Benefits

Complete Install and Configuration

- Installation and configuration is facilitated by experts
- Internal resources are freed up to focus on other business priorities

Internal Resource Training

- Staff is trained to maintain prevention status and respond to threats using best practices

Identification and Remediation of PUPs and Malware

- Malware is quarantined
- Recommendations for managing potentially unwanted programs (PUPs) are provided
- Alerts are classified

The Best Return on Investment

- CylancePROTECT® and CylanceOPTICS™ are optimized, increasing their efficacy in the environment
- ROI is increased and obtained faster by relying on experts to operationalize
- Prevention status is achieved quicker than with any other solution

While implementing new security solutions can be exciting for a company, optimizing them for specific environments can put a stress on already limited IT resources. The need to protect, identify, and act on progressive threats can be challenging for even the most experienced security teams. Cylance® Consulting's proven methodologies ensure maximum value and security are achieved as quickly as possible with little to no disruption to systems or vital processes.

That's where ThreatZERO Services can help. Cylance Consulting's experts provide a **refreshing mix of technological expertise and personalized white glove service to optimize CylancePROTECT and CylanceOPTICS and move environments into prevention while providing measurable results of progress** throughout the process..

Service Overview

Facilitated through a dedicated Engagement Manager, ThreatZERO Services provide a collaborative environment to assist clients in optimizing the installation, reviewing best practices, delivering training, supplementing internal resources, and receiving expert guidance in mitigating any risks that are identified. The phases of a ThreatZERO Services engagement include:

CylancePROTECT

Kickoff
- Overview of deployment schedule
- Discuss installation options/strategy
- Console training and setup
- Provision and configure disconnected options
- Review of best practices

Phase 1
- Consultants quarantine malware as alerts are generated
- Status meetings
- Completion of agent installation

Phase 2
- Consultants and the Threat Analysis team continue monitoring the console

- Status meetings
- Completion of agent scanning

Phase 3
- Continue monitoring the console
- All malware is quarantined
- All alerts are classified
- PUPs are reviewed
- Devices are moved to an auto-quarantine and memory alert policy
- Memory alerts are completed

Phase 4
- Continue monitoring the console
- Memory alerts are reviewed
- Devices are moved to a memory block/terminate policy

At the conclusion of the engagement, clients are brought to a state of zero active threats and can move into a state of *prevention*.

CylanceOPTICS
- Console setup
- Build InstaQueries

- Configure rules and actions utilizing the Context Analysis Engine
- General best practice and interface navigation

What You Get ThreatZERO Services

	ThreatZERO (Foundational)	ThreatZERO + Compromise Assessment	Managed Prevention	Managed Prevention and Response
Legacy AV Rip and Replace	●	●	●	●
Full Auto-Quarantine	●	●	●	●
Expert Handling of All PUPs and Malware	●	●	●	●
Memory Protection Blocking Exclusion Handling	●	●	●	●
Script Control / Macro Protection Handling	●	●	●	●
Best Practices Training	●	●	●	●
Remediation Based on HealthCheck Results	●	●	●	●
Compromise Assessment to Reveal Previous or Potential IOCs		●		
Ongoing Care and Remediation of Issues			●	●
Recurring Solution Health and Status Metrics			●	●
Active Hunting				optional
Incident Containment / Malware Analysis	optional	optional	optional	optional

ThreatZERO Add-Ons

Compromise Assessment
Determine if attackers are active in your environments or have evaded security measures.

ThreatZERO Resident Expert
This low-cost solution provides a dedicated, on-site administrator to support unique security requirements and help shut down critical incidents in less time.

Managed Prevention
An ongoing care strategy that assesses and remediates issues, and ensures maximum security and continued return on investment.

Managed Prevention and Response
Delivers solution optimization and adds varying levels of monitoring and threat intelligence up to 24x7 to provide seamless active threat identification and alerting using a prevention-first approach.

ThreatZERO Training Services
Learn to maintain ThreatZERO status and respond to threats in the environment utilizing best practices.

CYLANCE™

20180328-2018