Cyber Security Trend

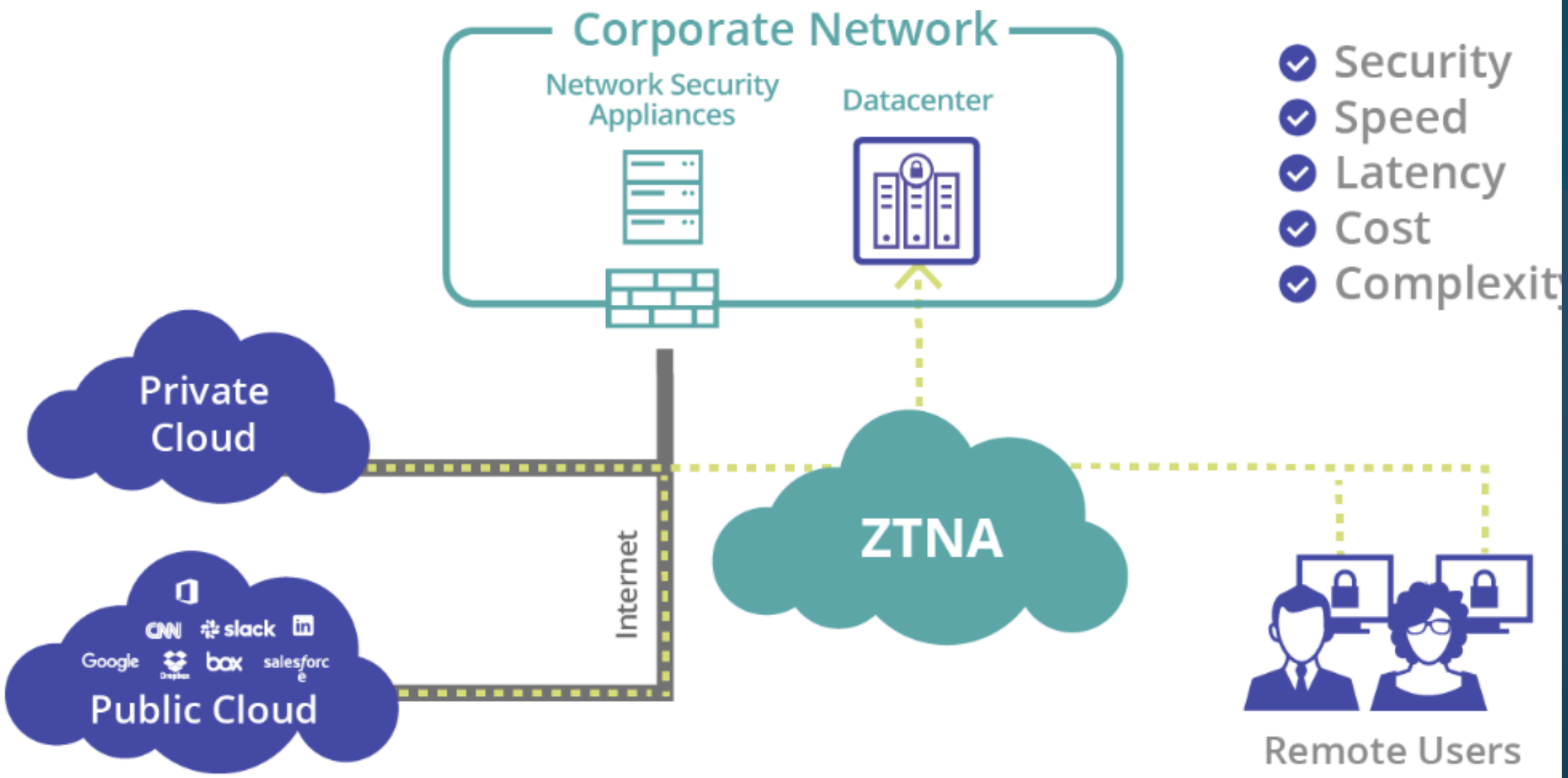
จุติภัตร บุญสูง [CEO, BlueZebra]

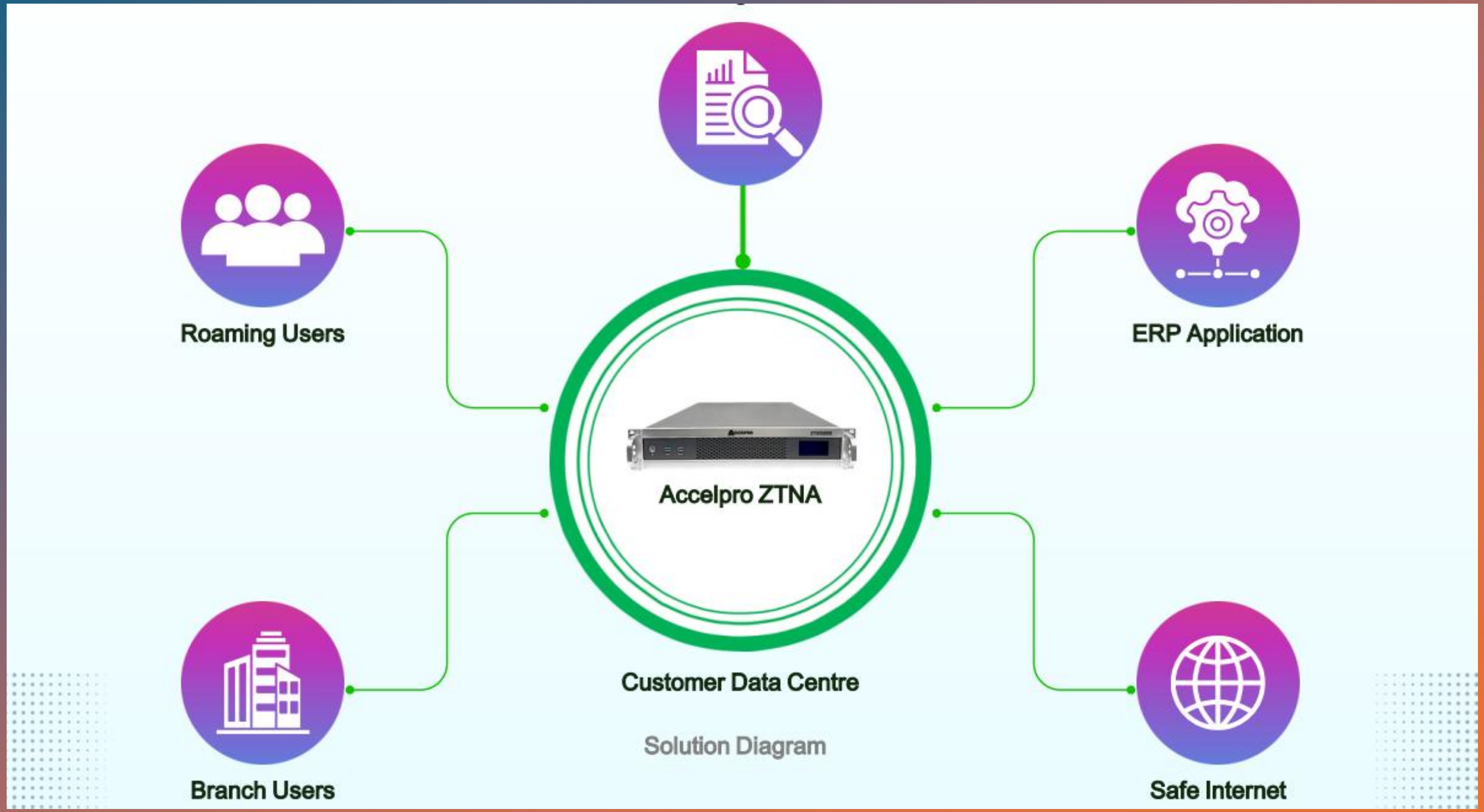

AI


AGENTIC AI
AGENTIC AI:
THE HACKER'S
NEW SUPERPOWER

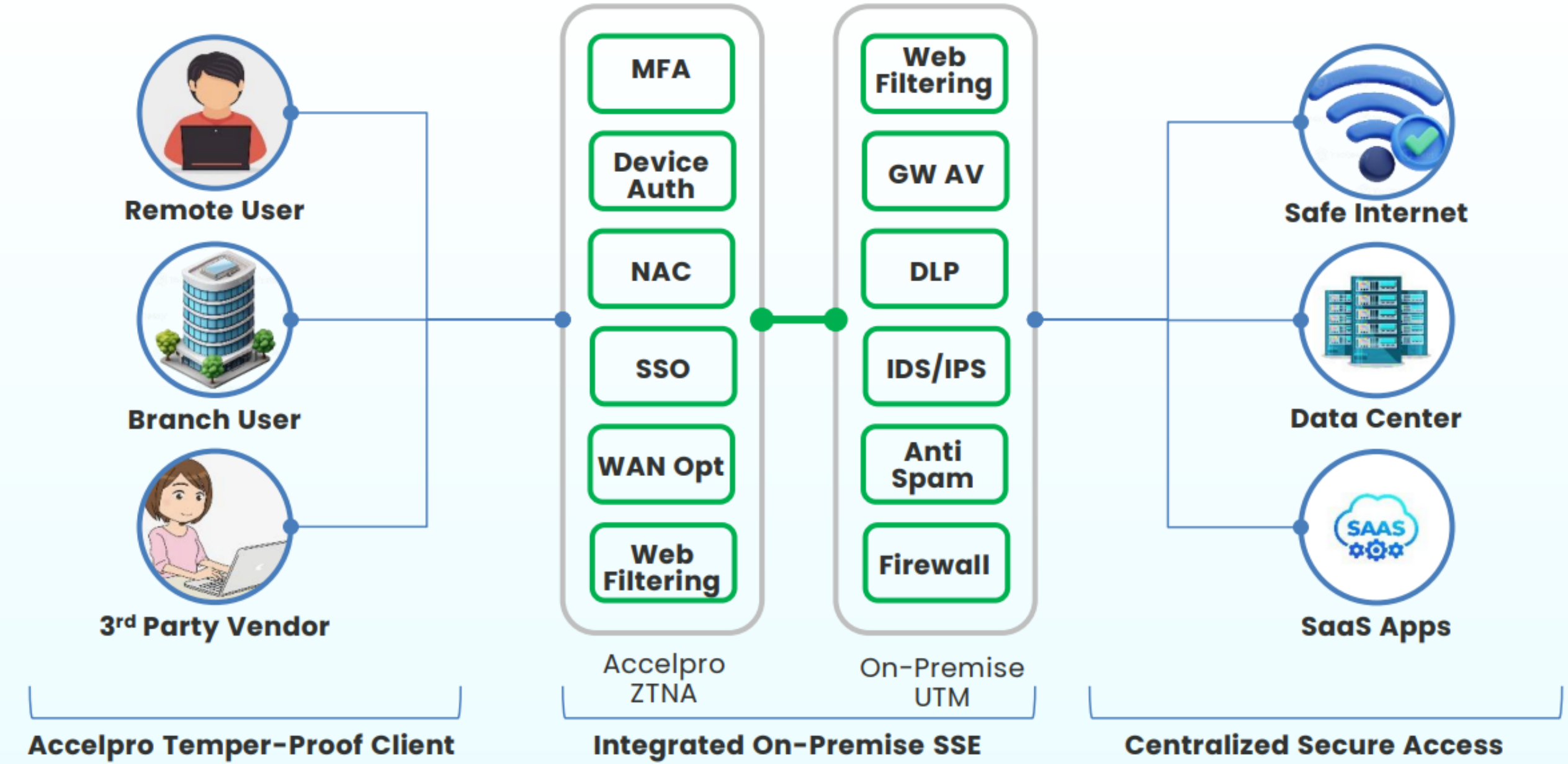
Cyber Solutions Trend 2026

BlueZebra
Network Security


Corporate Network
Network Security Appliances
Datacenter
Security
Speed
Latency
Cost
Complexity
Private Cloud
Public Cloud
Internet
ZTNA
Remote Users

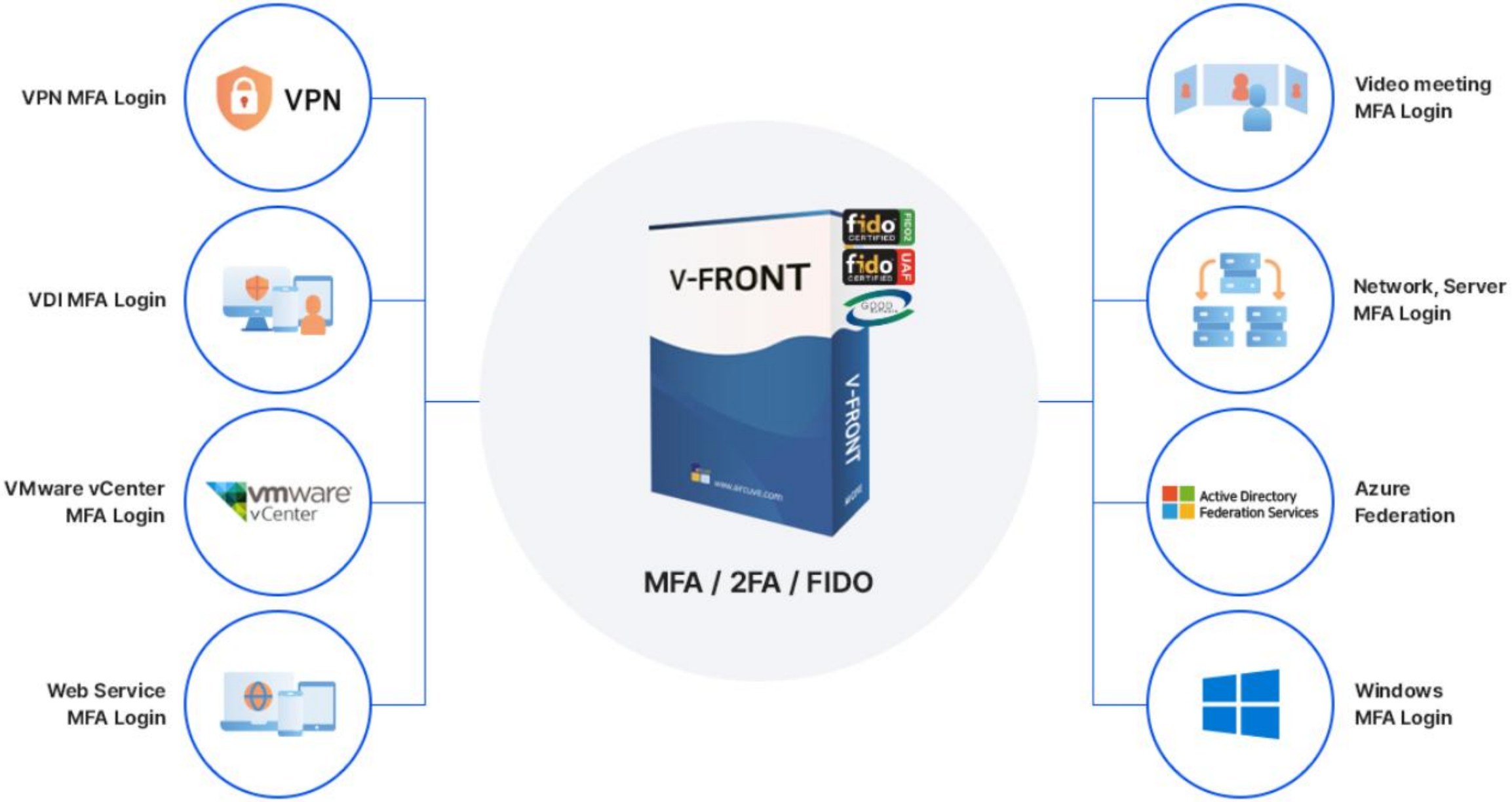


Solution Diagram



On-premise Accelpro ZTNA – UTM Integrated SSE platform Approach Diagram


Multi-Factor Authentication
Password
Verification
Access



Platform for additional user authentication

The quantum threat is approaching

Why organisations should start planning now

Part 1:
The problem

RSA & ECC today
Secure against classical computers by using factoring and discrete logarithms.

Quantum threat
Shor's algorithm on a quantum computer could break RSA and ECC.

Part 2:
The solution

Post-quantum cryptography (PQC)
New encryption methods based on math problems that remain hard for both classical & quantum computers.

Part 3:
Algorithm families

Lattice-based
Foundation of ML-KEM & ML-DSA; uses high- dimensional algebraic structures.

Hash-based
Relies on secure one-way hash functions; basis of SPHINCS+.

{...}
Multivariate
Uses polynomial equations; still in research stages.

Part 4:
NIST standards

ML-KEM (FIPS 203)
Standard for key establishment.

ML-DSA (FIPS 204)
Standard for digital signatures.

SLH-DSA (FIPS 205)
Stateless hash-based digital signature scheme.

Takeaway

PQC is the standards-led path forward — practical and deployable today.

PRIMUS X CYBER VAULT

when innovation meets performance

securosys

SOC AUTOMATION VS MANUAL SOC OPERATIONS

Morpheus AI
Security Intellingence

80% ⓘ This is a high priority case and we advise you to investigate this further.

When it happened	Attack Classification
July 8, 2025, 19:52:17 UTC	Credential Theft via Phishing and Malware

A phishing email titled HR Report was sent to Administrator. The user extracted the attachment HR Report.rar and opened the malicious file HR_Report.xlsm, which executed a macro launching EXCEL.EXE (PID 9484). This process initiated a chain of events that led to the download and execution of commander.exe and the credential dumping tool mimikatz.exe.

Morpheus Analysis

Attack Progression

1. Initial Access: Administrator received and opened a phishing email with a malicious attachment.
2. Execution: Malicious macro in HR Report.xlsm executed, launching cmd.exe (PID 11760) .
3. Persistence: Scheduled task created to execute tmp.vbs periodically.
4. Credential Access: mimikatz.exe executed to dump credentials on LAB1-PC1.

Why It Matters

The attacker successfully executed credential dumping tools, potentially compromising sensitive user credentials, which could lead to further unauthorized access and lateral movement within the network.

Morpheus AI Attack Timeline

Older First ↓

1/8/2025 11:53:00 UTC

Executed malicious macro.

EXCEL.EXE (PID 9484) opened a HR_Report.xlsm and executed malicious macro. This was performed by EXCEL. EXE (PID 9484) and initiated from a HR_Report.xlsm.

Execution | T1204.002

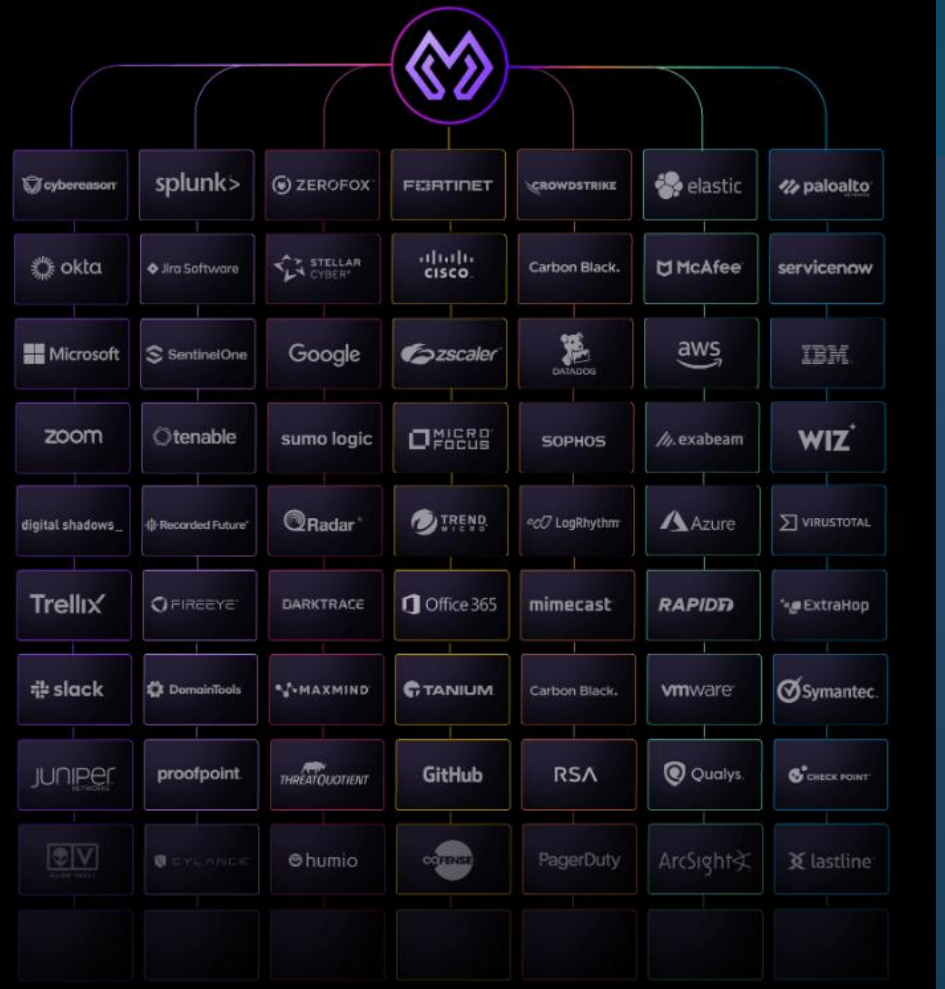
Morpheus AI Graph

Hi! How can help you today?

- Quarantine Affected Endpoint(s)
- Block Malicious IOCs
- Reset Credentials & Audit Accounts
- Harden Email & Endpoint Defenses

Autonomy + Control + ROI

Morpheus is like putting a world-class analyst on every alert. Morpheus runs 24×7 at machine speed, cutting per-investigation cost and improving MTTR. Unlike Tier-1 queues or unaccountable MSSPs, you get full visibility.



AI Foundation	Purpose-built cybersecurity LLM trained on attacker TTPs and real IR data	*Generic models or rule-based logic*
Investigation Depth	L2+ investigation depth on every alert	*Sample-based or manual analyst review*
Stack Coverage	Traces context across your entire stack and back through time	*Siloed tools, manual correlation*
Integration Maintenance	Self-healing integrations, zero engineering maintenance burden	*Dedicated engineering effort for break/fix*
Investigation Output	Attack path, risk score, MITRE mapping, and IR recommendations	*Raw alerts, minimal context*


Thank you