mongoose™ in a nutshell

Mongoose tackles endpoint traffic monitoring for the enterprise, enabling detection and mitigation of threats in concert with perimeter-based intrusion detection systems and big data analytics.

Mongoose is a tiny kernel agent residing on host endpoints (laptops, workstations, servers, VMs) that monitors ALL inbound and outbound traffic. Captured data is uploaded to the cloud for real-time and forensic analysis and threat response.

Why mongoose for endpoint monitoring?

- Monitored hosts are located anywhere (including servers/VMs in the cloud)
- Unique content - simple flow to full payload, host process, IP and domain
- Remote command and control for real-time threat response
- Automatic and remote IP and domain blocking
- Scalable deployment, data processing, big data analytics
- Extensible to multiple telemetries
- Adjacent technology that complements IPS/IDS platforms → full product solution

Key benefits

- Unrestricted traffic surveillance within and beyond the corporate campus
- Targeted telemetry greatly shortens the time to threat identification/mitigation
- Real-time remote interdiction supporting quarantine and forensics
- No new interface to manage - integrates with existing traffic collection/analysis platforms
- Extends reach of in-network IPS/IDS platforms and magnifies their selling proposition
- Patented technology. Flexible licensing, customization and branding opportunities

closing the circle of surveillance