New Methods for Post Event Investigation

Using Dynatrace tools and Endace Network History

Retrospective Analysis for Deep Insight

Software services are in constant flux

- Today's service definitions will not match tomorrow's network
- Quality of reporting relies on accurate software services configuration
- Auto-discovery and Activity Analytics enables precise service identification

Network history enables retrospective analysis

- Playback into AMD hosted in Application Dock on EndaceProbe
- Auto-discovery mode and all decodes can be enabled
- Enables regular, rapid and accurate tuning of software services

Deeper Insights into a Dynamic Network

Historical analysis of transactions of interest

- Ideal for transactions that don't meet threshold for immediate action
- Use results to retrospectively understand interaction and dependencies
- Ideal for new interactions that may not be considered "relevant" at discovery

Deep discovery through playback of days of network history

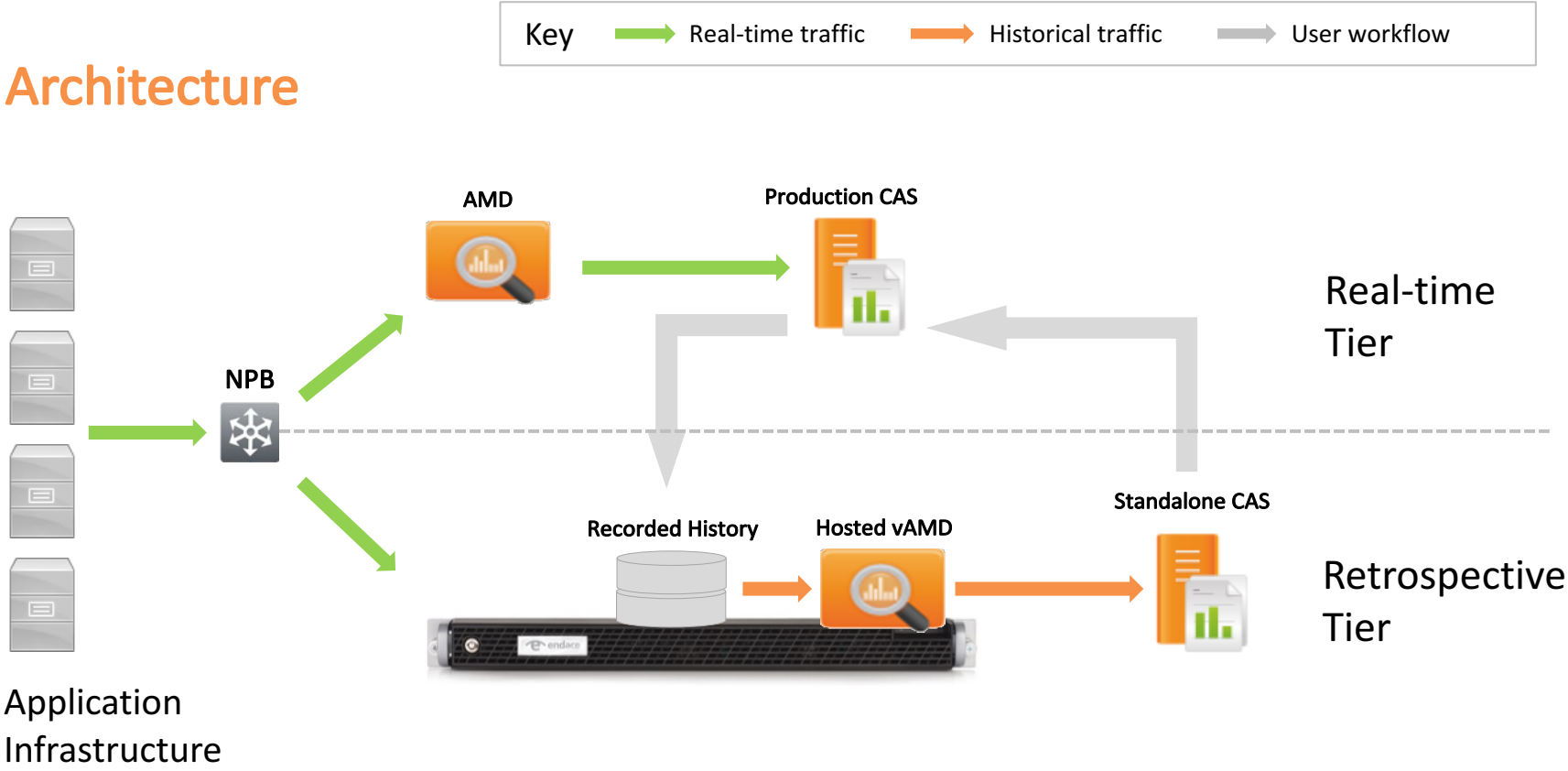
- Discovery mode results are valuable but Discovery is computationally expensive
- Playback weekday traffic over weekend for iterative network insights

How to Deploy

Retrospective Tier

- EndaceProbe records days to weeks of live network traffic
- Virtual AMD hosted in Application Dock on EndaceProbe
- Recorded traffic played back into hosted vAMD
  - Based on transactions seen in real-time CAS
  - Selected by user through drill-down in EndaceVision
- AMD connected to standalone Retrospective Tier CAS
- Analysis available for escalation or tuning of Real-time Tier configuration

Architecture



Network History for Real-time Investigation

Packets for real-time analysis

- EndaceProbe supplies packets on demand to real-time CAS via Smart Packet Capture integration
- Applications teams can provide Network teams with ground truth
  - No need to wait till next time when there will be a sniffer connected
- Dynatrace Network Analyser (DNA) can consume EndaceProbe PCAPs for use in expert analysis
- Long term archiving of PCAPs to NAS for subsequent investigations
- Security teams can access network history for breach analysis

Summary

Real-time analysis depth limited by fundamental physics

- Packet rate and cost of computation
- Analysis depth a compromise between cost and quality of information

EndaceProbe Playback provides a unique retrospective option

- Non-peak time deep analysis of days or weeks of history
- Selective deep analysis driven by analysts
- Regular auto-discovery mode analysis to capture dynamic network changes