TRACE3

SOLUTION PROPOSAL

Gigamon and Dynatrace Unified Observability Proof of Concept (POC) Four (4) Weeks

ENGAGEMENT PRE-REQUISITES

dynatrace Gigamon®

The Enterprise environment pre-requisites for the Gigamon and Dynatrace POC integration and operations consists of:

1. On-premises, customer managed datacenter, single and multi-cloud, and/or hybrid infrastructure with development or production operational instances of Gigamon and Dynatrace.
2. Production and/or DevTest workloads and services within the infrastructure that are currently being serviced by Gigamon and Dynatrace operational instances.

PHASE 1 – ASSESSMENT

FOCUSED TIMELINE – WEEK 1

Plan & Kick Off → Configuration Validation → Assessment → Review

INCLUDED ACTIVITIES

Workstream 1 – Phase 1: Enterprise assessment in the following areas:

- Pre-requisite infrastructure validation
- Baseline application performance, security, and visibility of the existing workloads
- Application migration and modernization journey
- Tool strategy for existing and migrating workloads
- Application security and architecture topology dependencies

DELIVERABLES

- Executive Level read out presentation:
  - Assessment session outcomes and tracking
  - Engagement and open items tracking
- Stakeholder Assessment Workshops
  - Up to (8) 1-hour Assessment Stakeholder Workshops

PHASE 2 - IDENTIFICATION

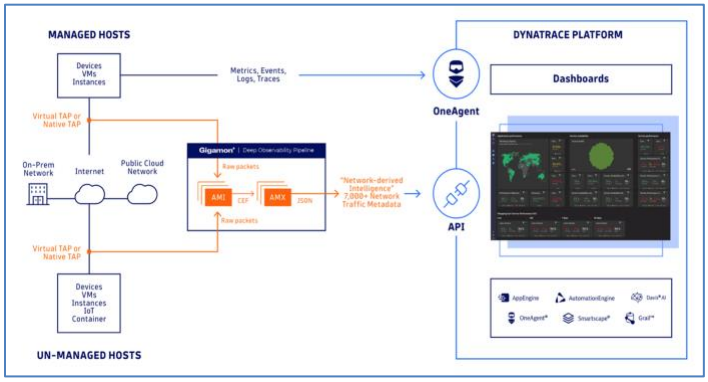
FOCUSED TIMELINE – WEEKS 2 - 3

Stakeholder Sessions → Use Case Validation → Design Acceptance → Planning

INCLUDED ACTIVITIES

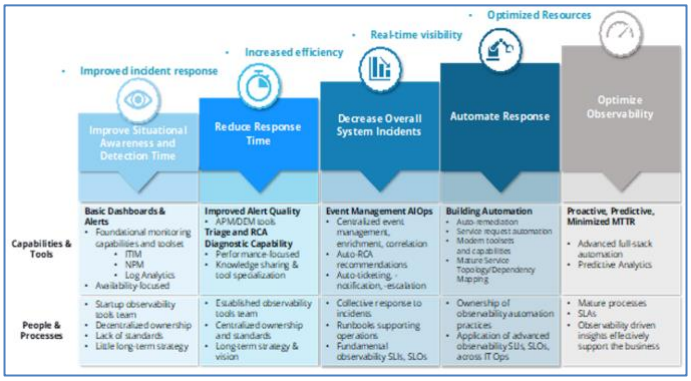
Workstream 1 – Phase 2: Identification of configuration and operational characteristics in the following areas:

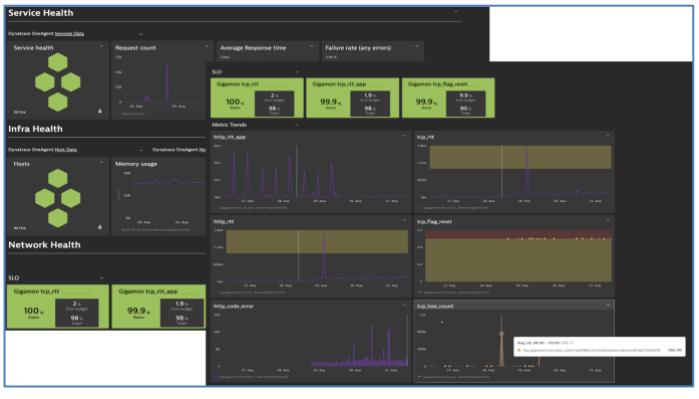
- Pillars: application, security, infrastructure, network, cloud
- Bring relevant Persona together
- Use Cases: Security, Application, Infrastructure, and Network
- Opportunities to reduce tool sprawl, inconsistent tooling experience across hybrid/cloud environment
- Scope for Architecture improvements
- Cloud Cost optimization
- Self-Healing/ Auto Remediation of issues
- Automation of observability – deploy, configure, maintenance
- Pipeline automation using observability data
- Automated Security/ Vulnerability Identification



DELIVERABLES

- Executive Level read out presentation.
  - Assessment and Identification session outcomes and tracking
  - Engagement and open items tracking
  - Detailed Use Case decision documentation
  - Design build documentation for POC integration
- Stakeholder Identification Workshops
  - Up to (8) 1-hour Identification Stakeholder Workshops





PHASE 3 – PROOF OF CONCEPT

FOCUSED TIMELINE – WEEKS 3 - 4

POC Implementation → Use Case Findings Analysis → Outcomes and Next Steps → Close

INCLUDED ACTIVITIES

Workstream 1 - Phase 3: Proof of Concept deployment, analysis, and recommendations for the following activities:

- High touch deployment set up and PoC targeted use cases on-prem or Cloud
- Provide Causation, SLO, and Starter Pack use case templates
- Identify key network metadata attributes to test
- Overhead EC2 agents tacked from Dynatrace
- Automate SLO creation
- Automate pipeline and release validation
- Automate self healing and self remediation
- Cloud cost optimization

Estimated Service Delivery Timeline
3 - 4 Weeks
Customer Investment
$45,000

DELIVERABLES

Finalized Executive Level read out presentation:

- Finalized engagement and open items tracking
- Use Case Analysis, and Adoption recommendations relative to the customer environment with roadmap
- Action items and next steps

- Deployment Documentation and Automation
  - Finalized As built documentation

KEY OUTCOMES

- Gain a full suite of security options directly to your SOC:
  - End-to-End Observability
  - Add Observability data to Network data in Pre-Production and production as developers
  - Leverage AI based tools for predictive and prescriptive analysis
  - Test code not only by CPU, response times, and failure rates, but also by packet size, number of DB calls, network response times, and user experience
  - Catch bugs before they ever make it to production
  - Enable the creation of security gates in your pipelines by auto failing builds on found vulnerabilities

Trace3's certified architects and engineers, partnered with client teams, and Partner SME's, will utilize our proven methodology and deep reference architecture experience to deliver an actionable, and prioritized, set of read-outs featuring the way Gigamon and Dynatrace Unified Observability can be adopted into the Enterprise Security and Operations.