City of San Bernadino – Solution Summary

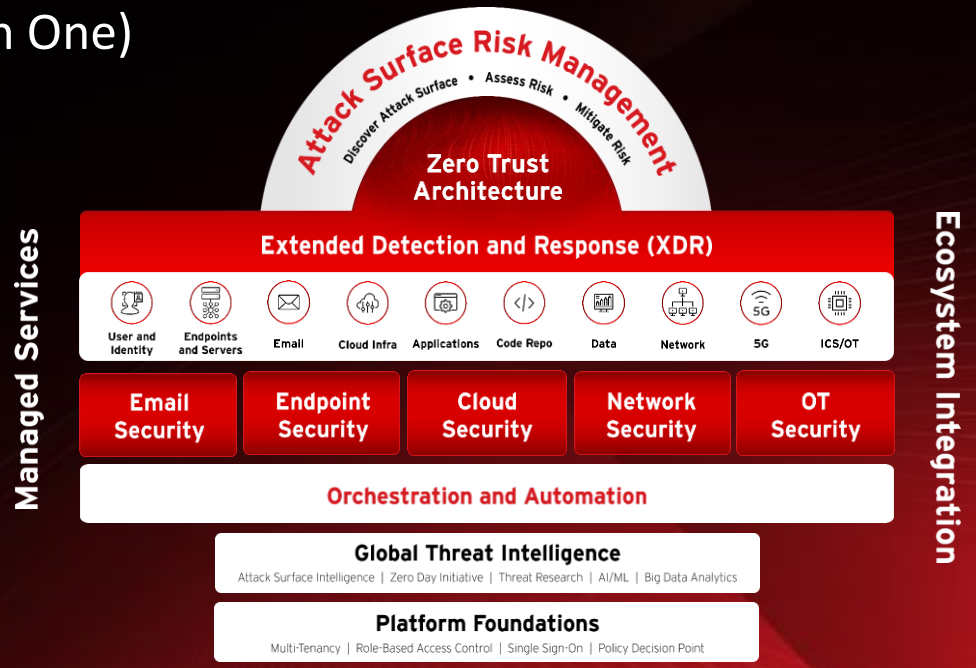
2024 Budget Spend

Cody Reagan

Regional Account Executive

Project Goals

- Streamline security process with single platform approach (Vision One)
- Prevent exposure to attack
- Add layers of redundancy for wider visibility of threats
- Shift process from reactive to proactive
  - Understand risks in a preventative way
- Continue to integrate tools into Vision One Platform



Budget Summary

Current Spend	Lisc.	Annual Cost ($) (est.)	Renewal Date
Smart Protection Complete Bundle	1,050	$27,000	18-Aug
V1 Network	2GB	$13,500	31-Oct
Service One Complete	1,050	$35,500	31-Oct
Credits	22,100	$11,500	31-Oct
Credits	21,000	$10,500	18-Aug
	Total	$98,000	

Proposed Spend	Lisc.	Annual Cost ($)
SPC -> Vision One Endpoint Security (core)	1,050	$13,251.00
Vision One Endpoint Security (Pro) - For servers	120	$14,928.00
Tipping Point (inline IPS) (two locations)	5GBx2	$107,436.22
V1 Network Sensor	2GB	$8,504.64
Service One Complete	1,050	$27,289.50
Credits	43,100	$17,240.00
	Total	$188,649.36

Vision One credits can be applied to any expansion of services or growth of current environment

Currently they are being used to add XDR and ASRM to all endpoints

Trend Vision One – Endpoint Security offerings

1,050 licenses for user and city devices

120 licenses for servers

	Core	Essentials	Pro
Primary endpoint type	User endpoints and basic servers	User endpoints and basic servers	Critical endpoints including servers and workloads
Windows, Linux and Mac OS	●	●	●
Antimalware, behavioral analysis, machine learning, web reputation	●	●	●
Device control	●	●	●
DLP	●	●	
Firewall	●	●	●
App control	●	●	●
Intrusion prevention – IPS (OS)	●	●	●
Virtualization protection	●	●	●
EDR-XDR		●	●
Intrusion prevention – IPS (server application)			●
Integrity monitoring / log Inspection			●
	Core	**Essentials**	**Pro**
Email Security	+	+	+
Mobile Security	+	+	+
Network Security	+	+	+
Cloud Security	+	+	+
Zero Trust Secure Access	+	+	+
MDR / Service One		+	+
Attack Surface Risk Management (ASRM)		+	+

+ indicates add-on option

Vision One - Endpoint Security (Pro)

TREND MICRO Vision One
Endpoint Security

Value Toward Goals

- Replacing Apex One in server environment (not designed for servers in mind)
- Strengthening Vision One with robust server data and acting as a backup to Tipping Point internally

- Purpose-built security for endpoint, server, and cloud workloads
- Single console for visibility and management; protection and EDR
- Connected IT/SecOps workflow
- Part of Vision One platform natively

Vision One - Endpoint Security (Core)

TREND MICRO Vision One
Endpoint Security

Value Toward Goals

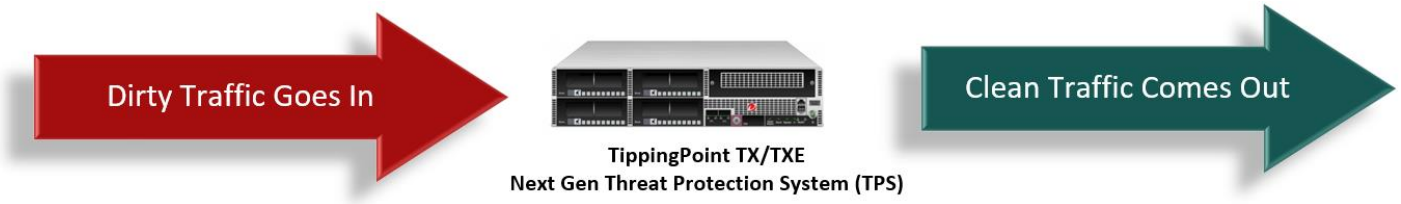
- Continued push into Vision One in all endpoints
- Simplify visibility with native connection into platform
- Will replace the on-premise Apex which was a target during attack

Threat detection capabilities

- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks)
- In-memory analysis for identification of fileless malware
- Variant protection
- Census check
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- Data loss prevention (DLP)
- Device and application control
- Ransomware rollback
- Sandbox and breach detection integration
- Extended detection and response (XDR)

Tipping Point – Threat Protection System (IPS)

Pre-emptive threat prevention TippingPoint TPS, deployed inline, inspects and blocks all directions of traffic (inbound, outbound, and lateral) in real time, protecting your environment against known, unknown, and undisclosed vulnerabilities.



Value Toward Goals

- Adds layer of protection that is physical and in your environment (sits behind firewall)
- Feeds essential data to Vision One when anything gets past edge security
- Blocks malicious behaviors automatically
- Virtual Patching to reduce overall risk exposure

Service One Complete

- Proactive Alerts and Threat Hunting
- Detect and Respond Faster
- Extend Your Team
- Maximize Effectiveness & Skills
- **24/7/365 global support**
- Assigned Service Manager and priority case handling
- Managed XDR using MITRE ATT&CK framework and proprietary threat hunting tools
- Product and threat training for your team
- Regular sync meetings and health checks
- 40 hours of IR Services (**used in October to stop an active threat**)

Value Toward Goals

- Essential in the mitigation the recent attack
  - Incident response team was involved within hours
- Round the clock monitoring at a fraction of the price of 24/7 staff or 3rd party SOC
- Drives involvement of the city and Trend to be aware of all risks, alerts, and attacks together
- Frees up time for proactive risk assessment and less time looking at alerts

Vision One – Network Monitoring

- All network connected assets continuously tracked
- Unsanctioned assets identified
- Endpoint protection methodically and holistically deployed
- Option to add sandboxing
- Assets not fit for agent protection defended at the network layer
- Provide actionable data to ASRM and XDR efforts in Vision One

Value Toward Goals

- Sees all network traffic and not just what has a Trend agent on
- Used for deep understanding of environment and forensics (similar to how our IR team does research with DDI)
- Strengthen view of the attack surface and risks associated
- Deep analysis of traffic and behaviors
- Virtual sensors highly adjustable and configurable to see anything missing or when the are infrastructure changes

