DATA SHEET

eSentire Atlas XDR Investigator

Enable your IT and Incident Response teams with state-of-the-art eDiscovery and forensics software.

Become Cyber Resilient

In today's threat environment, cybersecurity isn't just about knowing when a data breach occurs. To be cyber resilient, organizations need a combination of tools, methodologies, and hands-on personnel to discover, react, and minimize the potential impact of any digital security threat. Atlas XDR Investigator is a top eDiscovery, forensics and incident response enterprise software solution that goes beyond breach protection to enable real-time investigation, analysis and resolution of active, or potential threats, no matter the origin. No other enterprise software matches Atlas XDR Investigator's depth of endpoint visibility and speed to resolution.

Atlas XDR Investigator enables your Information Security, Incident Response and IT teams with unparalleled insight into incident response, threat hunting, digital forensic investigation, insider threat analysis and malware detection. With Atlas XDR Investigator, your cybersecurity personnel can quickly perform remote triage and forensic analysis, evidence capture, and incident remediation across networked servers and endpoint workstations, empowering forensic investigators to See More, Know More, and Respond Instantly to a wide range of digital security needs.

Key Benefits

✓ *Enable your IT and Incident Response teams with an eDiscovery and forensics tool trusted by government intelligence, federal law enforcement and military personnel.*

✓ *Address the ever changing landscape of potential cyber risk issues, such as malware infection, eDiscovery collection, IP protection, incident investigations/data spills, mergers and acquisitions, remote asset investigation, threat hunting, and internal investigations.*

✓ *Dramatically reduce the cost of any active or potential breach through our speed to resolution using our instant access to remote endpoints instead of traditional and costly "boots on the ground" incident response methods.*

See More. Know More. Respond Instantly.

With Atlas XDR Investigator, your IT team can evaluate running processes on every endpoint in near-real-time without impact to business or network operations. This unparalleled depth of endpoint visibility provides comprehensive investigation of data breach intrusions, zero-day exploits, and insider threats, providing a critical last line of defense for your network operations.

See More

- Search globally across your enterprise concurrently
- Perform remote, in-depth forensic investigations without leaving your office
- Perform live investigations in real time
- An optional agent stealth mode makes Atlas XDR Investigator activities difficult to detect on the endpoint

Know More

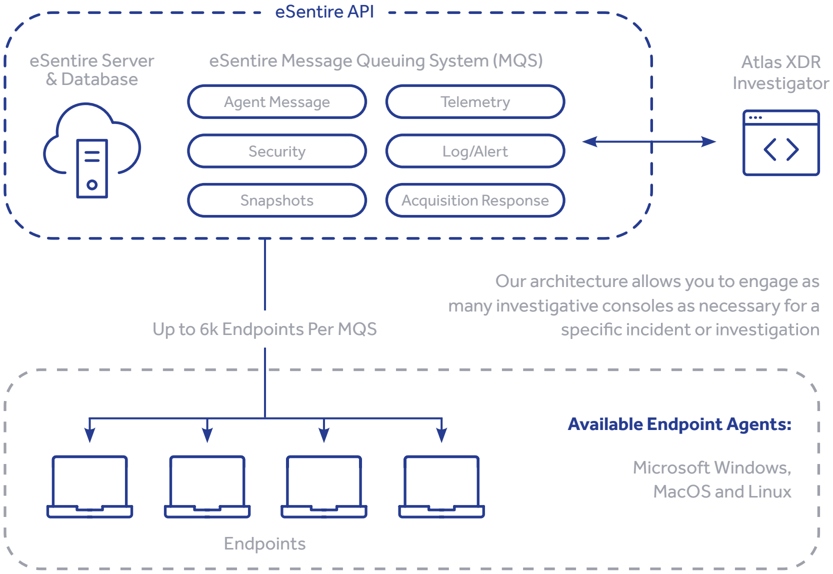
- Provides intelligence into system and network level activities through network and process telemetry
- View data about processes and their associated files, modules, registry settings, network connections and child processes running in RAM in real time
- View, analyze, recover, and acquire (if necessary) files and directories on disk
- Find malware or other indicators of malicious activity your other security tools and antivirus/EDR solutions might have missed

Respond Instantly

- Full remote imaging of hard drives (physical or logical), files, memory, or processes
- Collect screen shots of active user desktops and running process snapshots of remote systems
- Search across any number of endpoints for critical indicators of compromise
- Gain privileged command line access to any endpoint
- Selectively kill processes on an endpoint to stop active events
- Remotely mount an endpoint's media as a local drive to enable the use of additional forensic or operational tools

How It Works

Unlike solutions that limit your analysts to searching a small number of connections, eSentire Atlas XDR Investigator enables your team to search across the entire network of connected services and workstations concurrently.


eSentire API
eSentire Server & Database
eSentire Message Queuing System (MQS)
Agent Message
Telemetry
Security
Log/Alert
Snapshots
Acquisition Response
Atlas XDR Investigator
Up to 6k Endpoints Per MQS
Our architecture allows you to engage as many investigative consoles as necessary for a specific incident or investigation
Available Endpoint Agents:
Microsoft Windows, MacOS and Linux
Endpoints

> *"After we added Atlas XDR Investigator to our security stack, we were able to capture and analyze about 80% more data on our endpoints' health and activities than we could using 'our anti-virus solution' alone."*
>
> *CISO, Major Financial Services Institution*

> *"Once we demonstrated the capabilities of Atlas XDR Investigator, our legal department stopped requesting traditional full disk captures. By eliminating technical and logistical hurdles, eSentire has been a tremendous help in expediting our cases through increased productivity."*
>
> *Director, Global Cloud Provider*

Key Features

Best-In-Class Agent

- Data collection (applications, screen shots, network interface, file system, running processes, etc)
- Artifact retrieval
- Telemetry reporting
- File Search

Concurrent Endpoint Access

- Launch searches to concurrent endpoints
- Up to 6k endpoints per server
- Begin analyzing results almost immediately

Remote Forensic Analysis

- Connect remotely from anywhere to conduct or initiate an investigation
- System snapshots

Multiple Use Cases

- e-Discovery and data collection for HR investigations, M&A activity, corporate security and Personally Identifiable Information (PII) scanning
- Digital Forensics and Incident Response
- Endpoint process evaluation
- Compliance and litigation support

If you're experiencing a security incident or breach contact us ☎ 1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.