Versatility 2024

The Future of Infrastructure is AI/ML Driven

Kumar Mehta
Co-Founder & Chief Development Officer

VERSA

Versatility 2024

VERSA

What are Today's Pain Points - Networking?

Reactive Network Management
Too much time spent today addressing issues as they arise rather than proactively managing and anticipating network needs

Lack of Standardization
Device monitoring is not standardized. A mix of Rest APIs, SNMP, http'ping to monitor all the devices

We Are "Under Automated"
No automatic troubleshoot mechanism available, no easy and natural language interaction for managing networks, Lack of Prediction to aid planning and prevent failures

Complex Network Infrastructure
Complex multivendor networks can create challenges in integration, configuration, deployment, performance management, and troubleshooting.

Massive Data, but Little Insight
Our carefully crafted set of rules and alerts generates a massive amount of data, but are we getting insight?

No Anomaly Detection/Prioritization
There is no anomaly detection capabilities (Is the application performance worse that usual?) .
There is no automatic prioritization of things to look at.

VERSA

What are Today's Pain Points - Security?

Expanding Attack Surface
Digital transformation, shadow IT, and remote work are extending the network perimeter and introducing new vulnerabilities

Massive Data, but Little Insight
Massive volumes of threat data and alerts can overwhelm security teams and make it difficult to respond effectively. And integrating and analyzing data from diverse sources can lead to gaps.

Talent Shortages
Its hard for a small team to keep up with rapidly evolving threats, adding stress and burnout. A lack of skilled professionals can hinder the deployment of advanced security.

The Emergence of AI Powered Attacks
AI-powered attacks (like FraudGPT or WormGPT) can rapidly evolve and adapt to countermeasures, accelerating attacks and making detection and response more challenging

Complexity of Multi-Product Defense
Integrating and orchestrating multiple security solutions (On average there are 76 different security solutions), maintaining expertise across multiple products, and analyzing and responding to security incidents can be challenging and expensive.

Detection and Triage Still Very Manual
Attacks are faster than ever, but manual defenses mean slow response times (6 days to respond and remediate attacks) and human error that can amplify the impact of breaches. 83% of Data breaches are because of human error and 43% are due to misconfigurations

Security Events are Expensive
The cost per breach is over $4M; there are regulatory fines if compliance is breached; reputation damage that can be long-lasting

Versatility 2024

VERSA

What is AI good at?

- Analyzing vast amounts of data
- Quickly identifying trends and anomalies
- Forward looking prediction
- Automation of routine tasks
- Real-time response to changing conditions
- Ability to learn and adapt to changing conditions

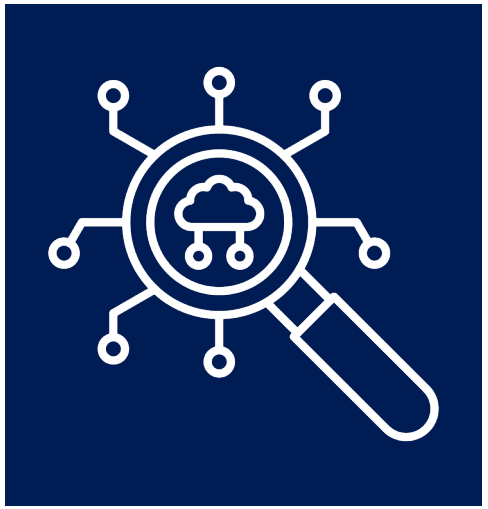
AI/ML to the rescue - Networking

AI/ML-powered self-protecting networks can redefine network operations, making them more proactive, predictive, and resilient.

Optimizing Network Performance

- By analyzing traffic patterns and usage data, AI/ML-powered systems can predict peak periods and potential bottlenecks, dynamically adjusting bandwidth and route traffic efficiently, and optimize network paths for performance and security.
- Ensures that critical applications have the resources they need, while less critical traffic is deprioritized, improving overall network efficiency and user satisfaction.
- Ensures that network operations are not only more efficient but also more agile, capable of responding to the needs of the business in real-time

AI/ML to the rescue – Networking (Continued)



Anomaly Detection

- AI/ML-powered self-protecting networks enhance network efficiency by leveraging sophisticated algorithms to detect anomalies swiftly and accurately, reducing downtime and maintaining operational continuity.
- By learning from data patterns, the AI systems identify deviations before they escalate into significant problems, optimizing resource allocation and ensuring smooth operation.

Predictive Maintenance and Network Health

- AI/ML-powered networks offer predictive insights into the health and performance of network infrastructure.
- Can analyze historical and real-time data to predict potential points of failure before they occur by identifying and addressing these proactively thus preventing downtime, ensuring optimal network performance.
- Additionally, AI/ML can help in capacity planning, identifying when additional resources are needed to meet demand, thereby supporting efficient network expansion and upgrades

AI/ML to the rescue – Networking (Continued)

Troubleshooting

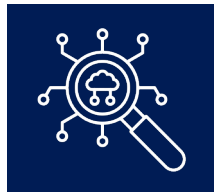
- With a context-aware, natural language chat window. AI/ML facilitates troubleshooting problems and can redirect users to the appropriate setting in the management console.
- AI System can be integrated with a comprehensive knowledgebase that assists IT personnel with suggested solutions, relevant documentation, and step-by-step troubleshooting guidance.

Data-Driven Insights for Strategic Decision-Making

- The vast amounts of data generated and analyzed by AI/ML-powered networks offer valuable insights for strategic decision-making.
- Network administrators can leverage these insights to make informed decisions about network design and investments in new technologies.
- This data-driven approach ensures that network enhancements are aligned with business objectives, user needs, and emerging threats, further optimizing network efficiency and performance.

AI/ML to the rescue - Security

Pivotal benefits of integrating AI/ML is the substantial improvement in threat detection and response times



- **Anomaly Detection**
  - AI-powered systems can sift through vast amounts of network traffic data to identify unusual patterns that may signify an attack.

- **Automated Response**
  - Once a threat is detected, AI-driven networks can automatically implement countermeasures, such as isolating affected systems or blocking malicious traffic.

- **Automated Incident Management and Resolution**
  - Upon detecting a security incident, these platforms can autonomously execute predefined workflows to contain the threat, such as isolating affected systems, applying security patches, or rerouting traffic.

- **Predictive Analytics for Proactive Security**
  - AI/ML algorithms excel in identifying patterns and predicting future occurrences based on historical data.
  - Within an AIOps framework, self-protecting networks can utilize these capabilities to forecast potential security vulnerabilities and threats before they materialize.

- **Continuous Learning and Adaptation**
  - AI/ML models can evolve based on new data, threats, and operational contexts, enhancing their accuracy and effectiveness over time.
  - This continuous improvement loop ensures that both security defences and operational processes remain aligned with the latest threat landscape and technological advancements.

Versa's Vision

Embed AI into the Versa Unified SASE platform

so that our customers can

create their own "self protecting" networks

VERSA

The Future of Infrastructure – AI/ML Driven

Models are many. Model selection is non-trivial and varies by use case. However, Data is the key.

The Versa Platform integrates a panoramic data set from across the entire SASE infrastructure and from the WAN Edge, Cloud, Campus, remote locations, users and devices – into a unified data lake.

VersaAI™ taps into this data lake to extract AI/ML insights that are seamlessly applied across the Versa platform.

Versa AI – Key Components

Threat Protection | *Data 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%*

GenAI Firewall: Security for GenAI

Controls access to Generative AI apps (e.g. ChatGPT) while protecting against unauthorized data upload.

- ✓ *Access controls for Generative AI*
- ✓ *Use "AI" to protect data dynamically from "other AI"*

Versa UEBA

Continuously monitors user and entity behavior to identify suspicious activities or deviations from typical behavior (internal threats)

- ✓ *Track user and device behavioral patterns to detect potential anomalies (e.g. impossible travel)*

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.*

Versatility 2024

VERSA

Versa AI – Key Components

Prediction and Anomaly Detection

Versa Advanced Network Insights (VANI)

What is it?

Prediction and Anomaly Detection and intelligent alerting across the Versa Unified SASE platform.

Key benefits

- ✓ *Identify patterns that might be indicative of security threats*
- ✓ *Prioritize incidents based on severity*
- ✓ *Raise proactive alarms and recommendations to aid planning and prevent failures*

Co-Pilots

Verbo

Generative AI Co-Pilot facilitates interaction and aids in troubleshooting across the Versa Unified SASE platform.

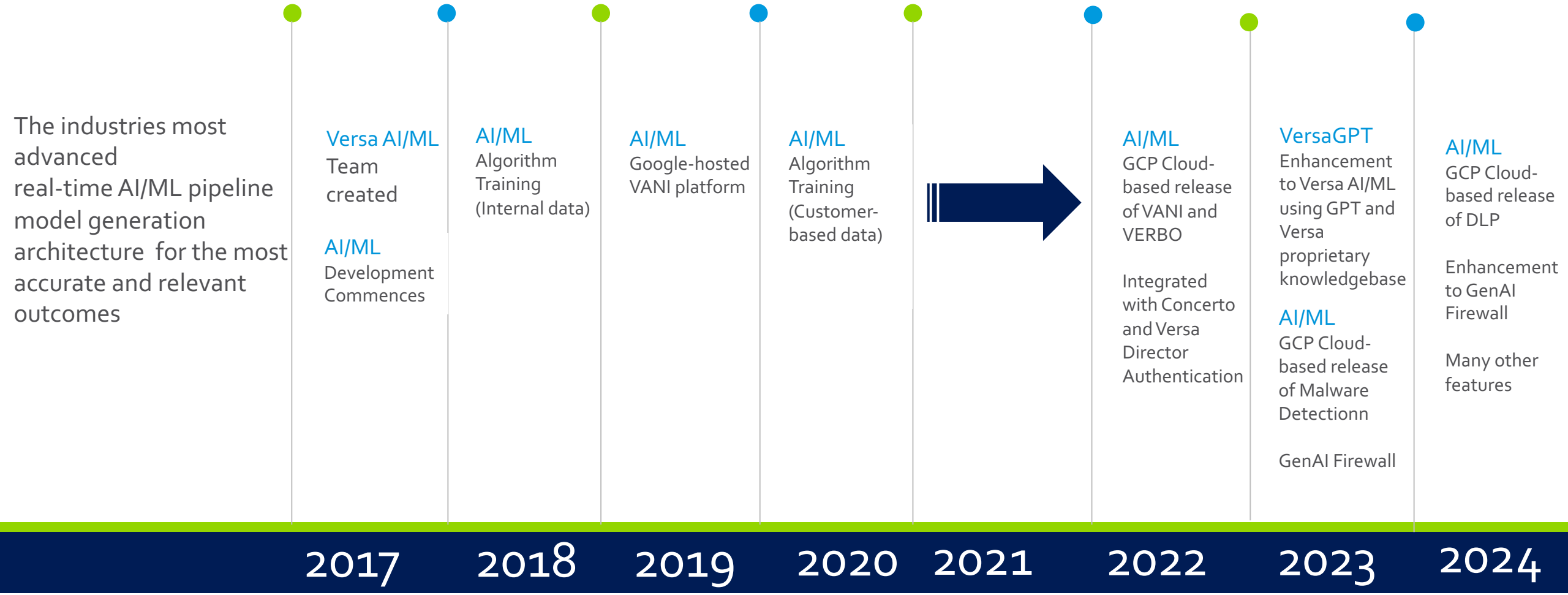
VersaGPT

It supercharges Verbo and enhances day-to-day operations with a guided experience across the Versa Unified SASE platform.

- ✓ *Co-pilot that creates guided experiences across the platform*
- ✓ *Can execute predefined workflows and run books or suggest appropriate actions for IT staff, reducing manual intervention and speeding up incident resolution*
- ✓ *Uses information from our docs and knowledgebases*
- ✓ *e.g. "How do I configure CASB?"*

VERSA

Rapid Pace of AI/ML Innovation…



AI/ML Use Cases

Threat Detection & Prevention

Analysis of vast amounts of data in real-time, enabling it to identify patterns and anomalies that might be indicative of security threats.

VersaAI (GenAI Firewall, AI/ML based Malware Detection and UEBA) *can*

Detect known and unknown threats, such as malware, and insider threats, by recognizing unusual behavior and indicators of compromise.

Anomaly Detection

Malicious pattern detection across various entities (e.g., users, laptops, phones, IoT devices, and more).

VersaAI (UEBA) and VersaAI (VANI) *can Identify common anomalous behaviors (infrequent destinations, impossible travel behavior, bulk deletions and downloads, access from different devices), and custom anomaly policies.*

VersaAI (VANI) can identify deviations from baseline and flag potential networking and security incidents for investigation.

Intelligent Alerting

Elimination of unwanted information in infrastructure data by correlating and prioritizing critical incidents

VersaAI (VANI) *can*

Analyze an unprecedented volume of data, and performance metrics to detect and prioritize critical incidents based on severity around business impact

It presents the most relevant cause of an alarm to provide the focal point to begin your investigation/debugging

Automated Remediation

Via integration with IT service management tools and automation frameworks to automatically trigger remediation actions.

VersaAI (Verbo) *can*

Execute predefined workflows/run books or suggest appropriate remediation actions for IT staff, reducing manual intervention and speeding up incident resolution.

AI/ML Use Cases

Troubleshooting

Context-aware, natural language Co-Pilot.

VersaAI (Verbo) *can*

Troubleshoot problems and can fix, suggest or redirect users to the appropriate setting in the management console to fix the problem.

It is integrated with a comprehensive knowledgebase that assists IT personnel with suggested solutions, relevant documentation, and step-by-step troubleshooting guidance

Data Protection

Protection & prevention of sensitive and confidential data proactively

VersaAI (DLP Engine) *can*

Use precision AI models to extract PII in text and images and

Use another set of models to perform DLP on extracted PII information.

Capacity & Performance

Optimization of network capacity while ensuring rich user experience

VersaAI (VANI) *can*

Execute AI informed analysis for predictive traffic steering for best user experience

Analyse historical data and usage patterns to forecast future resource demands

By predicting capacity requirements, it helps plan infrastructure upgrades, optimize resource allocation, and ensure scalability to meet evolving business needs.

Knowledge Base

Comprehensive knowledge base that has been built over a history of analysed support tickets & documentation

VersaAI (Versa GPT) *can*

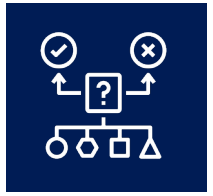
Ease daily operations with generative AI-powered access to Versa documentation and knowledge base

improves enterprise productivity through a guided experience and access to how-to guides, configuration information,

Challenges with AI/ML - Networking

Integrating AI/ML into network operations comes with some challenges

Complexity in implementing and managing AI/ML models.



Addressing potential biases in algorithmic decision-making is necessary. Ensuring the accuracy and fairness of AI/ML algorithms is essential.

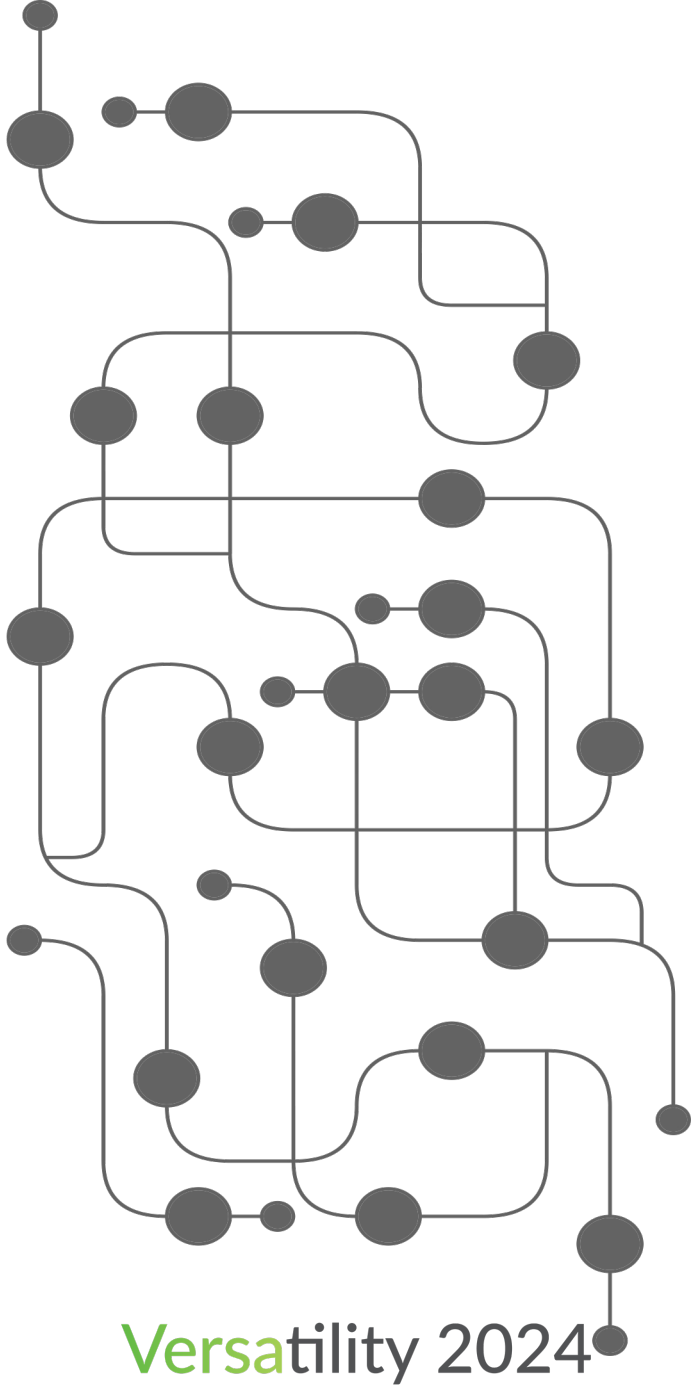
Potential data privacy concerns must be addressed.

Hallucinations

Challenges with AI/ML - Security

AI/ML-powered self-protecting networks offer clear benefits but face several implementation challenges

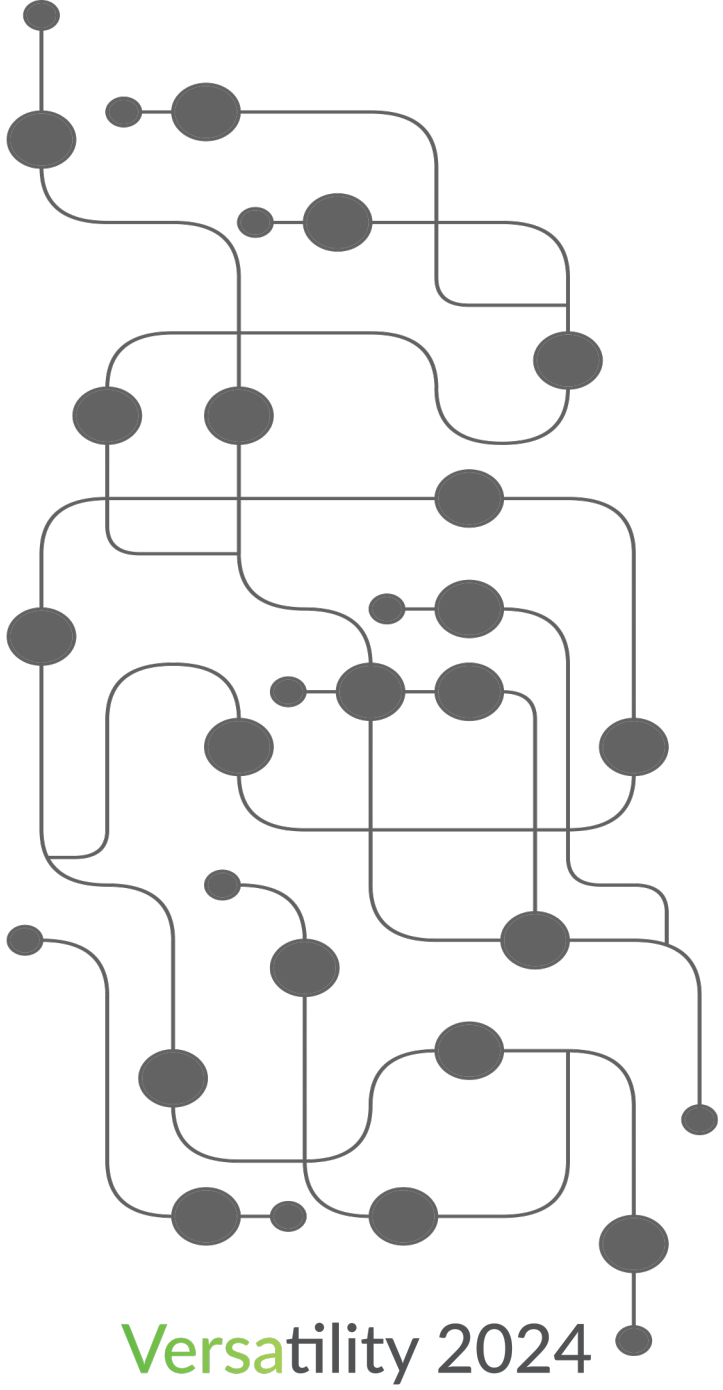
- Requirement for large datasets to effectively train algorithms.
- Risk of false positives (incorrectly identifying benign activity as threats) and false negatives (failing to detect actual threats). Effectiveness heavily depends on the quality and quantity of training data.
- Expertise in both cybersecurity and AI/ML is essential, which may be a barrier for some organizations.
- Data privacy concerns arise due to the sensitive nature of the information being processed.
- Potential for algorithmic biases, which can affect the fairness and efficacy of the protection mechanisms.



Roadmap for VersaAI

- **Enhance GenAI Firewall**
- **Adding Explanation to ML-based anomaly detections using Explainable AI**
  - Better analysis of anomalies using AI Models without using logs
- **Add MITRE attack detection on UEBA**
  - Strengthens an organization's cybersecurity posture by enabling more accurate threat detection, rapid incident response
- **Adding GraphML on/for UEBA's GraphDB for various use cases**
  - Better Security Posture
  - Allows for the representation of complex network structures and relationships within the GraphDB. Enables to model user behavior, entity interactions, and network connections in a comprehensive and intuitive manner.
  - Better Security Governance: i) Detect Anomaly ii) Detect the Blast radius of malicious activity iii) to find Root Cause Analysis of security lapse

VERSA



Versatility 2024

Roadmap for VersaAI

- **Use of Nvidia DPU in Versa Cloud Gateway**
  - Versa-Nvidia innovation with this technology is expected to deliver to our customers very high SSE and SSL Proxy performance. Versa is a DOCA eco system partner (https://developer.nvidia.com/networking/doca)

- **Versa-Nvidia partnership to leverage GPUs to improve training & inference throughput for mixed models for development of Precision AI/ML models for ATP**
  - Customers can leverage the benefits of fast AI/ML inference on the Versa SSE Gateways where relevant models are deployed as part of the ATP as well as DLP suites.

- **Versa-Intel partnership to improve inference throughput using dedicated tensor cores and AMX instruction on Intel CPUs, for low-latency in**
  - Customers can leverage the benefits of fast AI/ML inference on the Versa SSE Gateways where relevant models are deployed as part of the ATP as well as DLP suites.

VERSA

The AI doctor will see you …eventually

Network & Security

The AI doctor will see you ^ ...~~eventually~~ now...

VERSA

Questions

VERSA

Thank you

VERSA