Integrated to Add More Value

Extend the Value of Incumbent Tools

IT and Security Operations involve broad and deep responsibilities. You’ve made multiple system investments over time – systems responsible for long-term data collection, endpoint/network integrated analytics, SIEM compliance use cases, ticket resolution, workflow orchestration, forensics analysis, incident response and more. Endpoint management is vital – but it is not an island. It must fit into your overall IT and Security Operations infrastructure.

Siloed solutions pose significant limitations to the need for operations integration. And point-in-time oriented systems are a poster child for the silo approach. The data captured by point-in-time solutions will require significant effort to match and integrate with existing data analytics, systems management, and security tools.

Ziften’s real-time and historical visibility database is easily integrated with existing tool ecosystems. With Ziften, endpoint visibility and control is 100% fulfilled, but also in a manner that extends the value of existing solutions.

- Integrate with external scanning vulnerability assessment tools
- Augment existing patch management solutions and processes
- Add additional foreground and background software usage stats to license management tools
- Add endpoint visibility, context and attribution to SIEM and other data analytics
- Supply rich user and systems behavioral data to external user and entity behavior analysis solutions
- Make greater use of and get more value from existing malware analysis and sandboxing solutions
- Get additional value from existing global threat intelligence subscriptions
- Integrate with existing SIEM, ticketing, and orchestration tools

That’s the Ziften difference.

Typical Ziften Integrations