Illumio Workload, Service, and Traffic Report

Workload Summary

⚠ This section provides an overview of workloads in the environment.

Operating System	Count
centos-x86_64-7.0	134
win-x86_64-server	15
win-x86_64-client	10
ubuntu-x86_64-xenial	9
macOS-universal-catalina	5
	3
centos-x86_64-8.0	3
macos-universal-catalina	1

Status	Count
True	196

Top 10 Hostnames

⚠ This list represents the most frequently occurring hostnames in your environment.

hostname	Count
	3
claude-mcp-prod-01	2
ast-web03-prd	1
cat-web02-prd	1
ecm-web01-prd	1
ecm-proc01-prd	1
ecm-proc02-prd	1

hostname	Count
ecm-db02-prd	1
ecm-db01-prd	1
cat-web01-prd	1

Service Summary

⚠️ This section provides an overview of services and open ports across all workloads.

port	Count
22/6	152
68/17	146
5666/6	143
52311/6	143
111/6	143
111/17	143
443/6	48
8070/6	45
123/17	25
4500/17	25

Protocol	Count
6	1204
17	633

Open Ports Summary

This chart shows the distribution of the top 20 open ports across all workloads, sorted by the number of machines with each port open. Ports are represented as 'port_number/protocol', followed by the count and percentage of machines with this port open.
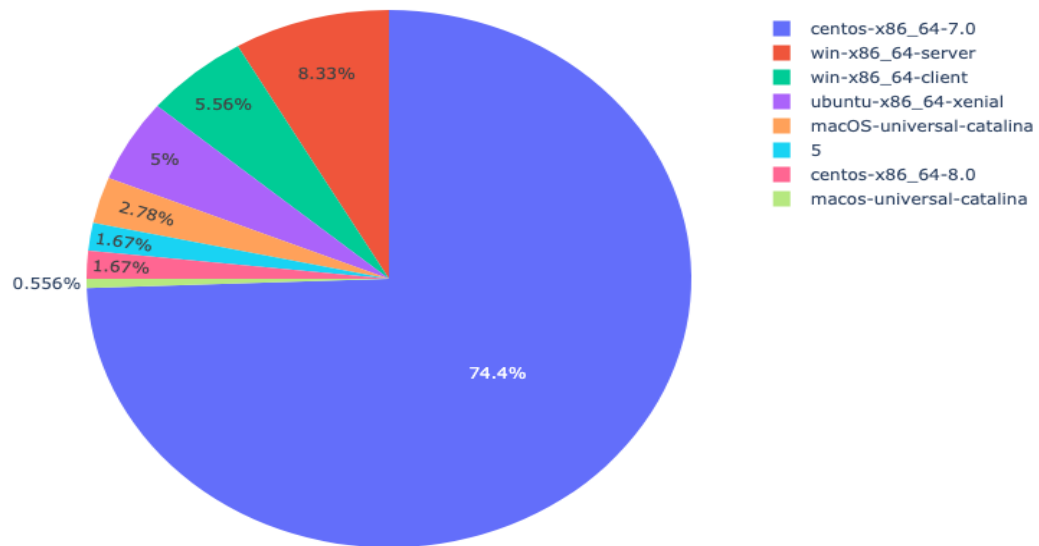
Top 20 Open Ports
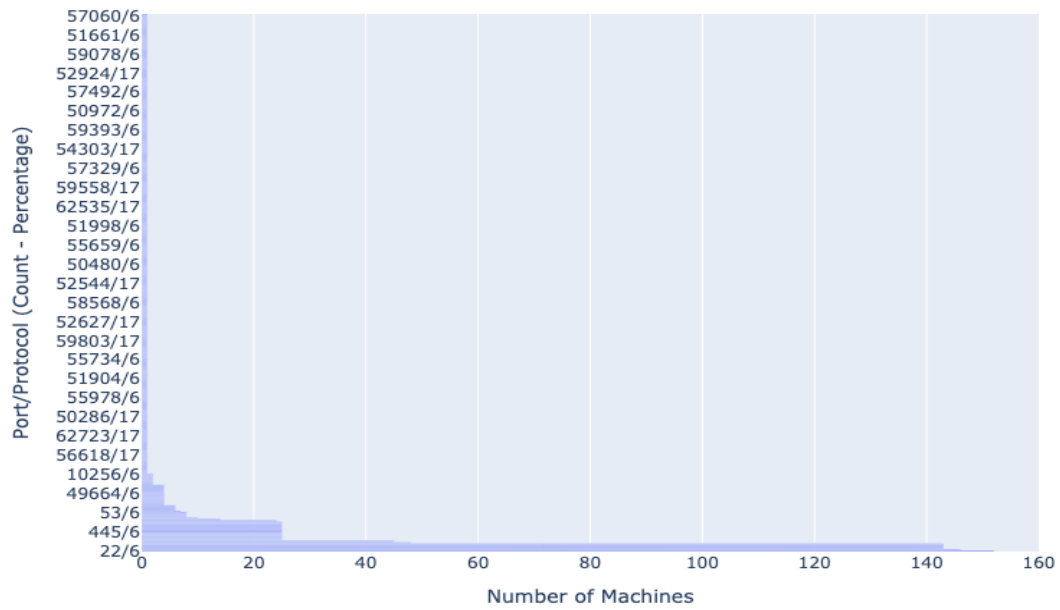
OS Distribution

This chart shows the distribution of operating systems across all workloads.

OS Distribution

Legend:
- centos-x86_64-7.0
- win-x86_64-server
- win-x86_64-client
- ubuntu-x86_64-xenial
- macOS-universal-catalina
- 5
- centos-x86_64-8.0
- macos-universal-catalina

Slice labels: 8.33%, 5.56%, 5%, 2.78%, 1.67%, 1.67%, 0.556%, 74.4%

Workload Enforcement Mode Distribution

This chart shows the distribution of enforcement modes across all workloads.

Workload Enforcement Mode Distribution
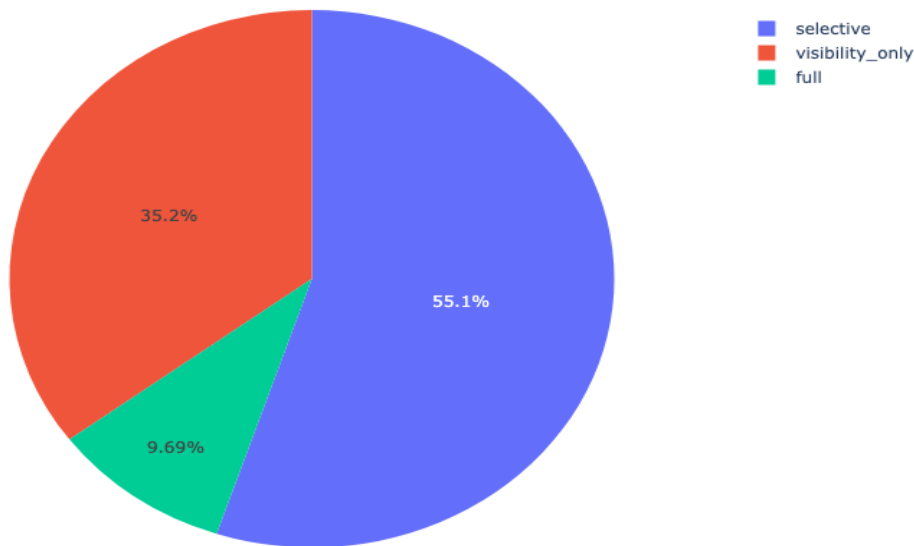
Enforcement Mode Summary

This table provides a summary of workload enforcement modes.

Enforcement Mode	Count
selective	108
visibility_only	69
full	19

Traffic Graph

This graph visualizes the network connections, potential issues, and recommendations.

AI Advisor Output

This section provides AI-generated security and microsegmentation recommendations based on the analyzed data.

1. Potential Security Risks

- **Wide Open Ports**: Several critical ports, such as 22 (SSH), 443 (HTTPS), 3389 (RDP), and others, are broadly open across the network. These ports are common targets for attackers.
- **Insecure Protocols**: Ports like 21 (FTP) and 135 (RPC) are known for security vulnerabilities. Their usage suggests the presence of insecure protocols which can be exploited.
- **Operating System Diversity**: The mix of operating systems (CentOS, Windows Server and Client, Ubuntu, macOS) increases the complexity of patch management and security configurations.
- **Outdated Operating Systems**: The presence of CentOS 7.0, which may be nearing the end of its support lifecycle, could pose risks due to unpatched vulnerabilities.
- **Inconsistent Enforcement Modes**: The distribution of enforcement modes (selective, visibility_only, full) indicates a lack of a unified security posture, leading to potential gaps in defense.

2. Microsegmentation Recommendations

- **Define Security Zones**: Segment the network based on the criticality and function of workloads, such as separating production from development and external-facing services from internal ones.
- **Implement Least Privilege Access**: Ensure that each segment only has access to the network resources it absolutely requires, minimizing lateral movement opportunities for attackers.
- **Apply Consistent Policies**: Develop a baseline security policy for each segment and apply it consistently, including firewall rules, intrusion detection/prevention, and malware protection.
- **Automate Policy Enforcement**: Use automated tools to apply and update policies to respond quickly to new threats and reduce the risk of human error.

3. Best Practices for Improving Overall Network Security

- **Regular Patch Management**: Implement a robust patch management process to ensure all systems are up-to-date with the latest security patches.
- **Secure Configuration**: Harden the configuration of all devices and services, disable unnecessary services, and use secure protocols (e.g., SSH instead of Telnet, HTTPS instead of HTTP).
- **Endpoint Protection**: Deploy endpoint protection solutions that include antivirus, antispyware, and host-based intrusion prevention on all endpoints.
- **Security Awareness Training**: Conduct regular security awareness training for all employees to recognize phishing attempts and other social engineering tactics.
- **Incident Response Plan**: Develop and regularly test an incident response plan to ensure readiness in the event of a security breach.

4. Recommendations for Optimizing Enforcement Modes

- **Visibility Only to Selective**: For workloads currently in "visibility_only" mode, analyze traffic and logs to identify legitimate traffic patterns. Gradually move these to "selective" mode while ensuring legitimate traffic is not disrupted.
- **Selective to Full**: For critical workloads in "selective" mode, consider moving them to "full" enforcement after ensuring that all necessary communications are allowed. This maximizes protection.

- **Continuous Monitoring**: Regardless of the mode, maintain continuous monitoring and logging to detect and respond to anomalies promptly.

5. Recommendations for Traffic Analysis and Security

- **Network Traffic Analysis**: Regularly analyze network traffic patterns to identify anomalies, unauthorized data exfiltration, or signs of compromise.
- **Security Information and Event Management (SIEM)**: Implement SIEM solutions for real-time analysis and alerts on security incidents.
- **Decryption and Inspection of Encrypted Traffic**: Where legal and practical, decrypt and inspect encrypted traffic for malware and unauthorized data leakage.
- **Regular Penetration Testing**: Conduct regular penetration testing to identify and fix vulnerabilities before they can be exploited by attackers.
- **Compliance Audits**: Regularly perform compliance audits to ensure that security policies are followed and effective in mitigating risks.

Traffic Summary

This section provides an overview of network traffic in the environment.

src_ip	Count
fe80::250:56ff:fe8b:f154	688
10.0.1.34	263
172.31.3.151	178
172.31.3.38	162
10.0.1.2	147
10.0.1.7	124
10.0.1.140	72
10.0.1.134	72
10.0.1.136	72
10.0.1.139	72

dst_ip	Count
fe80::250:56ff:fe8b:1d1	679
10.0.1.3	187
10.0.1.5	179
10.0.1.22	178

dst_ip	Count
10.0.1.32	172
10.0.1.133	172
10.0.1.130	166
10.0.2.132	48
10.0.2.72	42
10.0.2.66	37

port	connections
8070	15933449
123	13272261
5432	13000576
443	12636571
5666	12387985
3306	11139919
514	9089503
3389	7301934
22	5090867
445	4171128
389	3997417
135	3989479
88	3799532
8080	2815081
49668	2766465
49677	2414992
49674	2267712
104	1829818
50636	1036052
2762	736047

protocol	connections
6	128306408
17	6359211
58	9

Top 20 Ports

Protocol Distribution