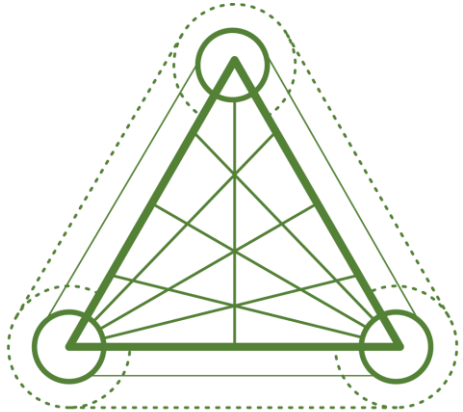


POLYLOGYX

TRANSFORMING CYBER SECURITY

The PolyLogyx VASP Agent

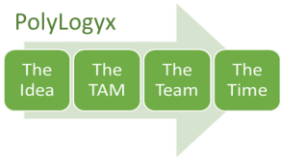
January 2018

For Sharing Within OpenC2 Member Organizations

Contact: atul@polylogyx.com or sridhar@polylogyx.com

Please note: PolyLogyx is in Stealth mode

<u>PolyLogyx Belief:</u> We can only provide sustained protection to enterprises with a paradigm shift in the application of technologies – towards universal integration and democratization of the market to promote large scale rapid innovation. "Security by a thousand silos" is putting businesses at risk. It is time we changed how security is built, sold, deployed and managed.



Endpoint Security: The Paradigm Problem

Problem statement: Enterprises continue to be breached despite spending* $80B+ on security and $10B on endpoint security this year. Customers complain about cracks in their security due to:

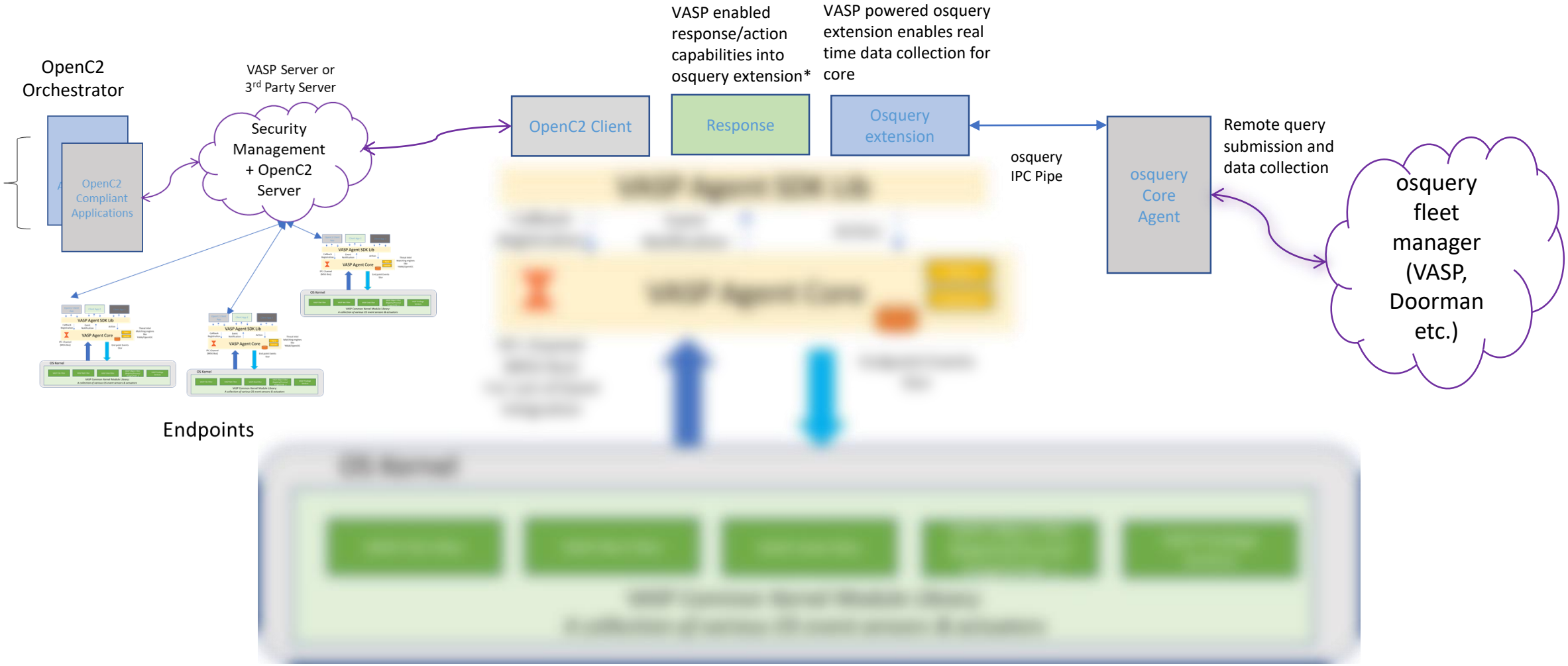
- Alert fatigue (e.g. Target, Equifax)
- Inflexible architecture -> (TCO, replacement costs, innovation)
- Agent congestion (a common enterprise compliant)
- Vulnerability gap (a result of the market paradigm)

**IDC Worldwide SemiAnnual Security Spending Guide March 2017*

PolyLogyx VASP Agent – A new paradigm

- Single agent infrastructure with plug-in APIs across vendor technologies
- Notification APIs for OS events and event context
  - Multiple consumers can subscribe for events
  - No need to write separate drivers for similar events
  - No need to determine the context (PID, FileHash, Cert reputation etc) multiple times
  - No need for multiple application hooking
- APIs to take response actions
  - Deep Actions based on proxying thru kernel API
- APIs to query historical events (and context)
- Security management interfaces consistent across vendors

PolyLogyx VASP Agent v1.0
*Integration with osquery illustrated**



**Parts of this diagram are blurred for confidentiality*

PolyLogyx VASP Agent – SDK APIs

API Types

- Event Notification Subscription APIs (Callbacks)
  - File system events
  - Network events
  - Hardware events
  - Raw disk events
  - External device (e.g USB) events
  - Process creation/termination events
  - Image load events
- Deep Action APIs
  - Write File
  - Process Terminate
  - Network isolation
- Privilege and Forensic APIs
  - Read physical/virtual memory
  - Read raw disk
  - Read IO ports
- Event Stor APIs
  - Query Events Based on PID
  - Query Events Based on time stamp
  - Query Event Extended data
- Code injection and API hooking APIs
- Command and Control APIs
  - Load/Unload app
  - Register
  - Configure policies
  - Upgrade agent
- Infrastructure APIs
  - Log Message
- Support for industry protocols
  - OpenC2
  - YARA/PCRE/OpenIOC engines

Integration Choices

- In-Stack Integration
  - Part of the same process – Binary linkage
  - Synchronous as well as asynchronous notifications and actions
  - Managed by VASP Console
  - C-style APIs
  - Each app ends up being a DLL loaded by the VASP Agent Core
- Out-of-Stack Integration
  - Different process, no binary linkage with VASP Agent
  - IPC channel linkage
  - Asynchronous only (Message Bus architecture)
  - Command followed by Data
  - Client app can maintain their binary form factor
  - Independent management control
- **Common security tech integration**
  - AV update status, update command
  - Integration with Virus Total, 3rd party Intel
  - Orchestration platforms
  - Alert (SIEM) and workflow automation

VASP: A Rich Set of OpenC2-compliant Actions

OpenC2 Action	Target (Note: Multiple targets possible)	Actuator	VASP Support
Scan	Disk, disk partition, file, process, memory,	Endpoint	Yes
Locate	File	Endpoint	Yes
Query	Artifact	Endpoint	Yes
Notify	User account	Endpoint	Yes
Deny	Process, User account	Endpoint	Yes
Contain	File/process	Endpoint	Yes
Allow	File/Process	Endpoint	Yes
Start	Process	Endpoint	Yes
Stop	Process, system	Endpoint	Yes
Restart	Process	Endpoint	Yes
Pause/Resume	Process	Endpoint	Yes
Set/Update	File/Process/User account/Registry	Endpoint	Yes
Move/Delete/Save/Substitute	File/Directory	Endpoint	Yes
Investigate/Remediate	File/Process/x509 Cert	Endpoint	Yes

VASP SDK – Potential use cases*

Security Operations Workflow
- Alert automation
- SIEM integration
- Response automation
- Consistent Dashboard (reduced training)

Anti-Malware (Static/Behavioral/Next Gen like ML)
- Ability to monitor system events in real time
- Ability to corelate events
- Ability to take remedial actions
- Root kit/Boot kit detection

EDR/IR
- Ability to hunt for threat indicators
- Ability to match various intel types
- Ability to generate context

Intrusion Detection
- Monitor crucial APIs in target process
- Monitor memory patterns for exploits (Heap Spray, ROP gadget, Shell code..)
- Monitor script parameters (File less intrusion)

Host Firewall
- Network packet inspection
- Port level filtering

End point monitoring and compliance
- File Integrity Monitoring (FIM)

Anti-Ransomware
- Ability to monitor IO behavior
- Ability to trap FS IOs and create virtual FS (e.g. COW, ShieldFS)

**Next level detail that may help with the OpenC2 language development will be supplied later*

Thank you!