Comparing Guardicore with Illumio

GUARDICORE STRENGTHS

- Process-level visibility and enforcement across OSs
- More flexible and more automated labeling approach
- Integrated breach detection and response

ILLUMIO STRENGTHS

- Ability to encrypt traffic between workloads
- Named a leader by Forrester in Zero Trust Wave report

	Guardicore	illumio
Visibility Depth and Breadth		
Agent-based activity discovery	✓	✓
Agentless activity discovery	✓	✗
Real-time and historical visualization of all communication[1]	✓	–
Granular, live view of app components and communications	✓	✓
Automatic application dependency map generation	✓	✗
Visibility insights to aid policy development	✓	✓
Built-in tag synchronization with orchestration tools	✓	✗
Comprehensive list of filter options	✓	✗
Micro-Segmentation Granularity		
Basic segmentation (geo, environment, zone)	✓	✓
Micro-segmentation (application by port, application tier, workload)	✓	✓
Process-level segmentation for dynamic port applications[2]	✓	–
Segmentation at the container level	✓	✓
Prevents and contains unauthorized devices on the network	✓	✓
Environment / OS Support		
Support for legacy OSs (e.g. Win2003, CentOS 6, RHEL5)	✓	✗
Support for systems where agents cannot be deployed	✓	✗
Support for Windows XP, 7, 10[3]	✓	–

1 Historical views in Illumination v20.1 are limited to 60 days. Explorer provides historical views in earlier versions.
2 Illumio ASP provides process-level visibility and enforcement only on Microsoft Windows-based workloads.
3 Illumio supports Windows 7 and 10 in limited configurations; only recommended for VDI with wired I/F.

Guardicore

Comparing Guardicore with Illumio

Policy Creation and Enforcement

	Guardicore	illumio
Consistent policy across Windows and Linux systems	✓	✗
Whitelist "zero trust" policy model	✓	✓
Blacklist security model	✓	✗
Hybrid security model	✓	✗
Automatic policy generation	✓	✓
Build and test policies before enforcement	✓	✓
Policy template library (e.g., Domain Controller, SharePoint, etc.)	✓	✓
Enforcement not dependant on the OS firewall	✓	✗
New workloads automatically inherit policy[4]	✓	–
Incorporates user identity in the security policy	✓	✓
Role-based views w/policy scoped to application/location	✓	✓

Breach Detection and Response

Built-in reputation analysis for files, IP addresses, domains, and DNS	✓	✗
Deception	✓	✗
Lateral movement detection	✓	✗
Incident response integration	✓	✗
Built-in threat intelligence firewall	✓	✗
Asset security history	✓	✓

[4] *To inherit policy on new workloads using Illumio ASP, labels must be defined as part of the agent installation.*

Guardicore