Transforming Cyber Defense with HPE Juniper SRX & AI Ops

Exploring how artificial intelligence is revolutionizing both cyber threats and digital defense strategies in our interconnected world.

HPE JUNIPER networking

AI: The Double-Edged Sword in Cybersecurity

Attack Acceleration

AI accelerates cyberattacks with deepfake phishing, automated malware generation, and mass-scale hacking capabilities that outpace traditional defenses.

Defense Enhancement

Simultaneously, AI empowers defenders with lightning-fast threat detection, intelligent response systems, and predictive security analytics.

HPE JUNIPER networking

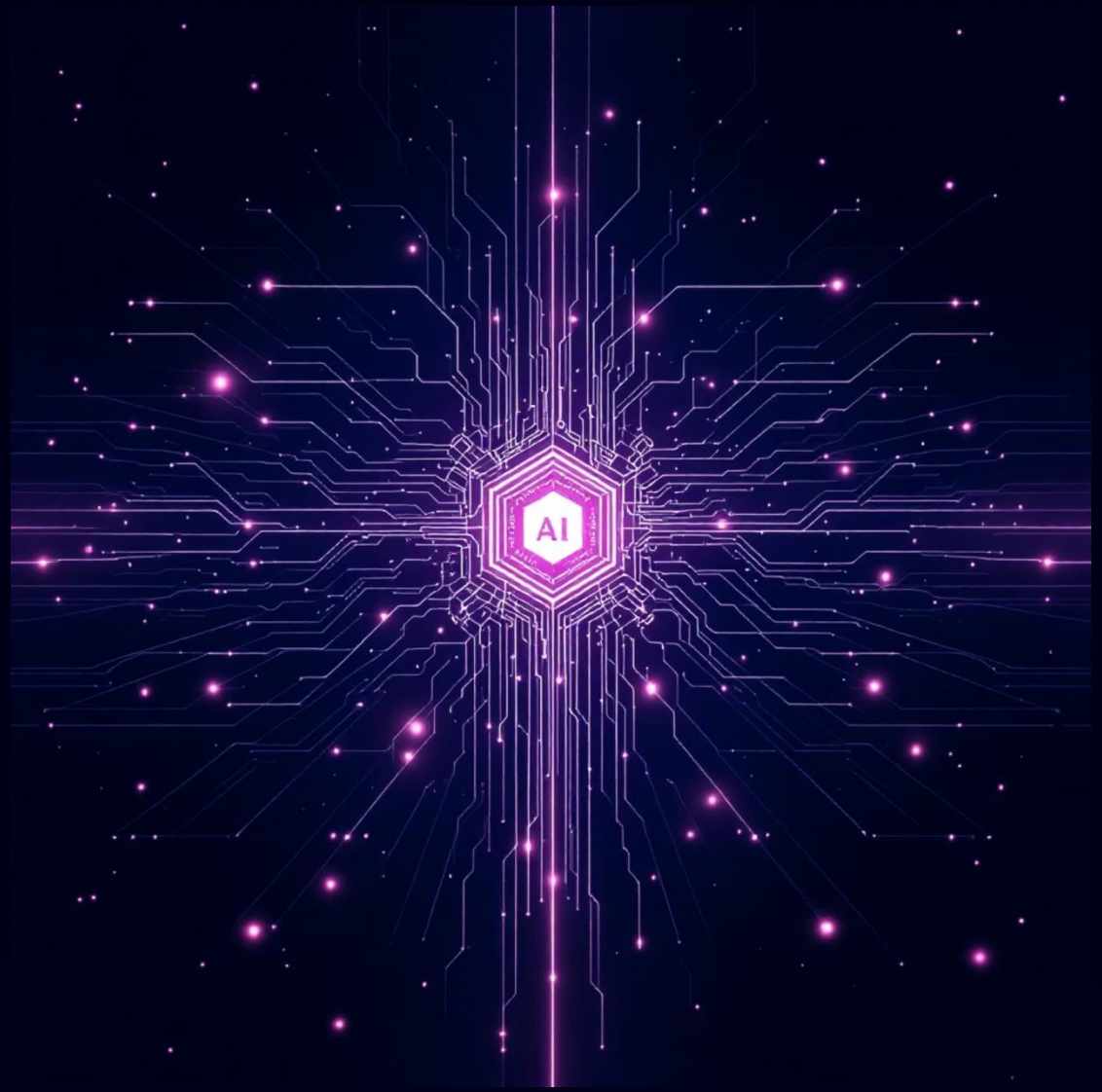
Cybercrime Powered by AI

Faster, Smarter, More Dangerous

The cybercriminal landscape is being transformed by AI technology, creating unprecedented threats that evolve faster than ever before.

HPE JUNIPER networking

The New Face of Cyber Attacks



Democratized Hacking

AI democratizes sophisticated hacking techniques, enabling anyone to launch complex attacks with minimal technical skills required.

Deepfake Phishing

Advanced AI creates hyper-personalized, convincing scams using deepfake technology to impersonate trusted contacts and executives.

Mass Automation

Hackers generate malware code at industrial scale and automate attacks with unprecedented speed and precision.

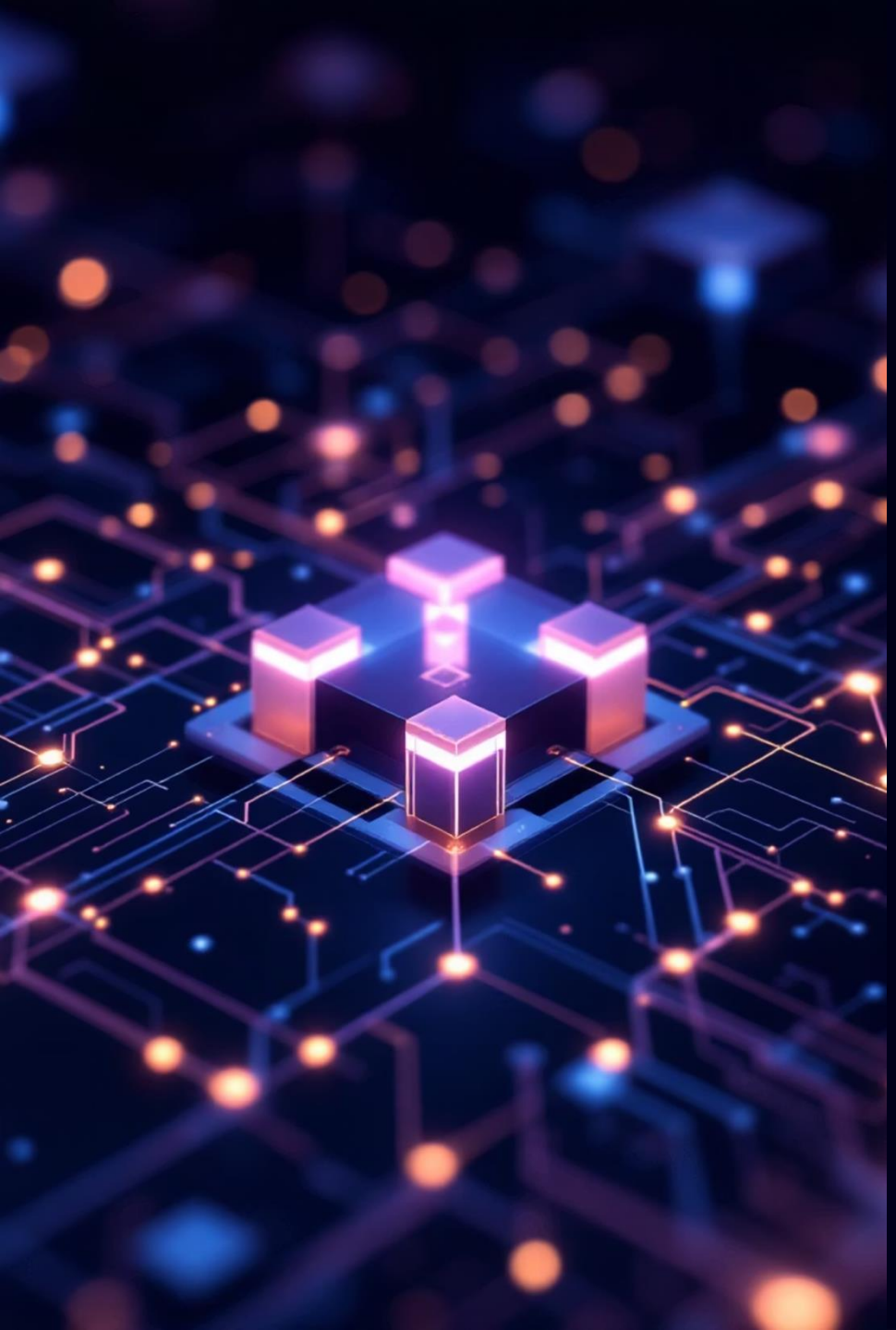
HPE JUNIPER networking

30 Minutes

to $25 Million Lost

The average time from initial breach to significant financial damage continues to shrink as AI-powered attacks move at machine speed.

HPE JUNIPER networking



Challenges Ahead: The Dark Side of AI Defense

Bias & False Signals

AI models can inherit dangerous biases from flawed training data, creating critical blind spots through false positives and negatives in threat detection.

AI Vulnerability

The AI software protecting us is itself vulnerable to sophisticated attacks, manipulation, and adversarial techniques designed to fool machine learning systems.

Trust & Validation

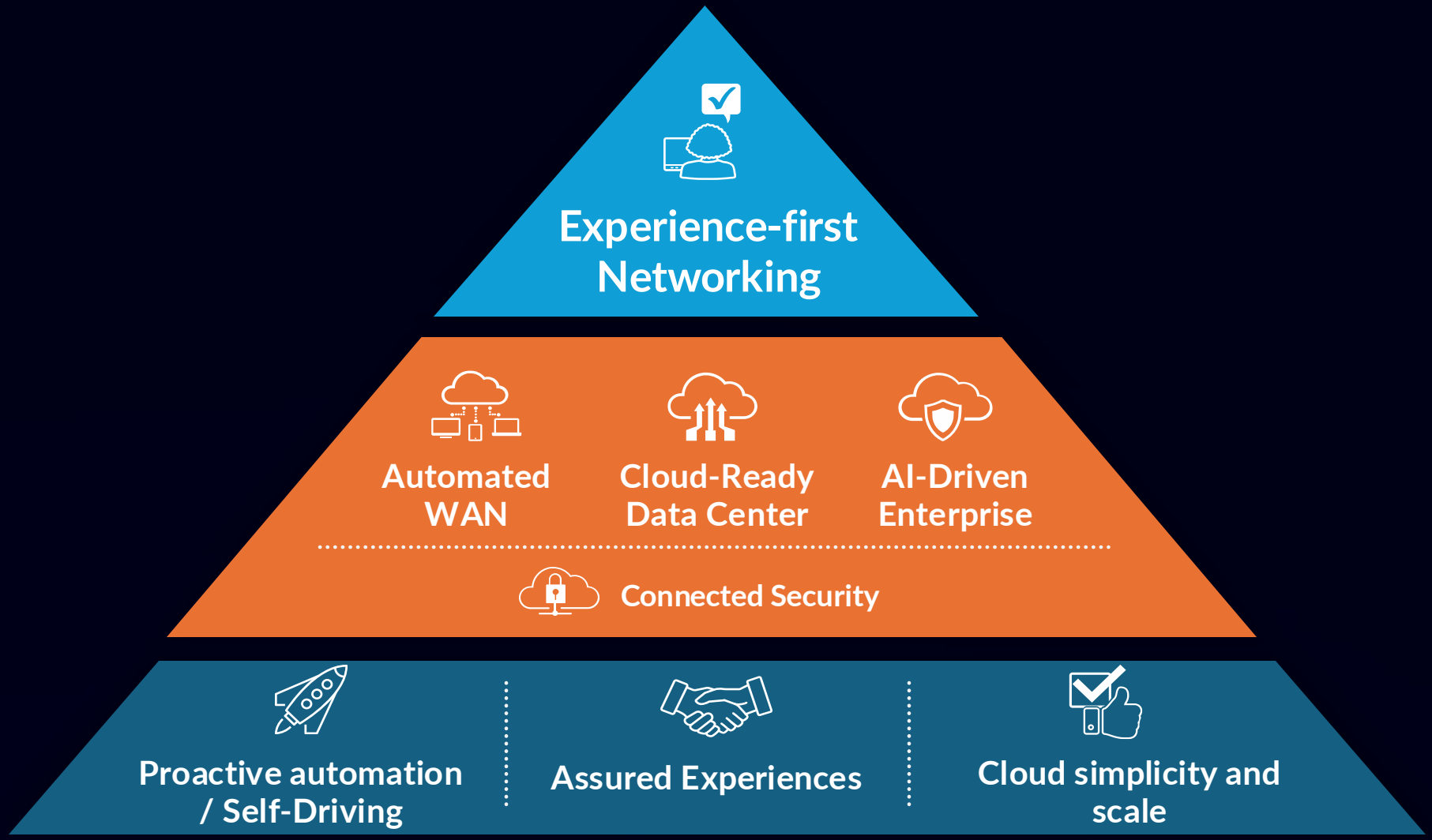
Continuous evaluation of AI models and data integrity becomes essential for maintaining trustworthy, reliable cybersecurity infrastructure.

Need for Strong Foundations

Built on a ‘house of cards’ no AI defense will help. Network and security tools must have the abilities needed (sensing and controls)

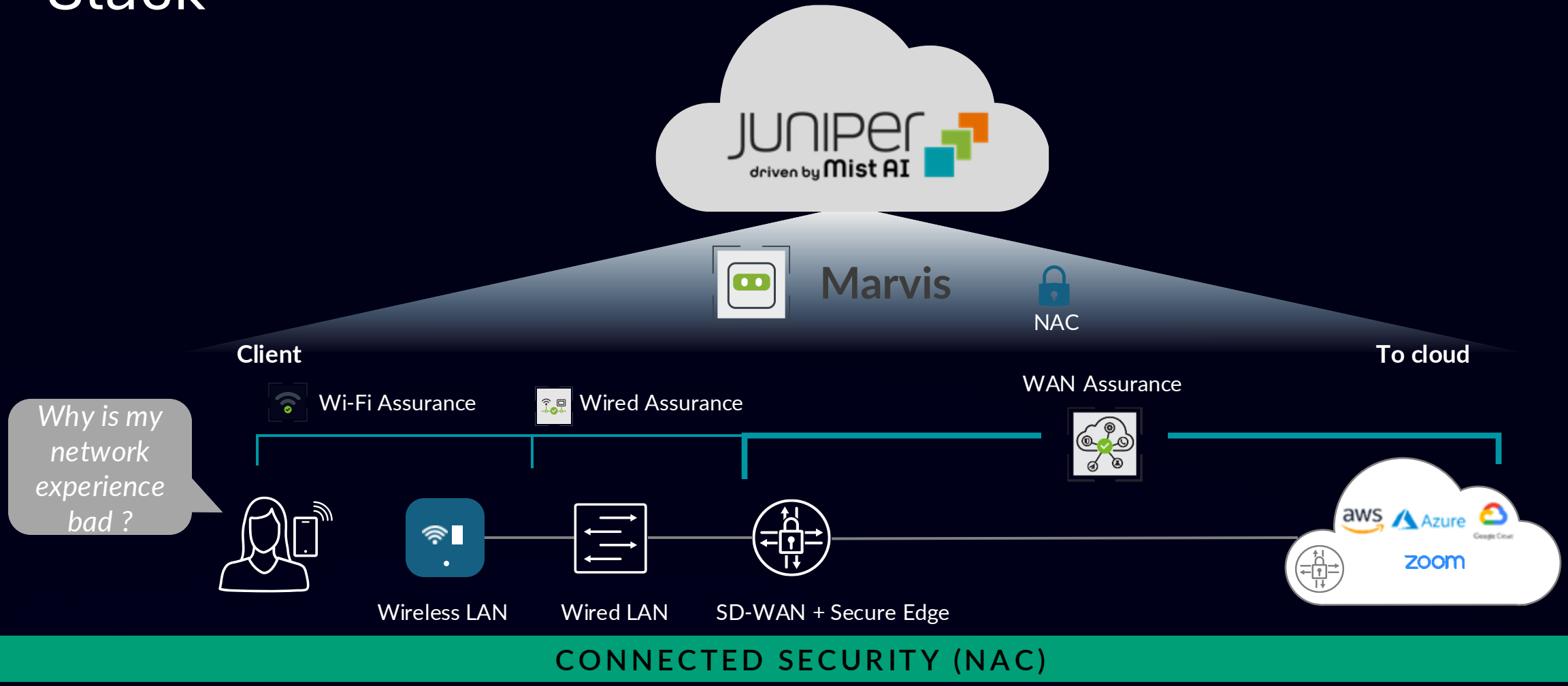
HPE JUNIPER networking

HPE Juniper's True North: Experience-First Networking



HPE JUNIPER networking

HPE Juniper's Client-to-cloud: AI-driven, Secure, Full Stack



Marvis - A Journey to an AI-Driven Enterprise

Marvis Client: Android, Windows

3rd Party

Graph DB

WAN-Marvis

Graph ML

NLP/ NLU *(natural language processing/understanding)*

User Sentiment

WAN Self Healing

WAN Self Optimization

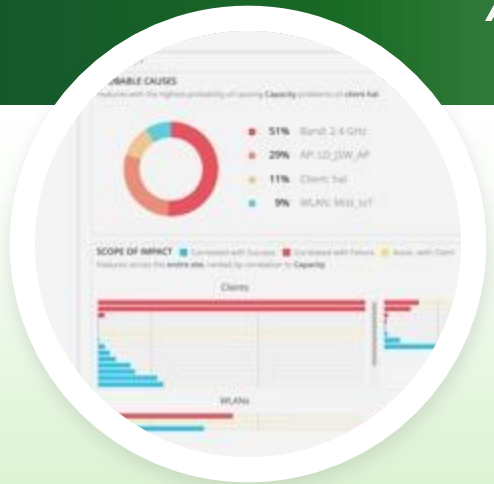
Data

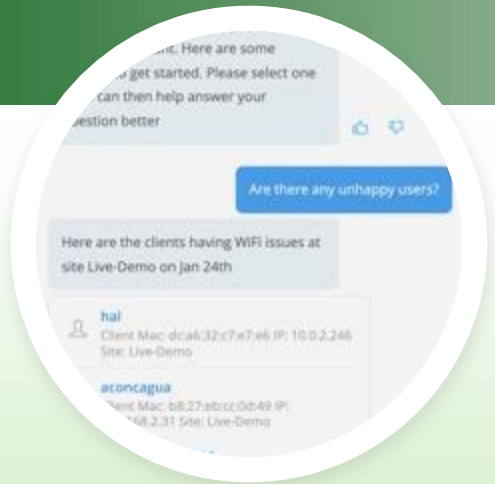
AI Primitives Event Timeline

Data Science Toolbox

Conversational Assistant -LLM

Self Driving Action Framework





CLIENT / WIRED / WIRELESS / WAN / SECURITY / MIST EDGE / 3RD PARTY

DISTRIBUTED SOFTWARE ARCHITECTURE

HPE JUNIPER networking

The key components of an AI based Solutions

AI Events/Insights

Reinforcement Learning
RRM

Unsupervised Learning
Location

Shapley
Feature assessment

LSTM – Neural Network
Time series anomaly detection, NLP, geo-spatial analysis

GAI / LLM / Transformers
Marvis conversational assistant

DEEP LEARNING

ARTIFICIAL INTELLIGENCE

MACHINE LEARNING

K-Means Clustering
Environment Learning

Logistic Regression
AP/Switch Health

Temporal Correlation
Root Cause Analysis

XGBoost/Decision Tree
Throughput Prediction

Probabilistic Graphical Models
Root Cause Analysis

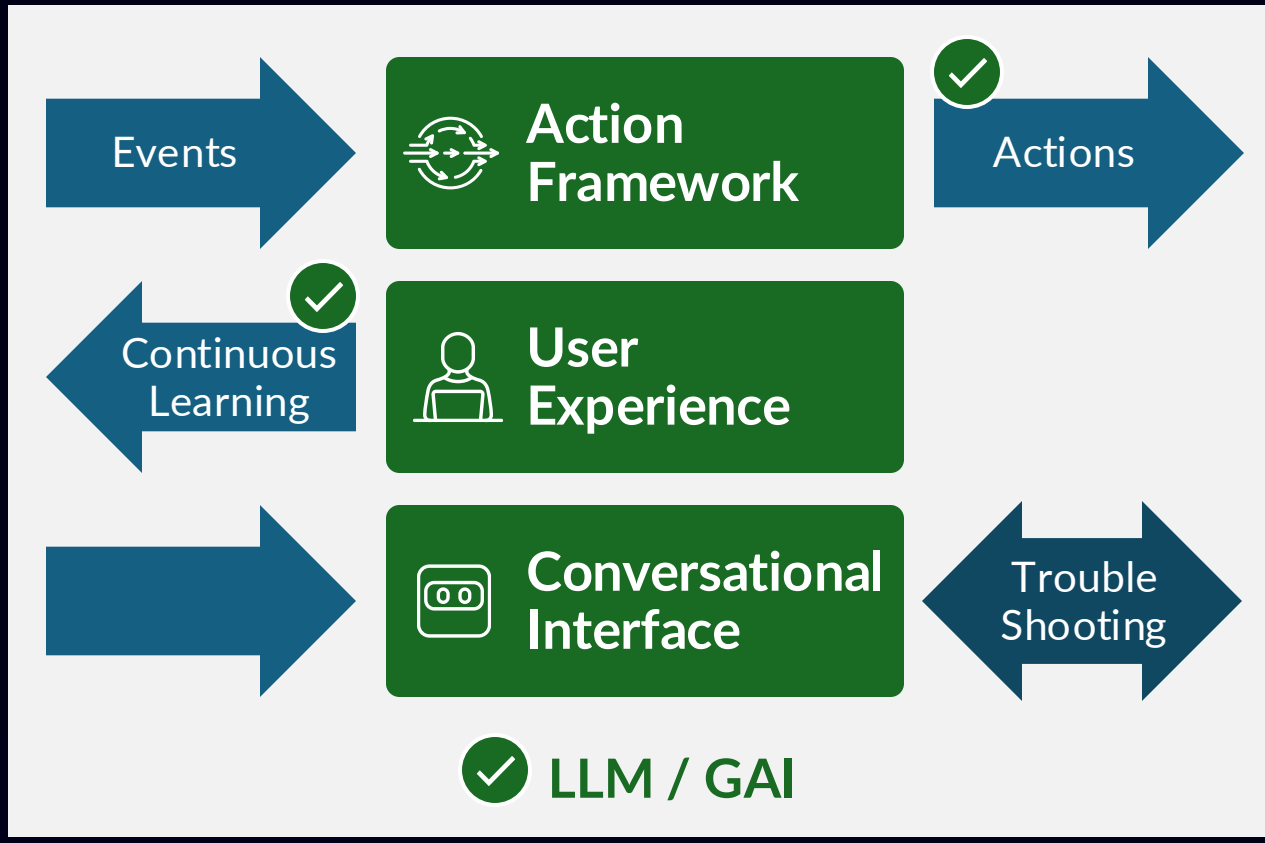
Decision Tree
AP/Switch Health, DHCP Health, Coverage Hole

Domain Expertise Classification
Service Level Metrics, Event Timeline

Bayesian Inference
Persistently Failing Clients, Auto Placement of AP

Online ARIMA
Time Series Anomaly

Mutual Information
Feature Discovery



GAI = Generative Artificial Intelligence

HPE JUNIPER networking

AIOps Requires a Well-stocked Data Science Toolbox

Conversational AI
Marvis Virtual Network Assistant

Reinforcement Learning
RRM

Unsupervised Learning
Location

Neural Network
Time Series Anomaly Detection, NLP, Geo-Spatial Analysis

NEW **Transformer-based Language Models**
Marvis Conversational Assistant

DEEP LEARNING

ARTIFICIAL INTELLIGENCE

MACHINE LEARNING

K-Means Clustering
Environment Learning

Decision Tree
AP / Switch Health, DHCP Health, Coverage Hole

Bayesian Inference
Persistently Failing Clients, Auto Placement of AP

ML threat Preventions
Uses both ML & AI Predictive Analysis

Logistic Regression
AP / Switch Health

Online ARIMA
Time Series Anomaly

Encrypted Traffic Insights
Know it is malware without B&I

Security Intelligence Amplifications
Learns and explore relations and determine Intent

Domain Expertise Classification
Service Level Metrics, Event Timeline

XGBoost / Decision Tree
Throughput Prediction

Probabilistic Graphical Models
Root Cause Analysis

Temporal Correlation
Root Cause Analysis

Mutual Information
Feature Discovery

Reverse Shell Prevention
Block remote SSH/RDP/etc. to bad Actors

HPE JUNIPER networking

SRX NGFW and Advanced Security Services

Comprehensive Security Stack

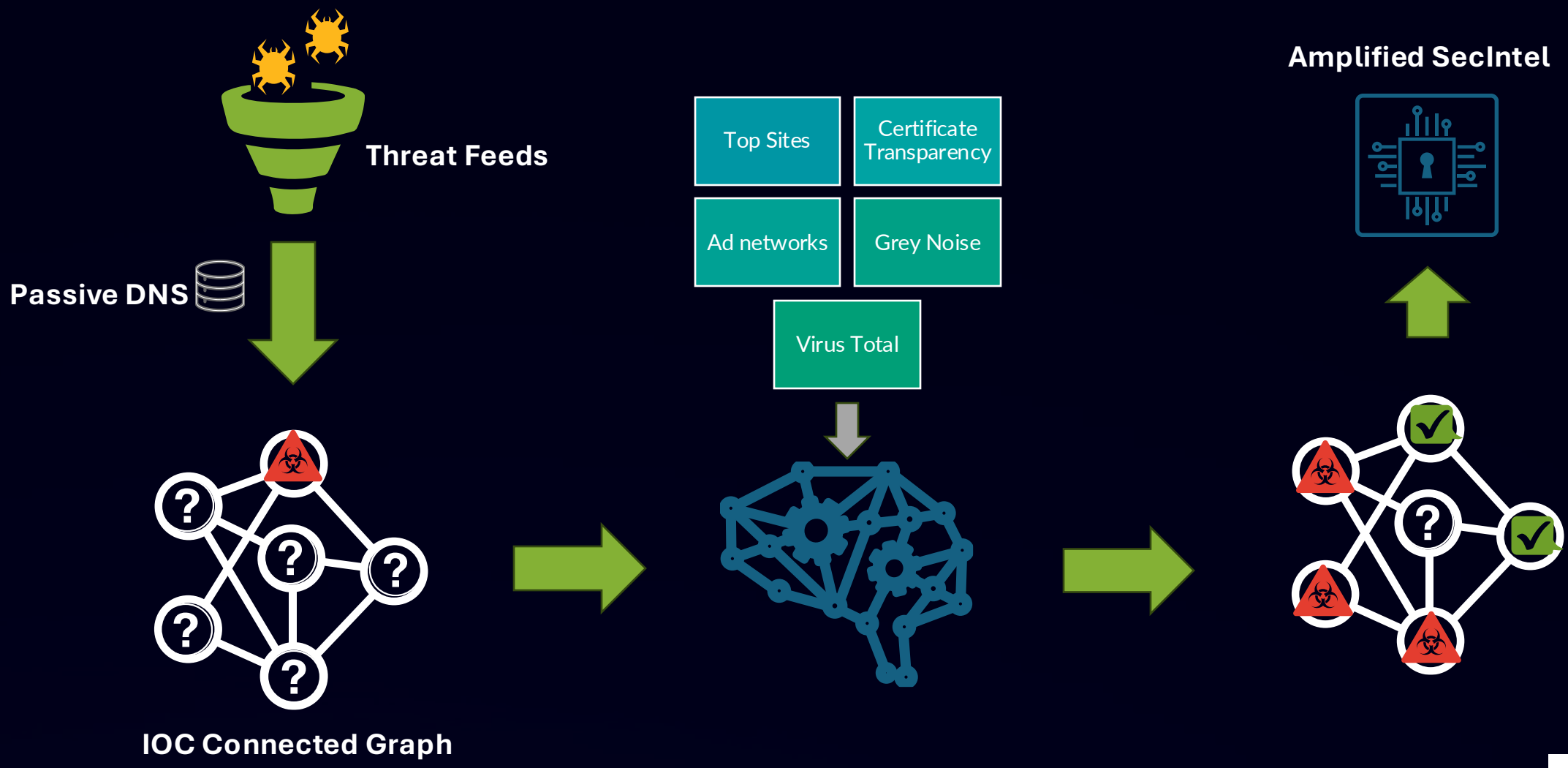
Application Firewall	Block access to risky apps Allow user tailored policies
Intrusion Detection & Prevention	Detect and block threats discovered in network traffic
Security Intelligence	Provide curated threat feeds to block bad IPs, URLs and domains across entire network infrastructure
Content Filtering	Inspect files being sent or received to protect against malware and prevent data loss
App tracking	Tracks Applications Provides reporting of Applications used in the environment.
Anti-Virus Protection	Detect and block known viruses, spyware, trojans etc. using static signatures
DNS Security	Inspect DNS traffic to detect hidden C&C communication, tunneling of malware
Anti-Spam Protection	Examine email messages to identify email spam and blocks, tags or allows based on policy
App QOS & QOE	Prioritize important apps Rate-limit less important apps
URL Filtering	Prevent users from accessing inappropriate websites
Anti-Malware Protection	Discover and mitigate known and zero-day threats malware threats, by scanning various files types
Encrypted Traffic Insights	Analyze HTTPS traffic without decryption to detect and block malicious activity
User Firewall	Identity-based firewalling to secure user access
SSL Proxy	Intercept and decrypt traffic to facilitate inspection
IoT Security	Detect and classify IoT devices, allowing the enforcement of granular security rules
Adaptive Threat Profiling	Use SRX devices as sensors for continuous learning of threat intelligence and data

NGFW feature *ATP feature*

HPE JUNIPER networking

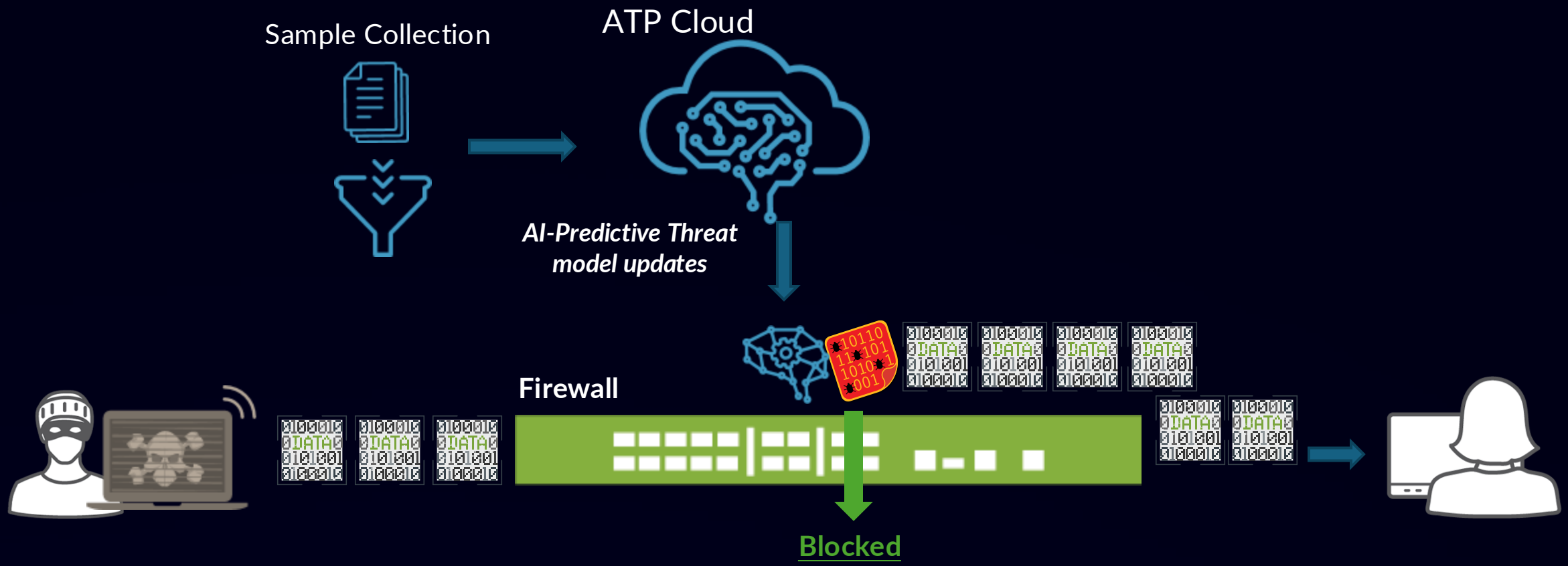
HPE Juniper SecIntel

AI-Enabled Threat Intelligence Amplification



HPE Juniper AI-Predictive Threat Prevention

In-line Protection at Wire Speed



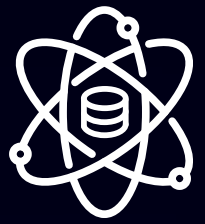
*Identify malicious **intent** prior to complete payload being sent to the client.*

HPE JUNIPER networking

AI – Not New To HPE Juniper Security

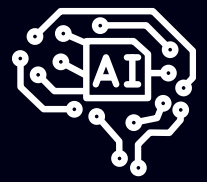
Zero Day / Anti Malware

Encrypted Traffic Insights



AI Predictive Threat Prevention

AI –Native Security Ops



AI –Agents

2016 → 2025

SecIntel

DNS Security

Security Assurance & FlowAV

JUNOS Model Context Protocol

+ MCP

HPE JUNIPER networking

Together, Building a Safer Digital Future

The future of cybersecurity lies not in replacing humans with AI, but in creating powerful partnerships that leverage the best of both worlds to protect our digital civilization.

HPE JUNIPER networking