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.

Components of an EndaceFabric

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 and performing investigations that span multiple physical EndaceProbes at the same time.

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

INVESTIGATIONMANAGER AT A GLANCE

Version 6.5.2

Released January 2019

- 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.

BENEFITS

- Rapid, network-wide investigations across an entire EndaceFabric. This fabric may consist of geographically distributed EndaceProbes and/or groups of EndaceProbes that have been stacked to form logical EndaceProbes with multi-petabyte storage capacity and packet capture rates of 100Gbps and beyond.
- 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.

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.

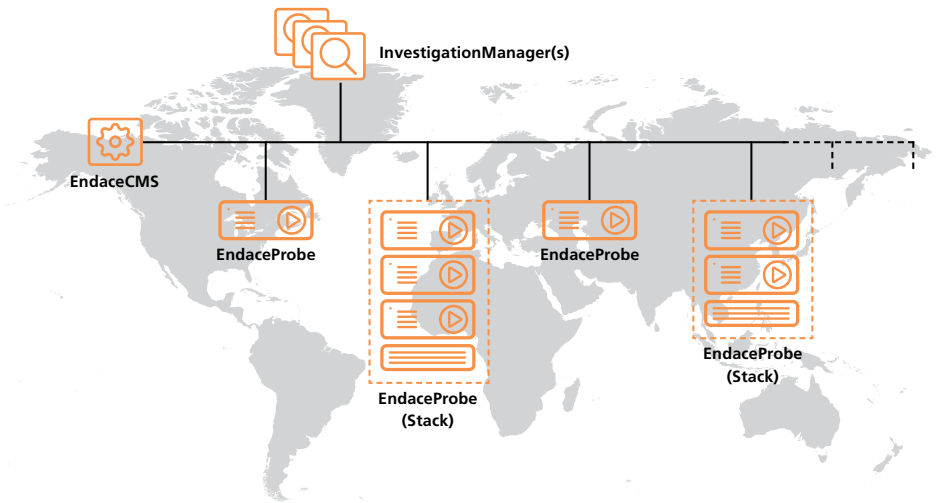

Diagram 1.
The EndaceFabric Architecture

© Copyright Endace Technology Limited, 2019. All rights reserved. Information in this data sheet may be subject to change.

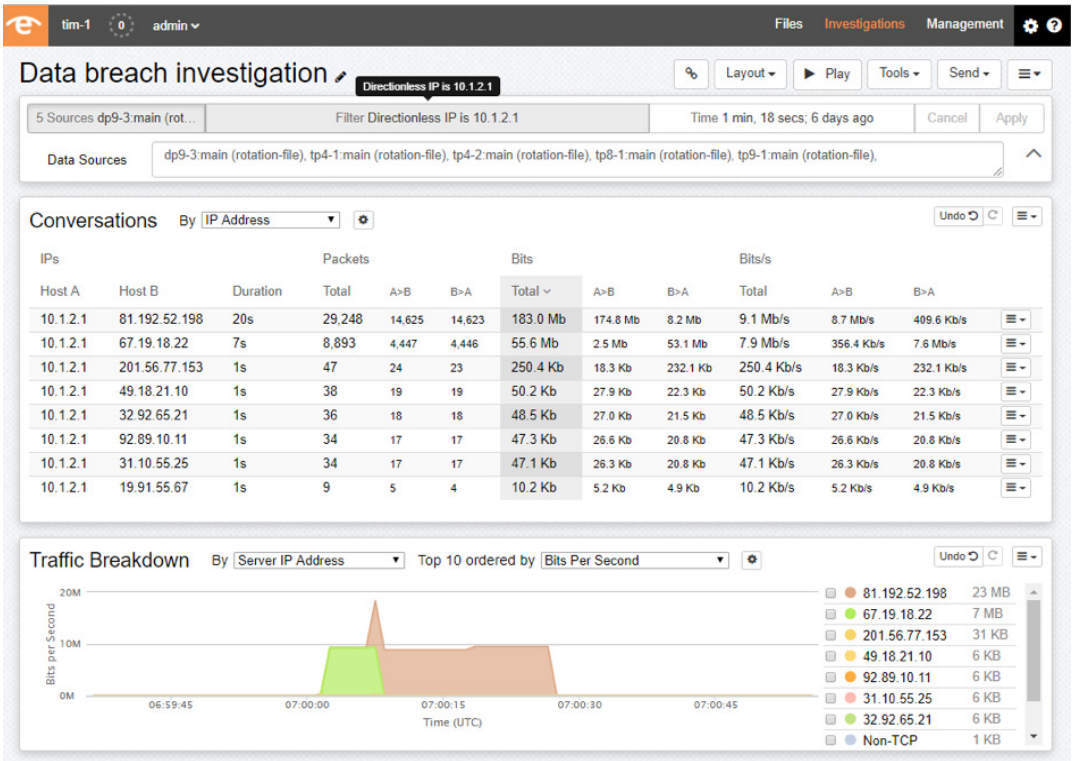

Diagram 2. The InvestigationManager UI

Flexible Deployment Options

InvestigationManager is available as a VMWare or KVM virtual machine image. Instances can be deployed on any appropriate server. We recommend deploying on a physical EndaceCMS appliance, where it takes a single Application Dock™ instance. The physical EndaceCMS appliance has storage that can be used for archiving packet data, and can host up to four instances of InvestigationManager.

Several analysts may perform investigations simultaneously using the same instance of InvestigationManager, with investigations potentially involving some or all of the same EndaceProbes.

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.

Orderable Items

VPRB-IM	Endace InvestigationManager for deployment in Application DockTM, VMWare ESXi, or KVM.
EP-4000-CMS	EndaceCMS pre-installed on server hardware. 1RU, 20 CPU cores, 128GB RAM, 16TB RAID storage, 750W redundant AC PSU.

InvestigationManager Specifications

Operating System	Endace OSm
User Interfaces	Browser based Graphical User Interface, Command Line Interface
Application Programming Interface (API)	REST
VM requirements - Application Dock	1 x Single Application Dock Instance
VM requirements – KVM, VMware	12GB memory, 50GB storage, 4 x vCPUs
Maximum number of EndaceProbes/vProbes	100
Maximum number of user accounts	>100
Maximum number of concurrent active users	5

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

For further information, email: info@endace.com

Endace™, the Endace logo and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

© Copyright Endace Technology Limited, 2019. All rights reserved. Information in this data sheet may be subject to change.