# Testimonial on PolyLogyx ESP by Leading MSSP

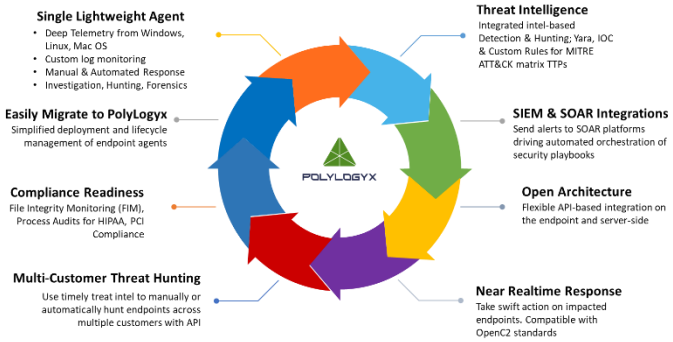
*"GuardSight evaluated PolyLogyx ESP with a target in mind for our small and medium business customer deployments. Their architecture makes it particularly suitable for MSSPs focused on endpoint monitoring and response services who need flexibility from the platform"* ***- John McGloughlin, Founder & CEO, GuardSight.***

Recently the PolyLogyx ESP endpoint security platform was put to test by one of our partners, GuardSight, a leading MSSP based in western United States, one that has, for over a decade, provided cybersecurity operations, assessments, response and consulting services. Their testing was focused on endpoint visibility and control features and use cases as listed in their report:

- Granularity of telemetry
- Multiple detection methods
- Multi-platform support
- [On demand] Query functionality
- Host isolation
- API Integration
- Extensibility – Custom rules, IOCs, Threat Intel
- Easy deployment
- Asset management
- File manipulation
- Compliance configuration
- Filtering
- YARA engine on endpoint
- Log forwarding

**Assessment Highlights:**
PolyLogyx Endpoint Visibility and Control Platform is a highly extensible platform that offers key features not found in other endpoint platforms, such as live querying, custom query building, and scheduling. Its economic model suits the needs of an MSSP that caters to small and medium size businesses.

The State-of-the-Art Endpoint Platform




**API:**
PolyLogyx REST API allows developers to use a programming language of their choice to integrate with the headless PolyLogyx server. The REST APIs provide the means to configure and query the data from the fleet manager [in real-time]. The APIs also allow an openc2 orchestrator to get visibility into endpoint data and activities, which can then be used to craft an [automated or manual] openc2 response action. All payloads are exchanged over REST and use the JSON schema.

**Log Forwarding**
Another feature of PolyLogyx EDR is their log forwarding. Rsyslog, Syslog-NG and logstash logs can be forwarded if needed. For GuardSight, this is a great feature as the logs can be forwarded to AlienVault.

**Bottomline Conclusion**: *"PolyLogyx ESP (Endpoint Visibility and Control Platform) meets, and in some cases exceeds, the basic functionality of an EDR required by GuardSight."*