illumio

Compare **Cisco Tetration Analytics** to **Illumio ASP**

Illumio Adaptive Security Platform® delivers live visibility and adaptive segmentation that works on anything (virtual machines, bare-metal, and containers), anywhere (data center, private or public cloud) by activating and centrally managing the native security controls in the workload. Illumio does this for the world's largest, most demanding computing environments with no dependency on the network or hypervisor.

CAPABILITIES

SYSTEMS	CISCO TETRATION ANALYTICS	ILLUMIO ASP
Primary Use Case	**Analytics**	**Micro-Segmentation**
VISIBILITY		
Live visibility into application components, communications, and dependencies across any data center and cloud via application dependency map	✔	✔
Visibility aids the development and monitoring of micro-segmentation policy	✔	✔
Visualizes over 2,000 concurrent workloads in an application dependency map	✖	✔
Comprehensive vulnerability map to understand risk, exposure, and potential attack paths in real time	✖	✔
Combines vulnerabilities, flow data, and security policy to calculate various risk scores	✔	✔
Role-based views (e.g., by application owner, location)	✔	✔
Network performance monitoring	✔	✖
Retains historical flow data for compliance reporting	✔	✔
SEGMENTATION		
Macro-segmentation (geo, environment, zone)	✔	✔
Micro-segmentation (application, application tier, workload, port/protocol, container)	✔	✔
Activates native enforcement point in critical modern operating systems (Windows, Linux)	✔	✔
Activates native enforcement point in critical legacy operating systems (Solaris, AIX)	✖	✔
Process-based segmentation for dynamic port applications (e.g., Domain Controller)	✖	✔
Encrypts data in transit between workloads	✖	✔
Ability to enforce identity-based (certificate) authentication for "zero trust" communication	✖	✔
Automatic policy generation tool recommends security policies based on vulnerability data to limit or block vulnerabilities	✖	✔
SECURITY POLICY MODEL		
Strict whitelist "zero trust" policy model with no complexity of rule order management	✖	✔
Leverages learned application communication to automatically generate security policies	✔	✔
Automatic policy generation tool provides recommended policies in just seconds	✖ (takes 2 min - 12 hours)	✔
Build and test policies before enforcement	✔	✔
Policy template library (e.g., Domain Controller, Sharepoint, etc.)	✖	✔
Any new workload from anywhere automatically inherit policy	✖	✔
Incorporates user identity in the security policy	✖	✔
Integrates with third-party vulnerability data for vulnerability-based security policy	✔	✔
SCALE & AVAILABILITY		
Scales to 5,000 workloads (servers required for redundant policy controller)	✔ (6 servers)	✔ (4 servers)
Scales to 10,000 workloads (servers required for redundant policy controller)	✔ (36 servers)	✔ (4 servers)
Scales to 25,000 workloads (servers required for redundant policy controller)	✔ (36 servers)	✔ (6 servers)
Supports multiple policy controllers for high availability and scale (100K+ workloads)	✖	✔

M02012019