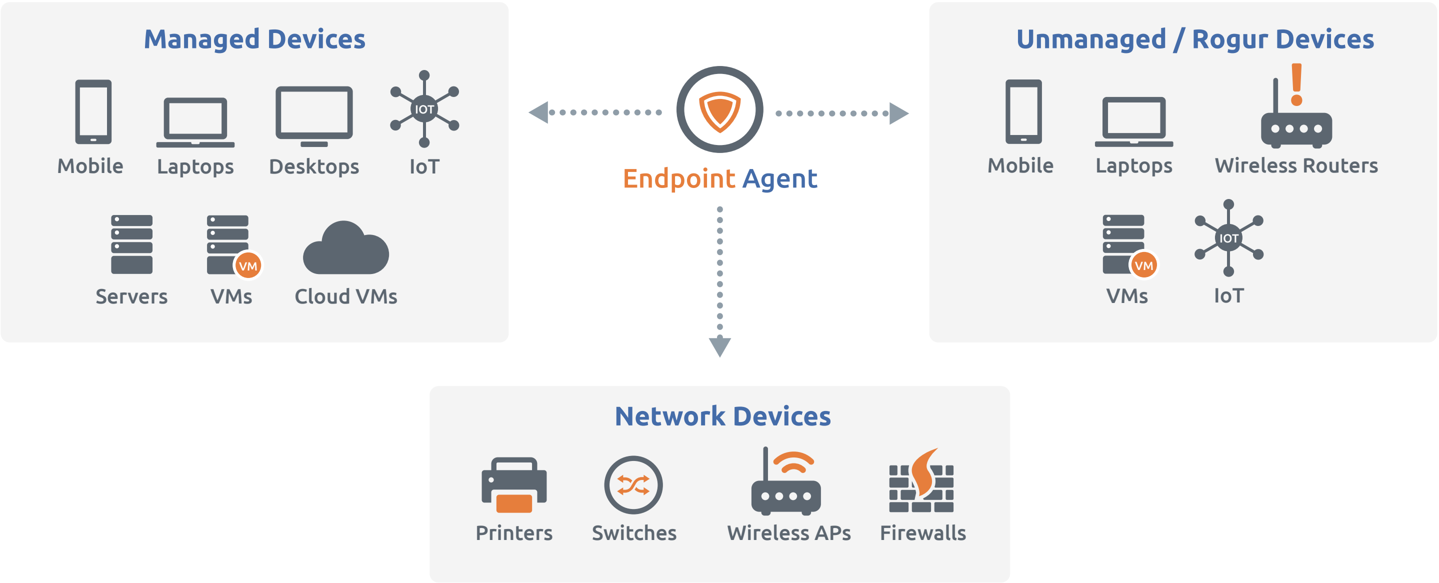
Data Sheet

Endpoint Agent: All-the-Time Visibility

User mobility and the migration of business-critical apps to the cloud have forever changed the way networks are managed end-to-end. Seeing, understanding, and controlling the end user experience now depends on visibility from data source to the endpoint device.

Siloed endpoint tools provide only partial, point-in-time performance data leaving gaps for IT teams – exposing organizations to unacceptable risks and unnecessary costs. LiveNX with Endpoint Agent provides all-the-time visibility and control for client devices, servers, and cloud VMs.



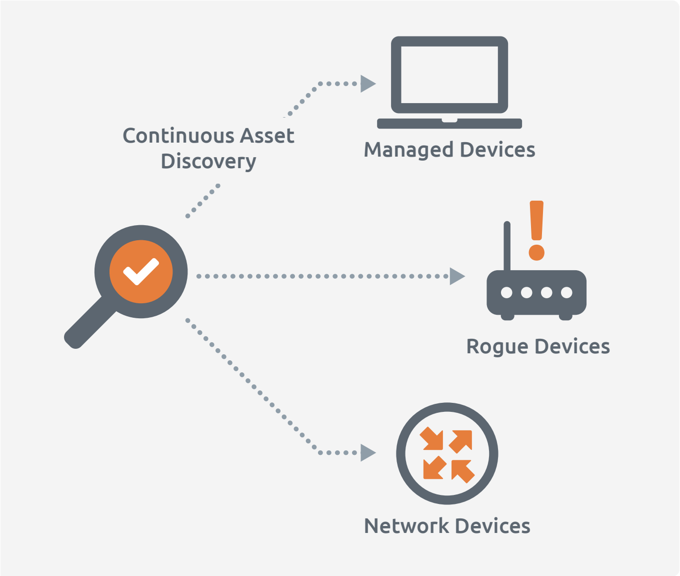
All-the-Time Visibility

Continuous Endpoint Data Collection

Endpoint Agent provides continuous, rich data collection from every managed endpoint including systems, user behavior, network connectivity, application, binary, and process data. Once collected, you simply ask the questions and Endpoint Agent provides the answers – now and for the past 12 months or more of activity.

Any Asset – Client Device, Server, and Cloud

Endpoint Agent easily deploys to client devices, data centers, and enterprise clouds. With the shift to cloud services well underway, Endpoint Agent solves the cloud visibility issue. The lightweight Endpoint Agent agent supports a full range of Windows, Mac OSX, and Linux operating systems and is quick and easy to deploy. Usually it is Deployed as part of the “gold image” for physical and virtual devices.



Anywhere – On-Network or Off-Network

Employees regularly work outside the corporate network, accessing cloud and data center applications. Monitoring and protecting users off network can be particularly difficult. Endpoint Agent, however, provides continuous monitoring and data capture for all managed endpoints, whether on-network (local), off-network (remote), or offline completely.

End-to-End Control

Continuous Monitoring, Alerting and Actions

Continuous device state and behavior monitoring; real-time issue, threshold, and threat based alerting and ticketing; and automated and/or manual endpoint actions provide IT teams control over every managed asset – just like being at the keyboard.

Unmanaged IT Asset Discovery

Endpoint Agent supports continuous discovery of all connected devices - physical and virtual - including on network, off network, in the data center and the cloud. Using continuous, passive discovery, Endpoint Agent avoids point in time, active scanning that misses infrequently connecting assets and risks triggering security tool alerts. Endpoint Agent provides rich data, fingerprinting each device including: IP address, hostname, MAC address, device manufacturer, and device type.

IT Systems and Vulnerability Management

Endpoint Agent's device monitoring enables common systems management activities such as IT asset discovery and inventory, and software discovery, foreground and background usage tracking, and on-going license rationalization. Additionally, proactive systems analysis and issue response / repair capabilities improve helpdesk operations and mean time to repair. Further, continuous device state monitoring enables risk management through on-going policy posture checks and enforcement, and vulnerability assessments and patch installs.

Incident Response and Containment

Remotely investigate and remediate any endpoint, anywhere simplifying and accelerating incident response. Endpoint Agent provides numerous isolation techniques like system network quarantine, USB key ejection, and USB port disablement. Further, threat containment actions such as registry key edits, file deletion, process termination, and service restarts help eliminate threats.

Deep Lookback Forensics

Endpoint Agent enables 12 or more months of robust forensic data storage. Deep forensics data accelerates tracking attacker's lateral movements and provides retroactive alerting on all systems that exhibit or have exhibited similar behaviors. And most importantly, finding the root cause of each issue to close the gaps and stop future attacks across the entire environment.

Extend the Value of Existing Tools

Broad IT and Security Tool Integrations

Data sharing is critical in today's IT and security tool ecosystems. Endpoint Agent's RESTful API provides simple data sharing and integrations, and access to all raw collected data, not just metadata. Workflow integrations include ticketing / orchestration systems, SIEM tools, and systems management platforms. And security tool integrations include vulnerability assessment tools, patch management systems, data analytics, etc.

Scalable, High-Performance Architecture

Cloud-Based or On-Premise Delivery

Endpoint Agent is built on a highly scalable Vertica Analytics Database, with an Apache Kafka message broker, and Jetty Web Servers. It exceeds the scalability and performance needs of enterprises and supports multi-tenant service provider capabilities. Endpoint Agent is available through a cloud-based delivery model, and for enterprises with unique requirements it can be deployed on-premise.

Dramatic Endpoint Scale and Performance

Endpoint Agent's architecture delivers a resilient, redundant backend that supports high-availability and ensures stability at massive scale. Endpoint Agent supports up to 1 million endpoints per customer with near real-time alerting performance. And it is designed to maintain the highest levels of data integrity and privacy protection to ensure a fully auditable data record across client devices, data centers, and cloud assets.

Continuous Feature Delivery

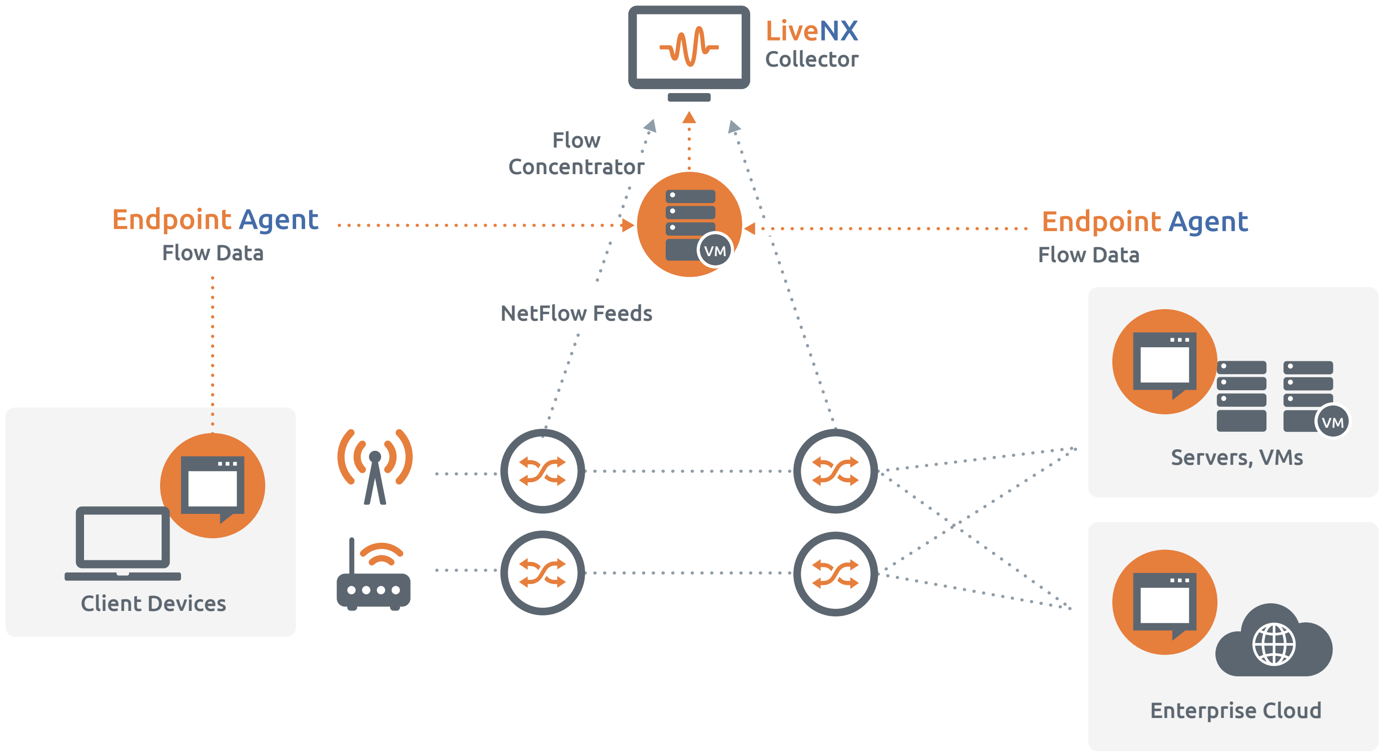
Endpoint Agent is designed for safe and continuous upgrades and feature delivery. This simplifies administrative maintenance, eliminates on-going software validation and IT teams, and eliminates waiting for pre-defined release schedules. Updates to active software is made with no downtime or loss of visibility or control. Continuous feature delivery is supported in both cloud and on-premise models.

Little to No Network or Endpoint Impact

Endpoint Agent is architected to deliver a low impact experience for end users and administrators. The simple agent has no driver, no kernel, and no reboot requirement. Running in user mode, the agent does not compete for device resources or impact normal user activity, and typically creates less network overhead per agent than daily email use – generally below 4MB per day.

Customizable Scripting

Endpoint Agent supports customizable data collection, monitoring, alerting, quarantine and remediation actions. Endpoint Agent's extensions allow organizations to create and run PowerShell or Bash scripts on any managed asset.



> *"Endpoint Agent gives us a handle on our company assets, and what our employees are doing with them. Our understanding of our endpoint environment is greater than it's ever been. Sticking with Endpoint Agent into the future was a no-brainer for us. It's helped our IT department in so many ways, and we're excited to see how we grow along with it."*
>
> **– Vice President of Information Security, Internet Services Provider**

> *"We're so much better informed than we were a year ago. Endpoint Agent has provided insights into our network that we didn't even know we needed."*
>
> **– Security Operations Center Manager, Business Intelligence Company**

Endpoint Agent Technical Specifications

Endpoint Agent Server Installation Requirements	
Endpoint Agent Intelligence	Java 1.8 JRE from the standard CentOS/RedHat repositories Jetty 9.3 included with the Cloud Installation Endpoint Agent installer Spring 4.3 included with the Endpoint Agent installer Spring Security 4.2 included with the Endpoint Agent installer
On-Premise Intelligence Cloud Installation	LiveAction will provide ready to use Endpoint Agent Server appliances in the form of OVA images. The images are created for ESXi 5.5+ but can be backdated by request. Endpoint Agent requires two VM's in production environments. An environment with over 35k endpoints requires custom setup from the LiveAction Support team.
Cloud Intelligence Cloud Installation	The LiveActionClient Services team will be solely responsible for config uring and maintaining customer's Amazon Web Services hosted server. Customers may also host LiveAction servers in their own cloud. The agent initiates an outbound SSL (HTTPS) connection to the server over ports 80 and 443 to send and receive data.

Endpoint Agent Installation Requirements	
Windows Agent Installation	Minimum Requirements Hardware: 1GHz processor / 2GB RAM / 10MB disk Software: Windows XP3 / Windows Server 2003
Mac OSX Agent Installation	Minimum Requirements Hardware: 1GHz processor / 2GB RAM / 10MB disk Software: Mountain Lion
Linux Agent Installation	Minimum Requirements Hardware: 1GHz processor / 2GB RAM / 10MB disk Software: CentOS 5+ / RHEL / Scientific Linux / Ubuntu 12+ / Fedora / Other flavors – Ask Support

Endpoint Agent Console Prerequisites Supported Browser Versions	
Endpoint Agent Console	• HTML5 compatible browsers only. • Google Chrome 34 or later (recommended). • Mozilla Firefox 29.0 or later. • Internet Explorer 10 and 11 (IE 9 is no longer supported). • Apple Safari 6.0 or later.

Key Features

- Single agent for client devices, servers, virtual machines, and containers
- Simple "no driver, no kernel, no reboot" agent installations
- Cloud-based or on-premise based delivery
- Continuous, not just point in time, silent IT asset discovery
- On-going visibility, and device state monitoring and assessments

Key Benefits

- Eliminate unmanaged IT assets
- Integrated IT asset and software management
- Reduce the number of non-compliant assets
- Protect against known and unknown threats
- Immediately respond to and contain detected threats
- Conduct lookback investigations for breaches and corrective actions

LiveAction 3500 West Bayshore Rd Palo Alto, CA 94303
Phone and eFAX: +1 888-881-1116
Email: sales@liveaction.com
Web site: www.liveaction.com