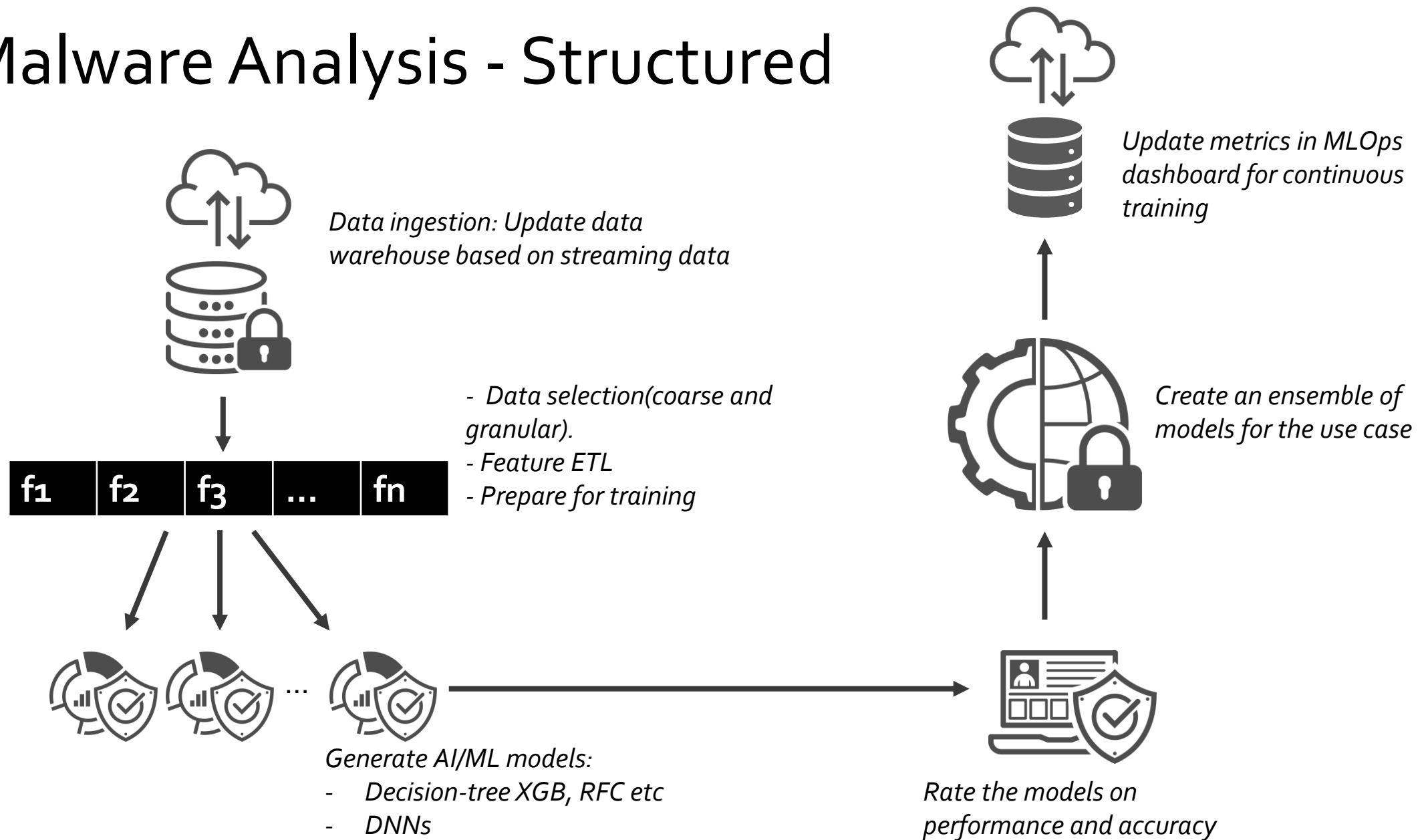
- Continuous Learning & Real Time Analysis

- ✓ *Adapts over time to new threats from updated data and models, improving its detection capabilities for zero-day.*
- ✓ *Ensemble of Models: Trained gradient-boosted trees, Deep Neural Networks as well as fine-tuned transformer models for the different file-types.*

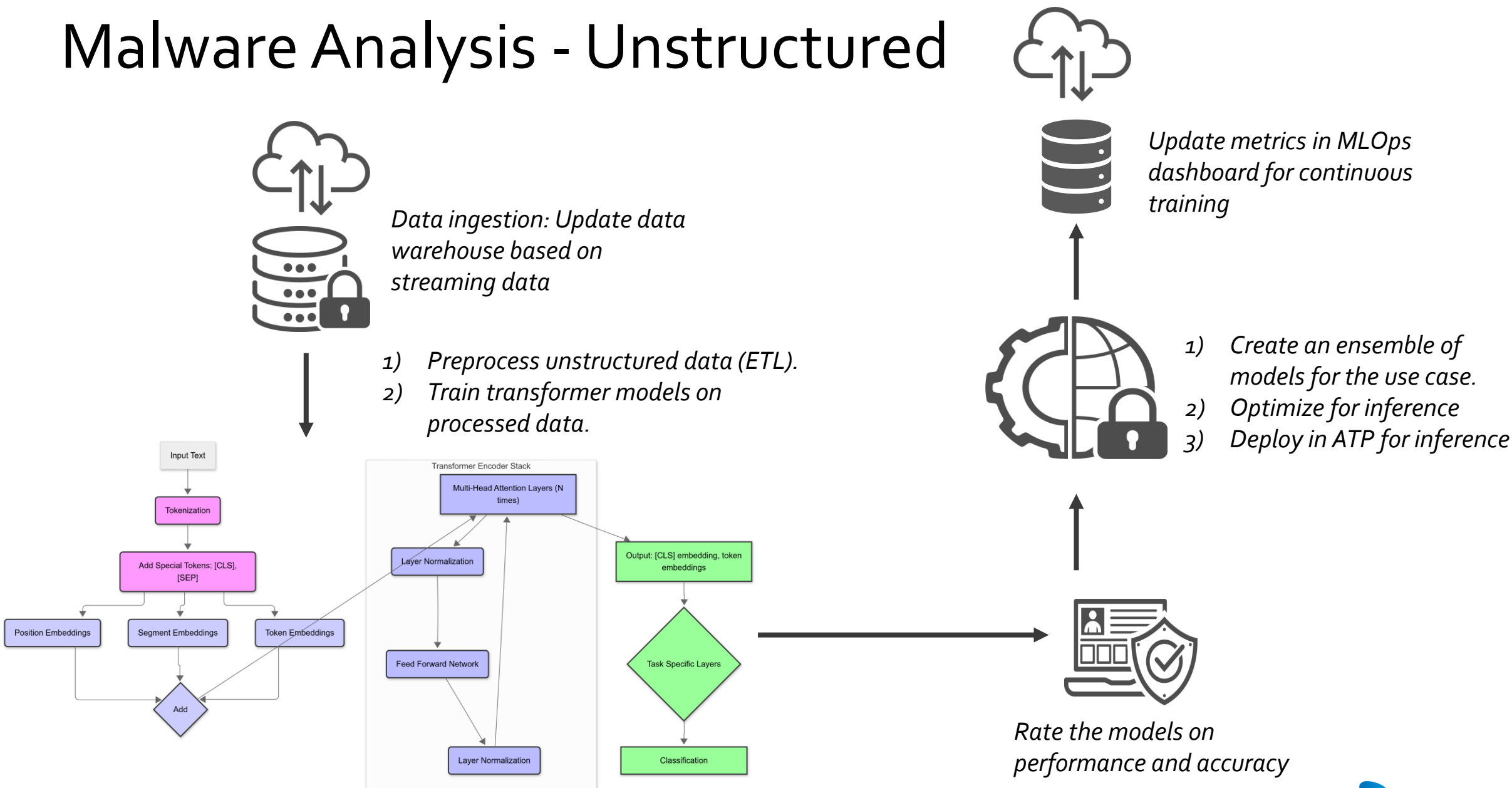
- Sophisticated Threat Identification & Remediation

- ✓ *Ingest file from any source (branch, users or SASE GWs, cloud services), with analysis & remediation using ATP cloud.*
- ✓ *Detect complex attack patterns and threats by training on diverse data.*

Malware Analysis - Structured



























Malware Analysis - Unstructured



AI based Malware Detection



- VersaAI™ deploys multi-stage AI/ML for real-time identification of malware
- Eliminates zero-day attacks covering 90 % of file types used to detonate malware while reducing sandbox load by 75%. Analytics dashboard shows detection by AI/ML and consequent policy action
- Consumed as part of ATP cloud (GA) as well as on-premise (2H'25).

Report	Appliance ↑↓	Application ↑↓	User ↑↓	Action ↑↓	Verdict ↑↓	Pr
 	SASE-GW-B2	http		block	SandBoxAIMLAnalysisFilesMalicious	ve
 	SASE-GW-B2	http		block	CloudLookUPFilesMalicious	ve
 	SASE-GW-B2	http		block	DefaultAction	ve
 	SASE-GW-B2	http		block	DefaultAction	ve
 	SASE-GW-B2	http		block	DefaultAction	ve
 	SASE-GW-B2	http		block	DefaultAction	ve
 	SASE-GW-B2	http		block	DefaultAction	ve
 	SASE-GW-B2	http		block	SandBoxAIMLAnalysisFilesMalicious	ve

ATP Logs (AIML)

☐ Show Domain Names

Set filters here... Apply | Clear | Copy Filter

Receive Time ↓↑	Report	Appliance ↑↓	Application ↑↓	User ↑↓	ATP Action ↑↓	ATP Pipeline ↑↓	Analysis Type ↑↓	Final Verdict ↑↓
Mar 31st 2025, 5:04:22 PM PDT	 	SDWAN-Branch1	http	Unknown	block	AIML	Predictive	Malicious

Showing 1 to 1 of 1 entries



AI/ML – Data Loss Prevention

Versatility 2025

© 2025 Versa and/or its affiliates. All rights reserved.



AI/ML based DLP – high-level components


DLP for multiple document types: - *Text, PDF, DOC(docx, pptx, xlsx), Images etc.*



Image and Text pre-processing for DLP training and inference

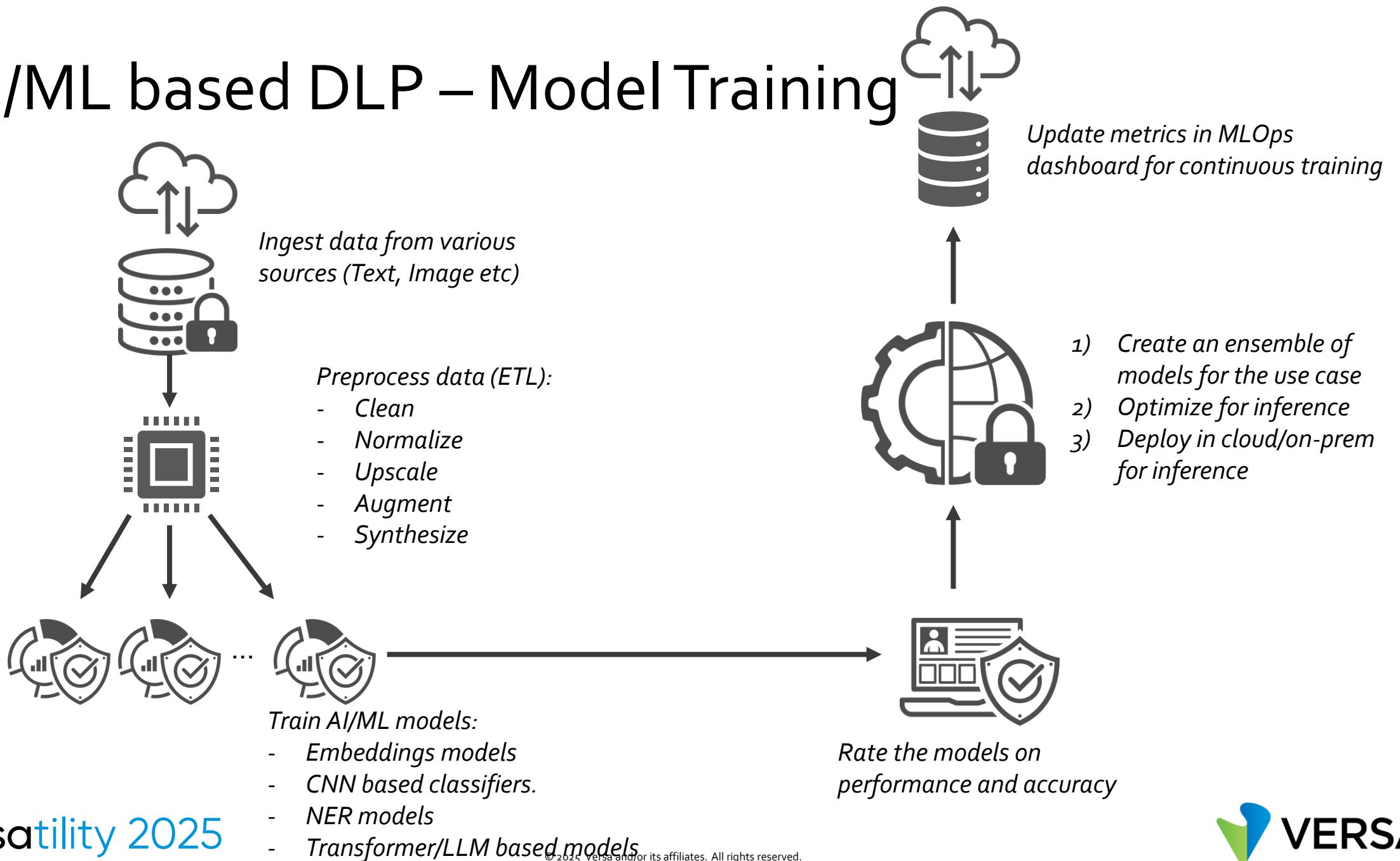


Bleeding edge transformer models used to detect the type of Enterprise document (e.g. Credit cards, Passport, source-code,) and extract multi-modal content.



Ability to fine-tune LLMs and smaller-footprint NER models for classification and detection of sensitive/PII for customer-specific data.

AI/ML based DLP – Model Training



DLP Extraction and Classification – Example 1

```
{
  "detection": {
    "Enterprise": [
      {
        "Document Type": "PERSONAL-IDENTITY",
        "Confidence Score": 99.0
      }
    ],
    "Generic": [
      {
        "Classification": {
          "Document Type": "DRIVER_LICENSE"
        },
        "Extraction": [
          {
            "Identifier type": "NAME",
            "Identifier": "ALEXANDER JOSEPH",
            "Confidence Score": "100%",
            "Sensitivity": "high"
          },
          {
            "Identifier type": "DATE_OF_BIRTH",
            "Identifier": "08311977",
            "Confidence Score": "100%",
            "Sensitivity": "high"
          }
        ],
        ...
      }
    ]
  }
}
```



DLP Extraction and Classification – Example 2

```
{
  "Enterprise": [
    {
      "Document Type": "FINANCE-REGULATORY",
      "Confidence Score": 98.5,
      "Sub-Document": {
        "Classification": {
          "Sub-document type": "Individual Tax Returns"
        },
        "Extraction": [
          {
            "Identifier type": "Taxpayer Name",
            "Identifier": "JOHN TAXPAYFR",
            "Confidence Score": 80,
            "Sensitivity": "Low"
          },
          {
            "Identifier type": "Taxpayer Social Security Number",
            "Identifier": "002-21-1252",
            "Confidence Score": 90,
            "Sensitivity": "High"
          },
          ...
        ]
      }
    }
  ]
}
```

Form 1040 Department of the Treasury -- Internal Revenue Service 2010 (99) (RIS Use Only -- Do not write or staple in this space)

For the year Jan. 1-Dec. 31, 2010, or other tax year beginning 2010, ending 2010 OMB No. 1545-0074

Name, Address, and SSN JOHN TAXPAYER
10 EAST 10 STREET APT 5
NEW YORK NY 10003

Your social security number 002-21-1252
Spouse's social security no. 010-25-5545

Make sure the SSN(s) above and on line 5c are correct. Checking a box below will not change your tax or refund.

Presidential Election Campaign Check here if you, or your spouse if filing jointly, want \$3 to go to this fund (see instructions) ☐ You ☐ Spouse

Filing Status 1 ☐ Single 2 ☐ Married filing jointly (even if only one had income) 3 ☒ Married filing separately. Enter spouse's SSN above and full name here. MARY MAYER 5 ☐ Qualifying widow(er) with dependent child (see instructions)

Exemptions 6a ☒ Yourself. If someone can claim you as a dependent, do not check box 6a. b ☐ Spouse c ☐ Dependents: (1) First name Last name (2) Dependent's social security number (3) Dependent's relationship to you (4) ☒ If child under age 17, enter first last (see instructions) No. of children on 6a and 6b 1 No. of children on 6c who lived with you and did not live with you due to divorce or separation (see instructions) 0 Dependents on 6c not entered above Add numbers on lines above 1

d Total number of exemptions claimed 1

7 Wages, salaries, tips, etc. Attach Form(s) W-2 7 0

Income 8a Taxable interest. Attach Schedule B if required 8a 358
b Tax-exempt interest. Do not include on line 8a 8b 6,885
9a Ordinary dividends. Attach Schedule B if required 9a 6,491
b Qualified dividends 9b 5,907
10 Taxable refunds, credits, or offsets of state and local income taxes 10 1,359
11 Alimony received 11
12 Business income or (loss). Attach Schedule C or C-EZ 12 208,621
13 Capital gain or (loss). Attach Schedule D if required. If not required, check here ☐ 13 -1,500
14 Other gains or (losses). Attach Form 4797 14 -27
15a IRA distributions 15a b Taxable amount 15b
16a Pensions and annuities 16a b Taxable amount 16b
17 Rental real estate, royalties, partnerships, S corporations, trusts, etc. Attach Schedule E 17 71
18 Farm income or (loss). Attach Schedule F 18
19 Unemployment compensation 19
20a Social security benefits 20a b Taxable amount 20b
21 Other income. NYC UBT REFUND 4971 21 4,971
22 Combine amounts in the far right column for lines 7 through 21. This is your total income 22 220,344

Adjusted Gross Income 23 Educator expenses 23
24 Certain business expenses of reservists, performing artists, and fee-basis government officials. Attach Form 2106/2106-EZ 24
25 Health savings account deduction. Attach Form 8889 25
26 Moving expenses. Attach Form 3903 26
27 One-half of self-employment tax. Attach Schedule SE 27 9,163
28 Self-employed SEP, SIMPLE, and qualified plans 28
29 Self-employed health insurance deduction 29 18,811
30 Penalty on early withdrawal of savings 30
31a Alimony paid b Recipient's SSN 31a
32 IRA deduction 32 5,000
33 Student loan interest deduction 33
34 Tuition and fees. Attach Form 8917 34
35 Domestic production activities ded. Attach Form 8903 35
36 Add lines 23 through 31a and 32 through 35 36 32,974
37 Subtract line 36 from line 22. This is your adjusted gross income 37 187,370

For Disclosure, Privacy Act, and Paperwork Reduction Act Notice, see separate instructions. Form 1040 (2010)

Traditional DLP

- No “context” in analysis

Relies on pre-defined pattern matches which may lead to false positives or negatives in certain attack scenarios

- Static Detection Techniques

- a) *Keyword Matching*
- b) *RegEx for Pattern Recognition (Social Security #s)*
- c) *Document Fingerprinting (unique hash or "fingerprint")*
- d) *File Type and Metadata Analysis*
- e) *Data classification by Tagging*

Leads to unnecessary False Positives, noisy alerting and can be easily circumvented.

- Limited Adaptation

Non-trivial real-time updates to DLP signatures (user or pre-defined)

VERSA AI/ML BASED DLP

- Enhanced Detection with Contextual Analysis

- ✓ *Understands the context (spatial or temporal) of data usage, allowing for more nuanced protection strategies that adapt to different scenarios.*

- Dynamic Adaptation with Real Time Protection

- ✓ *Ability to fine-tune and learn from new data, improving its understanding of what constitutes sensitive information and potential threats over time*
- ✓ *Analyze data in-motion in real-time, providing immediate response to potential data leaks or unauthorized access.*

- Advantage AI/ML

- ✓ *Detection of Sensitive Information in Unstructured Data*
- ✓ *Adaptive Protection Against Evolving Data Types and Policies*
- ✓ *Anomaly Detection in Data exfiltration using UEBA triggered user risk analysis.*



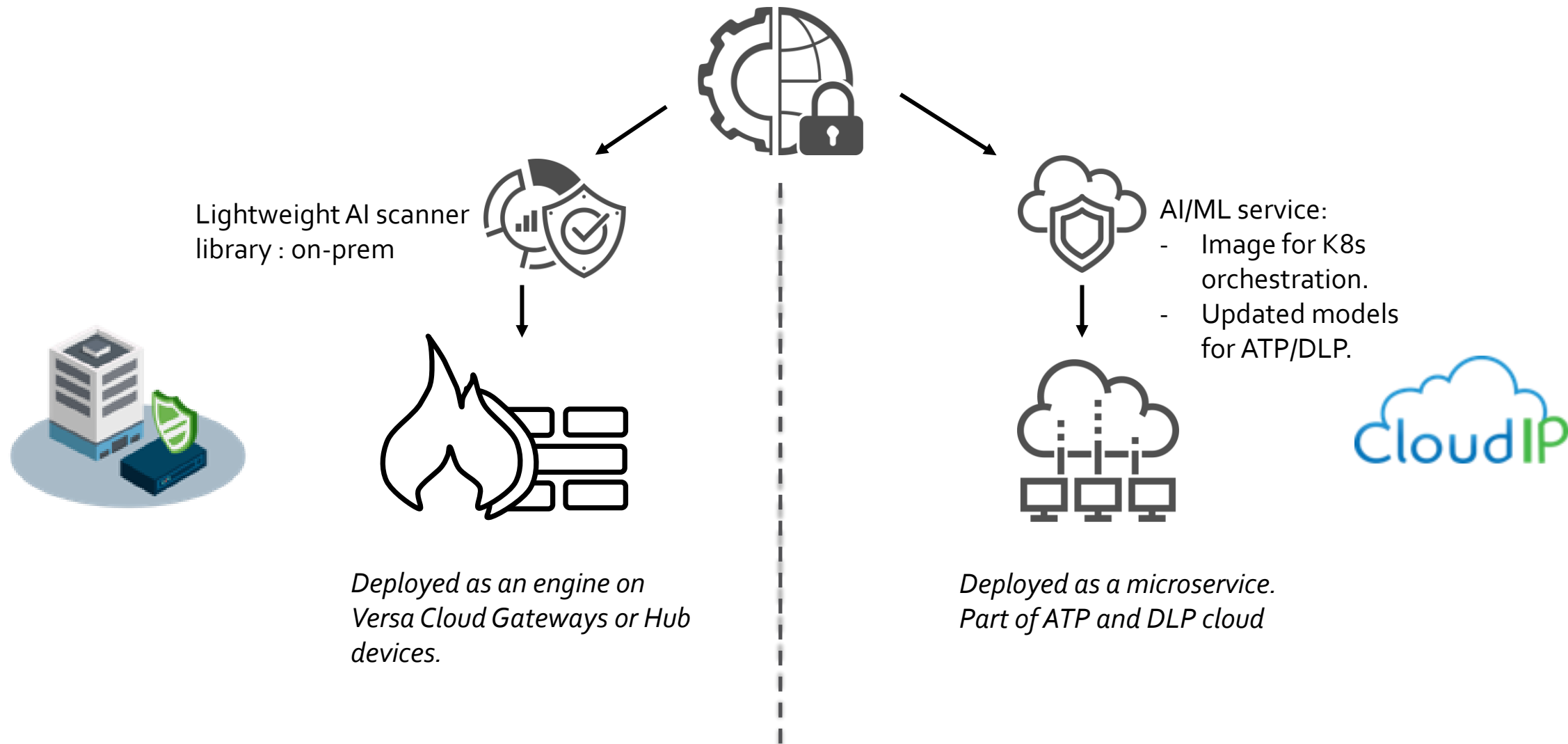
AIOps for ATP/DLP

Versatility 2025

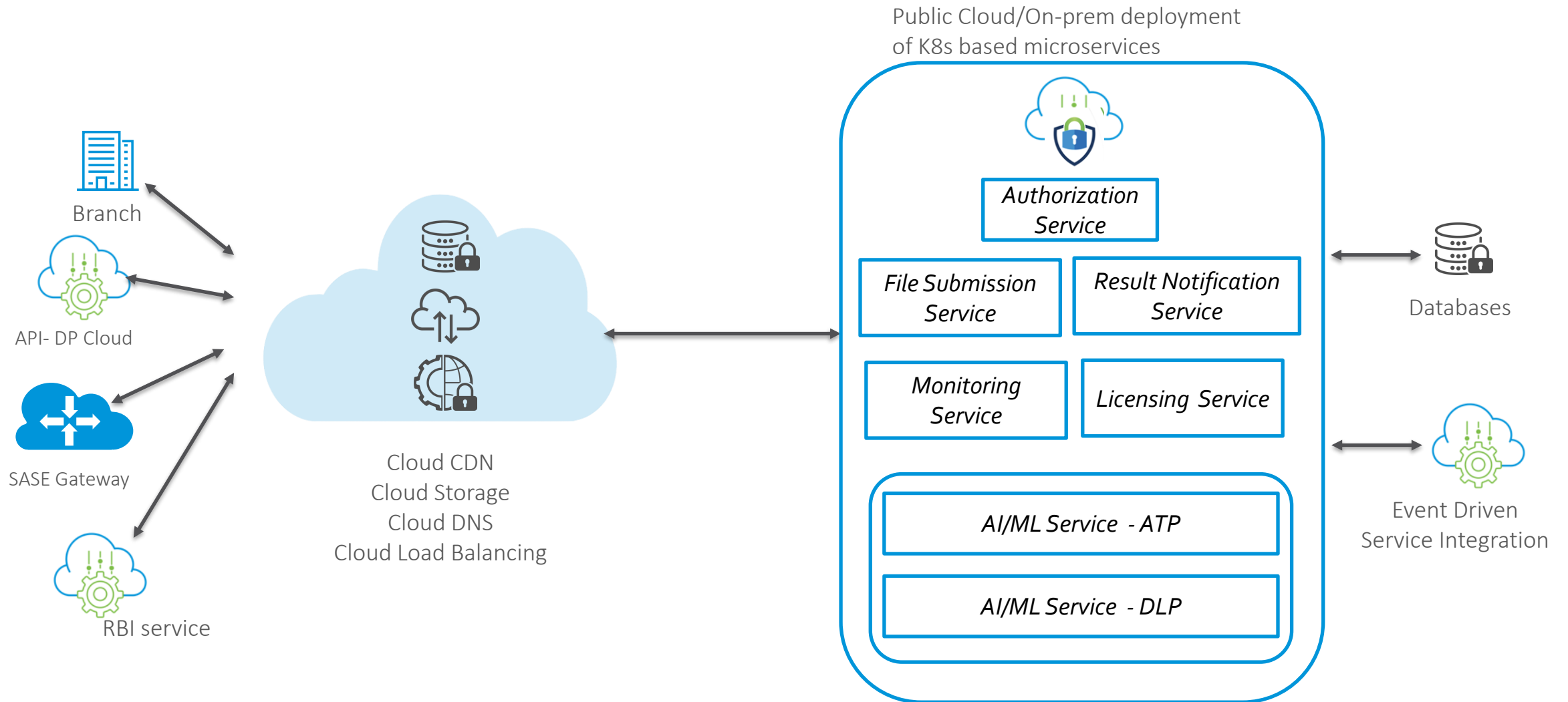
© 2025 Versa and/or its affiliates. All rights reserved.



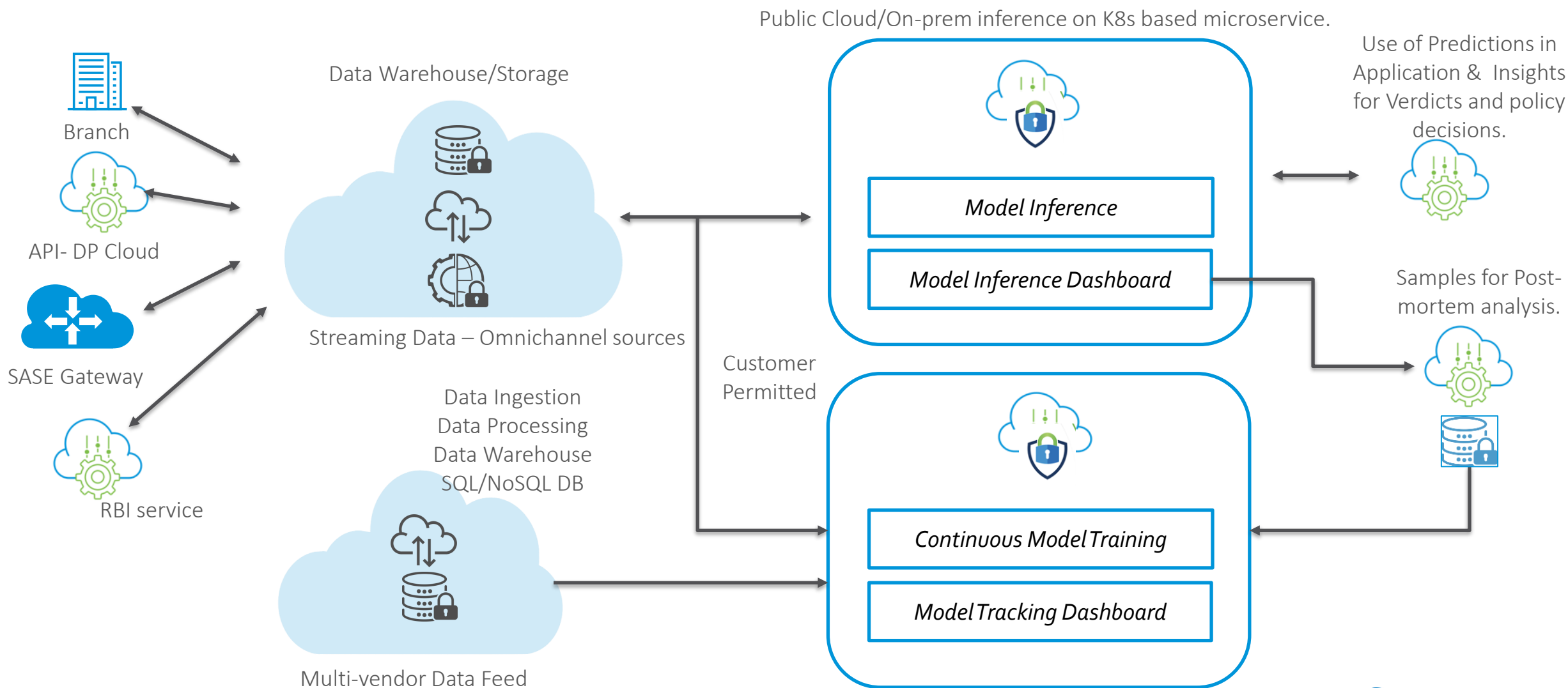
Model Consumption Strategies



Public Cloud Based AI/ML Services Flow Diagram



Public Cloud Based AI/ML ATP/DLP Data Pipeline



Thank you

Versatility 2025

