

REAL-TIME INFORMATION FOR MAXIMUM ENDPOINT SECURITY



The Challenge

Modern endpoints operate more “out” of the corporate physical and network boundaries compared to their traditional counterparts – which leaves them exposed to threats. Attackers and cyber criminals have also determined that endpoints have become the more vulnerable targets, and have started focusing their attention on endpoint applications. IT today lacks real-time information from these endpoints in order to be able to discover critical security, compliance and configuration issues quickly. This can lead to:

- Larger security issues across the broader IT setup than just the endpoints
- Time-consuming efforts of hours and even days to do routine endpoint health-checks
- Financial losses due to data breach
- Costly delays in identifying the precise location and scope of an ongoing attack
- Lack of visibility on how far the incident has spread and how deep a penetration has occurred



Solution

Accelerite Sentient for timely and quick actions

“Identifying a problem is often the hardest part of fixing it”

Accelerite Sentient pulls together real-time information from enterprise endpoints for IT administrators to quickly identify critical security threats and vulnerabilities, and address compliance and configuration issues in their endpoint network within minutes. Sentient allows administrators to proactively query the current status and existence/non-existence of configurations and files from the point of view of actively unearthing issues in real-time. It classifies and presents the information gathered in visual format with drilldown information, and makes it easy for IT to locate problem areas in their network of endpoints quickly. The search queries in Sentient are in freeform text format, which enables IT to easily query their endpoints using natural language phrases.

Sentient Solution Components

Sentient consists of components that enable easy querying, visual representation and quick response to endpoint information.

Up to date information straight from the source!

Sentient gets real-time information directly from endpoints within seconds, and not from a cache that is outdated with data that is hours or days old!

Natural language query processing

Sentient is equipped with entity-based natural language processing, which emphasizes key entities of interest to IT such as software, file, version, patch, CPU, memory, and so on. This enables administrators to type in their query as free form text and search through their critical assets and entities easily.

Dynamic graphical representation

Sentient provides dynamic and real-time graphs as query outcomes, which administrators can slice and dice in different ways, and filter them by subnets, platform types and operating systems. The visual representation provides immediate view of the health of the organization's network of endpoints. The entire dashboard is clickable to provide easy drill downs into various points of interest.

In-place remediation

Sentient provides the option to integrate with endpoint management tools (e.g. Radia Endpoint Manager) to do in-place remediation of endpoints: kill rogue processes, delete files, install patches and apply updates in minutes.

Fast querying and action for maximum reliability

The queries are run in real-time, and are quick for administrators to be nimble and responsive to changing endpoint dynamics. For example, administrators can apply the latest patch on non-compliant endpoints and quickly check the updated status to ensure that all endpoints are compliant and secure.

Scalability and reliability that is tested for hundreds of thousands of endpoints

Sentient has been scale-tested with hundreds of thousands endpoints. The design of Sentient along with small footprint, and low bandwidth usage ensures that it can respond to critical administrator queries in a matter of seconds - not hours and days.

Sentient Benefits

- ✓ Mitigates risks considerably with real-time and instant check on status and health of endpoints across the corporate network
- ✓ Reduces security incidents caused due to vulnerable endpoints running older patches, rogue software, processes, etc.
- ✓ Provides better control and improves decision-making based on precise and real-time information with deep endpoint insights
- ✓ Provides real-time and dynamic graphs to view endpoint status, and act on them quickly
- ✓ Significantly reduces operational costs with proactive and targeted endpoint management

About Accelerite

Accelerite delivers secure business-critical infrastructure software for Fortune 500s, telecom operators and SMEs around the globe. Accelerite's product suite includes solutions for cloud life cycle management, endpoint security, enterprise mobility management, and the Internet of Things. Headquartered in Santa Clara, California, Accelerite serves as the products business of Persistent Systems (BSE & NSE: PERSISTENT), a global leader in software product development and technology services. For more information, visit www.accelerite.com.