ziften SOLUTION

SOLUTION BRIEF

Unparalleled Endpoint Visibility

Ziften Zenith's unparalleled endpoint visibility simplifies improving endpoint hygiene, threat prevention and detection, and threat response and look-back investigations.

Yes. We mean "unparalleled endpoint visibility". Your endpoints are where the action is, and where your users and corporate applications live. And those endpoints are exactly where the vast majority of your security operations and even IT operations use cases come into play. So, let's take a closer look at why endpoint visibility is so important.

Continuous, Not Point-in-Time Visibility

Ziften Zenith provides continuously streamed visibility into endpoint activity. The other guys give you point-in-time snapshots.

Point-in-time queries are sometimes useful, like the following tasks:

- Asset Posture Query, e.g., "Tell me how many Windows 10 machines aren't up to date from a patch perspective."
- Asset Update Command, e.g., "When any endpoint of this profile type joins my network, update App 1.2.3 to Release x.y.z."

But continuous endpoint visibility is critical when tasks like the following come up:

- Asset Inventory Monitoring, e.g., "What assets have connected to the network over the past 6 months for any period?"
- Malware Infection / Potential Data Loss e.g., "Mary Jane's machine has been hit by a keystroke logger. How long has it been resident and is there any evidence of data exfiltration or other machines with the same issue?"

Continuous endpoint visibility is a requirement in modern endpoint protection.

Immediately Available Endpoint Data

But what about then the endpoints are turned off at night or aren't connected to the corporate network. Because all endpoint data collection is captured at the endpoint by the Ziften agent and sent to Ziften's next generation cloud storage environment, endpoint visibility is always up-to-date, and immediately and continuously available to security and IT operations teams.

Further, Zenith's rich data collection includes visibility of systems, user behavior, network connectivity, application, binary, and process data allowing thorough threat detections and prevention, plus thorough endpoint IT hygiene.

Get the visibility you need immediately when you need it.

6 Months of Historical Data

And see more than real-time endpoint data – look into the past. Understand how things happened, when they happened, and how to respond to and fix the root cause issue.

Zenith retains 6 months of data storage at a minimum. This historical endpoint visibility simplifies in-depth security forensics, identification of systems exhibiting similar threat behaviors, lateral threat tracking, and breach root cause identification and remediation.

The Ziften Zenith difference is clear.

ziften