InvestigationManager

InvestigationManager is a software application for performing centralized investigations across multiple EndaceProbes and vProbes.

Designed for analysts involved in APM, NPM, and threat hunting, it provides network-wide traffic search and analysis from a single pane of glass.

At the heart of InvestigationManager™ is EndaceVision™, a browser-based investigation tool that lets analysts select data sources from multiple EndaceProbe™ Analytics Platforms and analyze recorded traffic from all these sources simultaneously.

EndaceVision provides a variety of data visualization tools, including traffic breakdowns, top talkers, flows and conversations. Users can drill-down by time, user, server, protocol, application, or a variety of other attributes.

Once they have identified relevant 'packets of interest', analysts can view these packets directly using a Wireshark™ UI – removing the need to download large packet capture files across the network to a local host for analysis. Analysts can also use the File Extraction feature to automatically recreate files and generate Zeek logs from recorded packet data.

INVESTIGATIONMANAGER AT A GLANCE

- A powerful software tool for conducting investigations that span fabrics of Endace appliances, including geographically distributed EndaceProbes, vProbes™ and EndaceProbe stacks.
- Browser-based graphical user interface, CLI, and REST API
- Incorporates EndaceVision, which provides a variety of data visualization tools, including traffic breakdowns, top talkers, flows and conversations.
- Decode and view packets of interest with the built-in UI, or using Wireshark via one-click integration.
- File extraction feature automatically extracts files and generates Zeek logs from selected packet data.

BENEFITS

- Rapid, network-wide investigations across on-premise, private cloud and public cloud networks.
- Amazingly fast search times. A needle-in-a-haystack search[2] across mutiple EndaceProbes and stacks containing petabytes of network history typically takes less than a minute regardless of the number of appliances being searched.
- Automation of investigations across multiple Endace appliances, a "single pane of glass" view, and amazingly fast search times dramatically increase analyst productivity.

Components of an EndaceFabric

EndaceProbe Analytics Platform

To ensure end-to-end visibility, EndaceProbes are typically deployed in various locations across the network, often at points of interconnect with the public internet, subnetworks, branch offices and private data centers.

The EndaceFabric™ architecture (see Diagram 1) solves the challenge of managing large numbers of distributed EndaceProbes across multiple environments (including public cloud) and performing investigations that span multiple EndaceProbes at the same time. Multi-tenancy enables multiple organizations or deparments to share

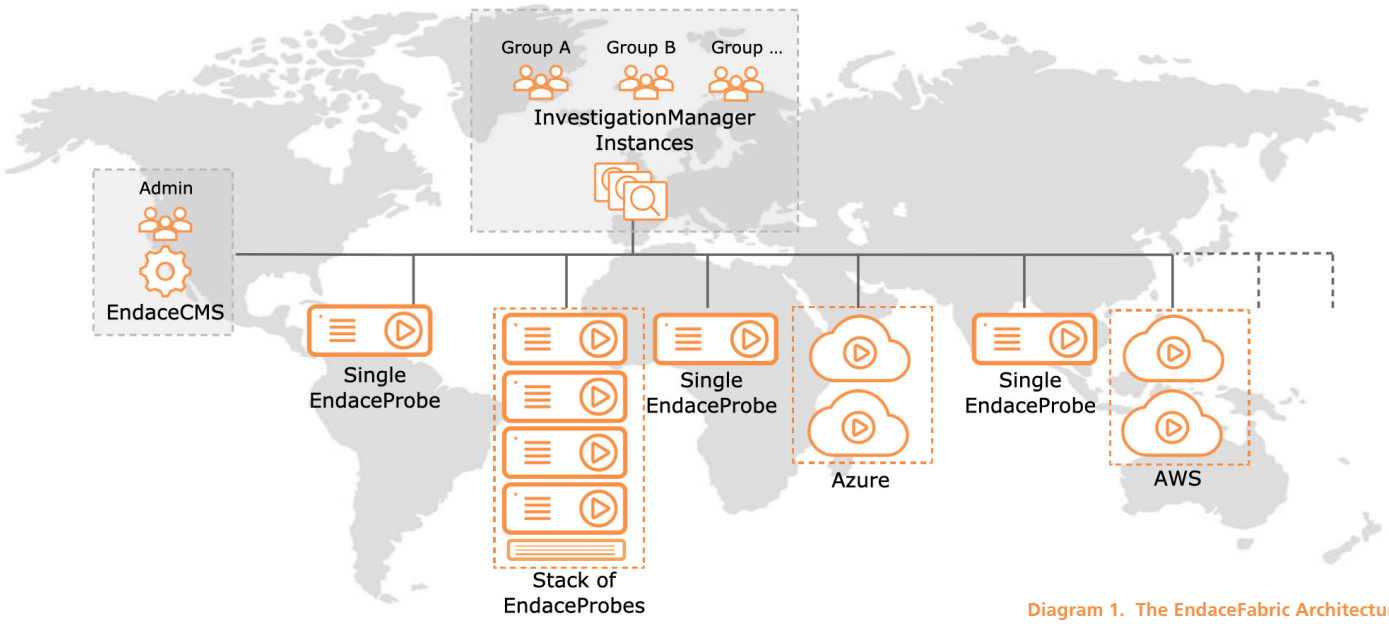

Diagram 1. The EndaceFabric Architecture

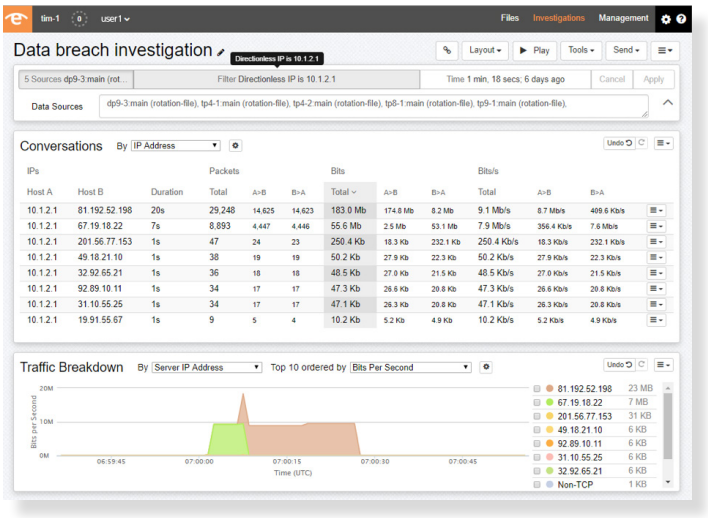

Diagram 2. The InvestigationManager UI

an EndaceFabric while being restricted to accessing only their own packet data.

EndaceCMS

EndaceCMS™ Central Management Server enables centralized administration of the fabric, such as user account management, software upgrades, appliance configuration, and health monitoring.

InvestigationManager

InvestigationManager lets SecOps, NetOps and DevOps analysts conduct centralized investigations across a fabric of Endace appliances using InvestigationManager's rapid, network-wide search and datamining, and EndaceVision's powerful traffic visualization and analysis capability.

Flexible Deployment Options

InvestigationManager is available as a VMWare or KVM virtual machine image. Instances can be deployed on any appropriate server including on an EndaceProbe (where it requires a single Application Dock™ instance), or in AWS and Azure.

Several analysts may perform investigations simultaneously across some or all EndaceProbes on the network using the same instance of InvestigationManager.

Multiple instances of InvestigationManager can be deployed as required – increasing the number of investigations that can be conducted simultaneously by different users. InvestigationManager instances are deployed as virtual appliances and have a no-cost license.

InvestigationManager Specifications

Operating System	Endace OSm
User Interfaces	Browser based Graphical User Interface, Command Line Interface
Application Programming Interface (API)	REST
Maximum number of EndaceProbes/vProbes	100
Maximum number of user accounts	>100
Maximum number of active users	Unlimited. Scales up by deploying additional instances.
Storage	Minimum 50GB storage per instance
Application Dock	2 users: Single Dock 4 users: Double Dock 8 users: Quad Dock > 8 users: multiple instances
VMware	2 users: 12 GB RAM, 4 vCPUs 4 users: 24 GB RAM, 8 vCPUs 8 users: 48GB RAM, 16 vCPUs > 8 users: multiple instances
AWS	4 users: m5.2xlarge instance 8 users: m5.4xlarge instance > 8 users: multiple instances
Azure	4 users: Standard_D8s_v4 instance 8 users: Standard_D16s_v4 instance > 8 users: multiple instances

Orderable Items

VPRB-IM	Endace InvestigationManager for deployment in Application Dock™, VMWare ESXi, or KVM.

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com