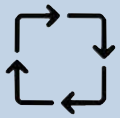
Pete Slade, Founder & CEO
info@threatwarrior.com
+1 512-937-3837

PROBLEM

Existing threat detection solutions are inadequate


Perimeter


Cloud

Log Reader

Software Agent

They miss many places that bad actors can hide


Printers


Raspberry Pi


Cameras


Watches/Phones/Tablets


Industrial Control Systems


Copiers


Thermostats


Speakers


Intrusion Hardware

Crypto-Miners

Example: Rogue Device & Hack

Jet Propulsion Laboratory
California Institute of Technology

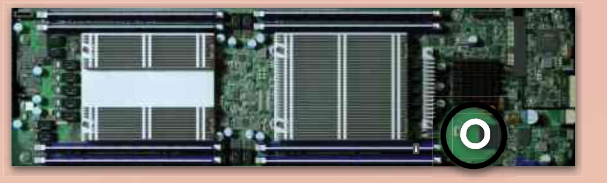
- Compromised via unauthorized device
- Stole major mission data
- Used as gateway into deeper network

Example: Industrial Control Systems

TARGET

- Attacked through 3rd party HVAC vendor
- Stole 40+ million credit and debit cards
- Stole 70+ million customer records

Example: Nation State Hardware Implant



- Embedded mini-computer during manufacturing
- Compromised technology supply chain

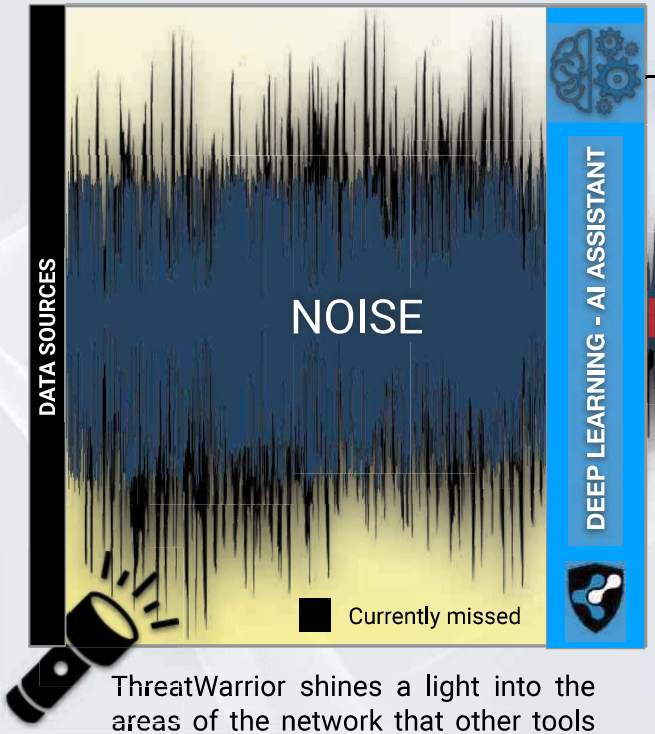
https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

PROBLEM vs. SOLUTION

- Lots of data, lots of noise!
- Lack of actionable information
- Forces companies to use their most expensive IT Security labor on lower tier issues

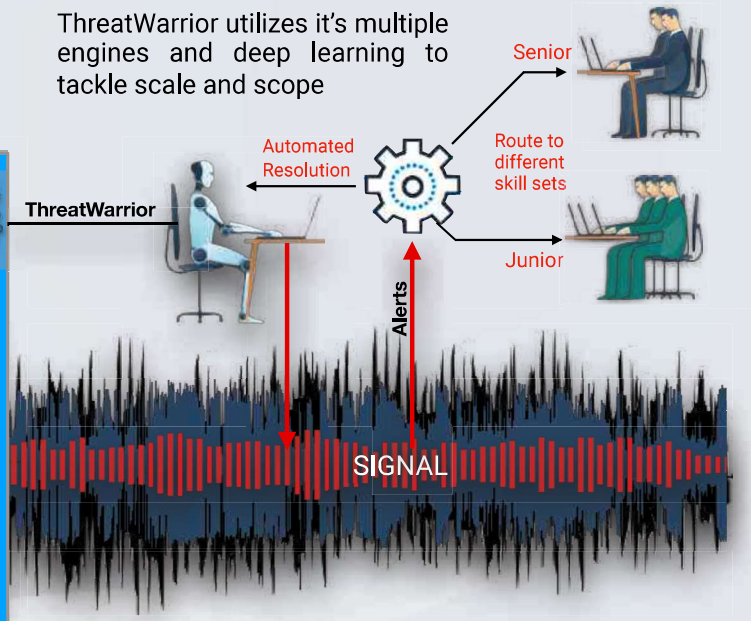
- Scaling noise to resources is not the answer
- Scale and Scope is too large for humans

Most Organizations Are Not Seeing Everything!



ThreatWarrior shines a light into the areas of the network that other tools miss

ThreatWarrior utilizes it's multiple engines and deep learning to tackle scale and scope



- Superior visibility via 3D user experience
- Continuous asset detection
- Single view of assets & threat surface
- Policy recommendations
- Skills based routing
- Empowers cheaper IT Security labor

MULTIPLE ENGINES

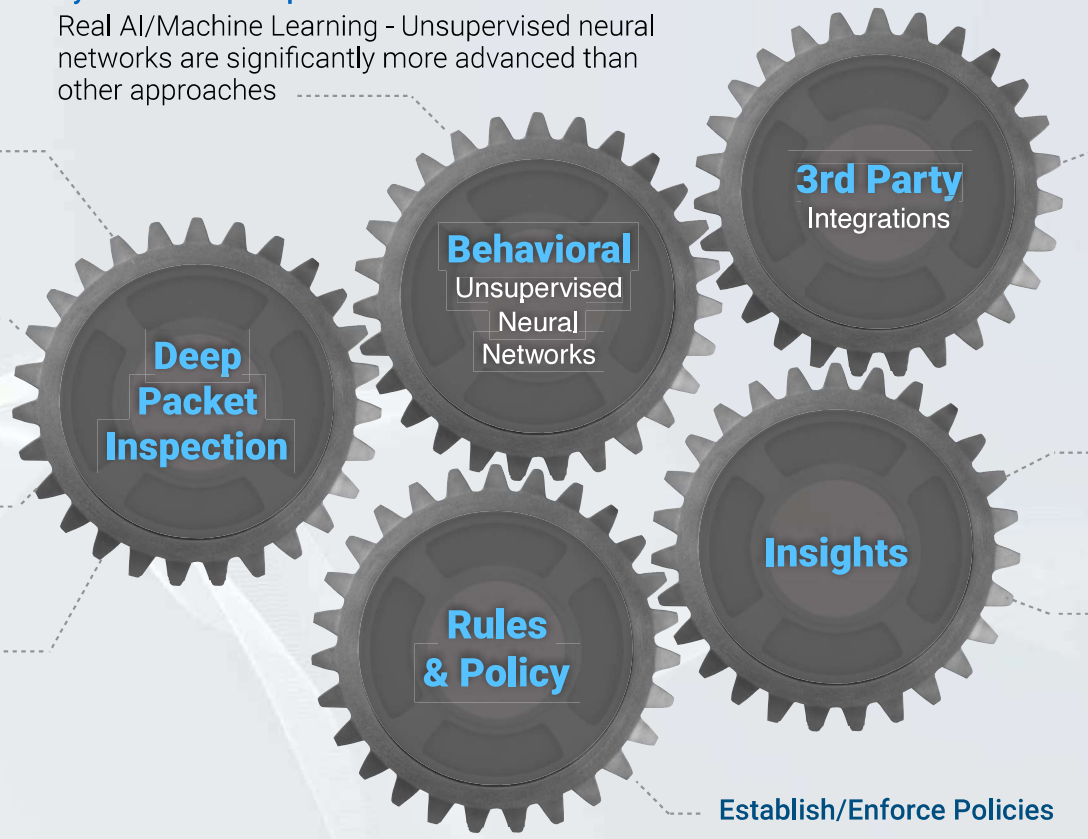
Cyber Immune Response™
Real AI/Machine Learning - Unsupervised neural networks are significantly more advanced than other approaches

Asset/Dependency Mapping
Gain complete visibility into all assets and resources, tracking any changes or additions

Identify Malware/Trojans
Identify all threat types - known and unknown- including malware, trojans and APTs

TLS/Encrypted Traffic
Observes encryption handshake, packet headers and compares behavior

Traffic Discovery
230+ protocols
6+ million traffic classifications



Optional - 3rd Party Integration
Pluggable engine technology to allow full integration.
Carbon Black.

Coherent Change Detection
Alert to slow changes and emerging patterns observed over time

Learns from traffic and analyst
Learns from observing network traffic and from how analysts respond to threats

Establish/Enforce Policies
Define policies and compliance rules for your organization

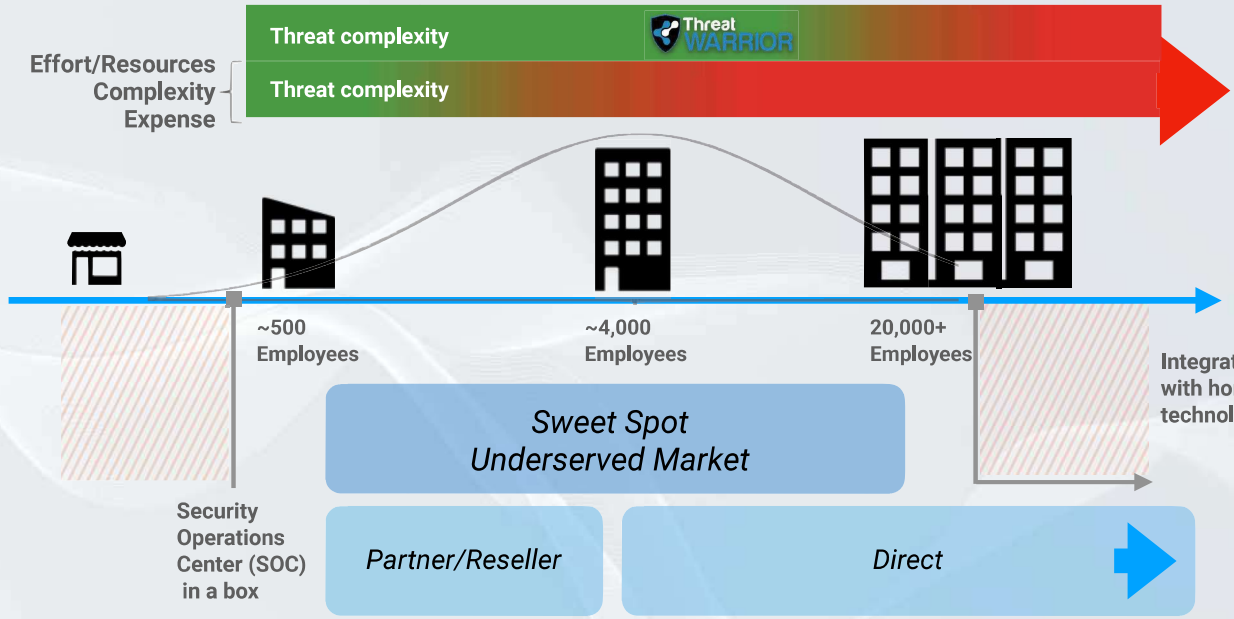
- Agentless solution
- Visibility into everything connected
  - On-premise
  - Cloud environments

On Premises Co-Location

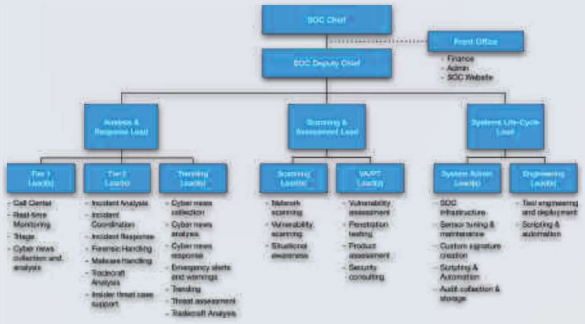
Azure aws Google Cloud

MARKET FIT

Everybody wants to prevent threats…



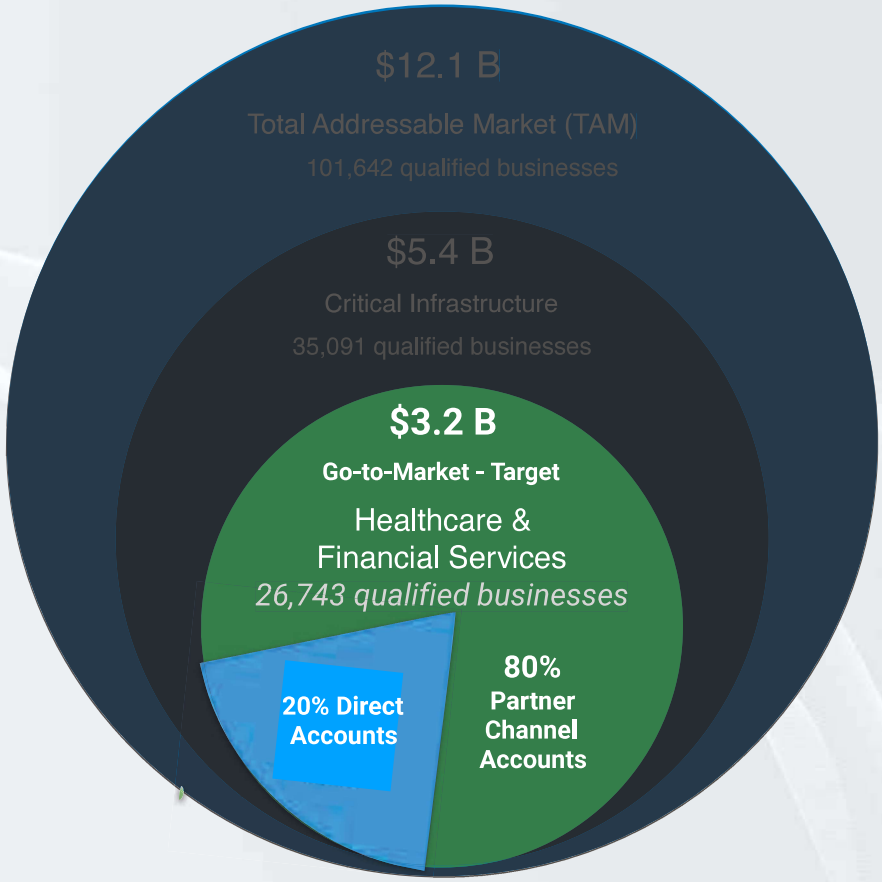
Cybersecurity Resources



ThreatWarrior levels the playing field in the fight against global cybercrime by equipping all organizations with advanced cybersecurity

https://www.nmhc.org/news/articles/cyber-hygiene-prevents-80-percent-of-breaches/%

USA Total Addressable Market / Go-to-Market



- Focus: United States
- Average annual subscription: $120,000
- Statistics of U.S. Businesses Employment and Payroll Summary: 2012, released February 2015

Target Customer

- High threat targets
- Regulated
- 3-6 people in their SOC
- 300+ employees, $10M+ Revenue
- Buyer: CIO, CTO, CISO

Go-to-Market

- Leverage Moffitt
- Leverage Experian
- Leverage Carbon Black
- We build the best product and let partners provide services


Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
Network Firewall
Deception
ICS + OT
Network Threat Detection & Forensics
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Operations & Incident Response
SIEM
Security Incident Response
Market
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting & Services
Blockchain
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB
Security Analytics
AWAKE
Bay Dynamics
DARKTRACE
Dtex
empow
exabeam
Fluency
FORTINET
HanSight
haystax
IMVISION
IronNet
JASK
MICRO FOCUS
mistnet
observe it
paloalto
patternex
Reservoir Labs
RSA
Sec
SECURONIX
TripleCyber
ERAMIND
THETARAY
VECTRA
Veriato
vmware

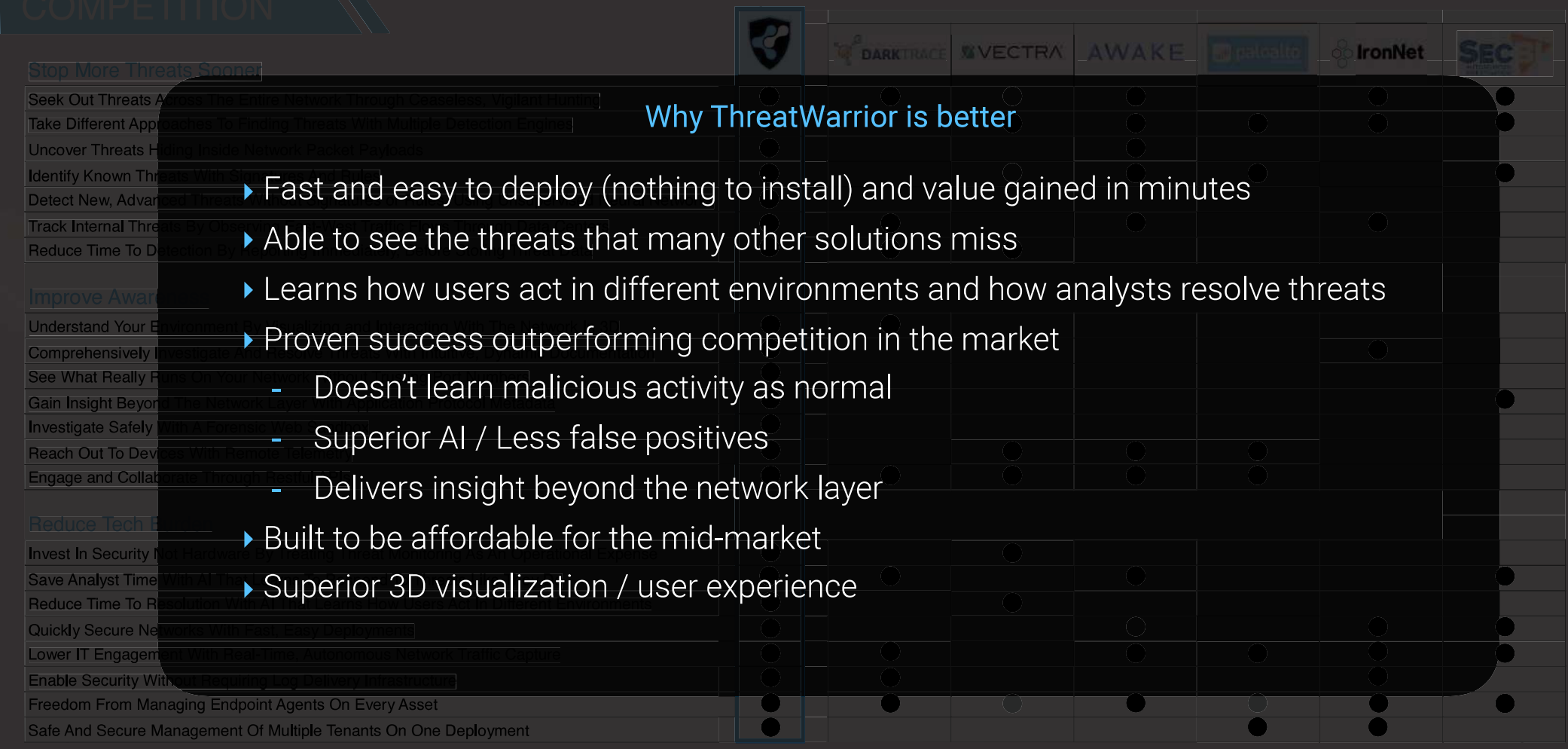
CATEGORY

Threat WARRIOR = (Network Threat Detection & Forensics + Security Analytics)

COMPETITION

	Threat Warrior	DarkTrace	Vectra	Awake	Paloalto	IronNet	Sec3
Stop More Threats Sooner							
Seek Out Threats Across The Entire Network Through Ceaseless, Vigilant Hunting	●	●	◐	●		●	●
Take Different Approaches To Finding Threats With Multiple Detection Engines	●		●	●	●	●	●
Uncover Threats Hiding Inside Network Packet Payloads	●			●			
Identify Known Threats With Signatures And Rules	●		◐	●	●		●
Detect New, Advanced Threats Without Signatures or Rules, Using Unsupervised Neural Networks	●						
Track Internal Threats By Observing East-West Traffic Flows Through Data Centers	●	●		●		●	
Reduce Time To Detection By Reporting Immediately, Before Storing Threat Data	●	●	●				
Improve Awareness							
Understand Your Environment By Visualizing and Interacting With The Network In 3D	●	●					
Comprehensively Investigate And Resolve Threats With Intuitive, Dynamic Documentation	●					●	
See What Really Runs On Your Network Without Trusting Port Numbers	●						
Gain Insight Beyond The Network Layer With Application Protocol Metadata	●						●
Investigate Safely With A Forensic Web Sandbox	●						
Reach Out To Devices With Remote Telemetry	●		●	●	●		
Engage and Collaborate Through Restful APIs	●	●	●	●	●		
Reduce Tech Burden							
Invest In Security Not Hardware By Treating Threat Monitoring As An Operational Expense	●		●				
Save Analyst Time With AI That Learns To Respond To Threats Like They Do	●	●		●			●
Reduce Time To Resolution With AI That Learns How Users Act In Different Environments	●		●				
Quickly Secure Networks With Fast, Easy Deployments	●			◐		●	●
Lower IT Engagement With Real-Time, Autonomous Network Traffic Capture	●	●		●	●	●	●
Enable Security Without Requiring Log Delivery Infrastructure	●	●				●	
Freedom From Managing Endpoint Agents On Every Asset	●	●	◐	●	◐	●	●
Safe And Secure Management Of Multiple Tenants On One Deployment	●				●	●	

COMPETITION



Why ThreatWarrior is better

- Fast and easy to deploy (nothing to install) and value gained in minutes
- Able to see the threats that many other solutions miss
- Learns how users act in different environments and how analysts resolve threats
- Proven success outperforming competition in the market
  - Doesn't learn malicious activity as normal
  - Superior AI / Less false positives
  - Delivers insight beyond the network layer
- Built to be affordable for the mid-market
- Superior 3D visualization / user experience

GO-TO-MARKET

Direct

Sell To

Segment Focus

Enteprise | Federal/DoD

Notable Customers

experian.

MOFFITT CANCER CENTER

Notable Pipeline

mastercard

windstream.

Alliance Partner

Sell With

Segment Focus

Enteprise | Federal/DoD

Notable Partners

Carbon Black.

Notable Pipeline

Secureworks

windstream.

Channel Partner

Sell Though

Segment Focus

Enteprise | Federal/DoD

Notable Partners

Involta

Notable Pipeline

CDW

Guiding Principals

- Leverage the sales teams of Alliance Partners and Channel Resellers wherever possible
- Avoid building large Enterprise Sales organization and demand generation engines until financial conditions justify the investment
- Invest in alliance partner management and channel programs
- ThreatWarrior Marketing to focus on very specific persona messaging and the digital experience
- Incremental headcount will align to growth expectations

PROVEN RESULTS

Results

Malware | Content | Compromised | Configuration | Policy/Compliance | Infrastructure

Case Studies

experian

Involta