

Risk analysis 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	8
macOS-universal-catalina	5
centos-x86_64-8.0	3
	2
macos-universal-catalina	1

Status	Count
True	185

Top 10 Hostnames



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

hostname	Count
	2
cat-proc01-prd	1
pos-web03-pci	1
pos-db03-stg	1
cat-web02-prd	1
swf-web03-prd	1
pos-db01-stg	1

hostname	Count
pos-proc06-stg	1
pos-proc05-stg	1
win-endpoint-7	1

Service Summary



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

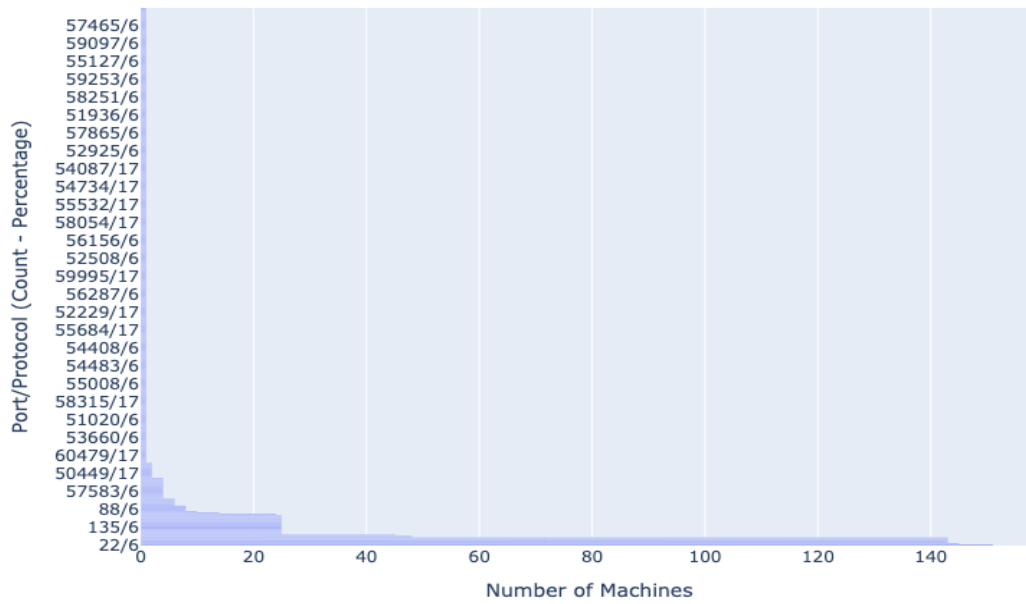
port	Count
22/6	151
68/17	145
5666/6	143
52311/6	143
111/6	143
111/17	143
443/6	48
8070/6	45
500/17	25
52311/17	25

Protocol	Count
6	1202
17	631

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.

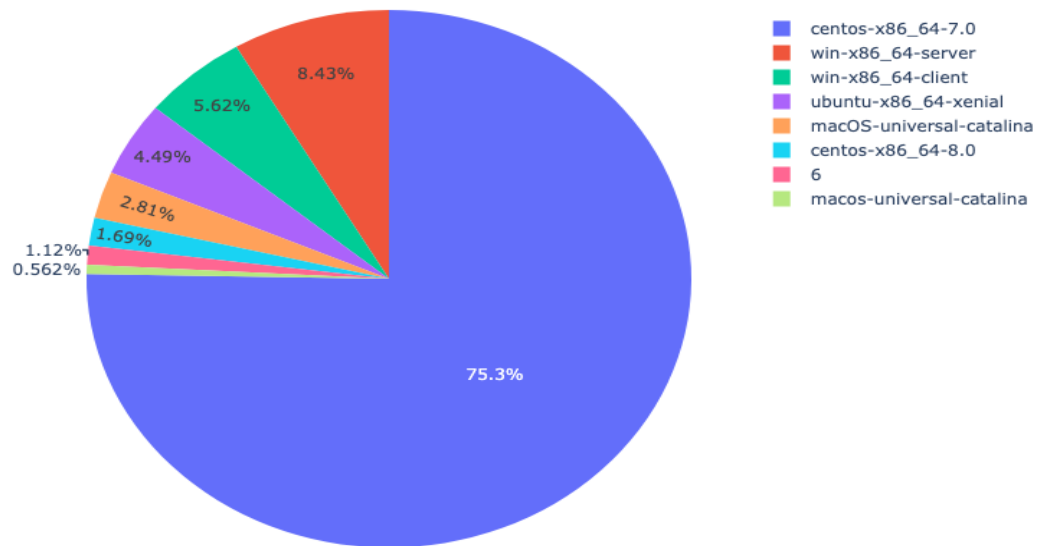
Top 20 Open Ports



OS Distribution

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

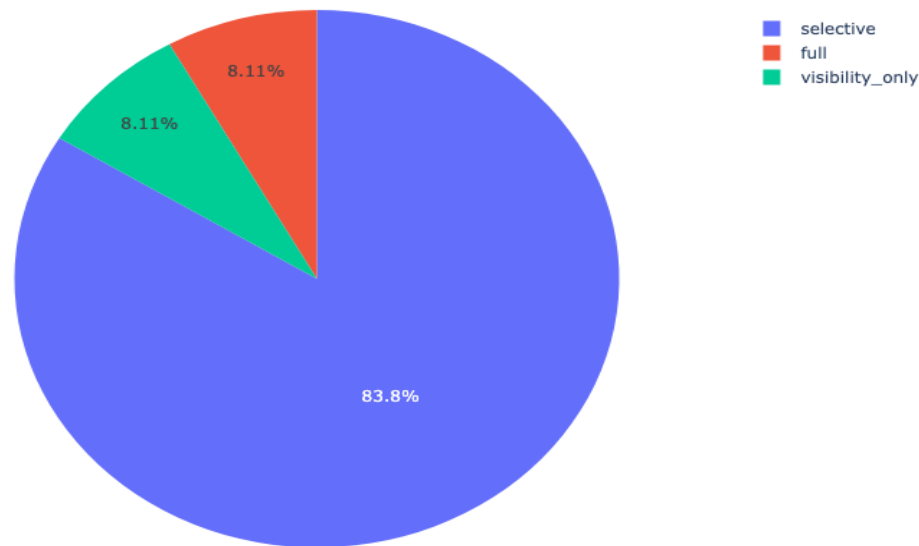
OS Distribution



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.

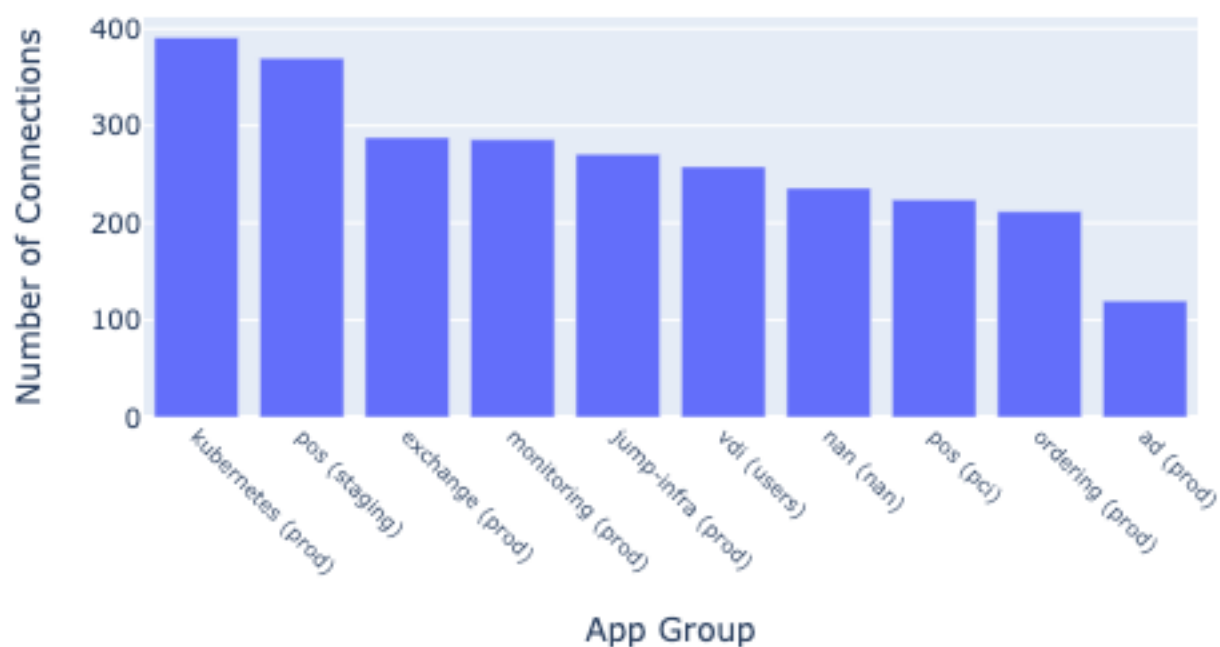
Enforcement Mode	Count
selective	155
full	15
visibility_only	15

Traffic Summary

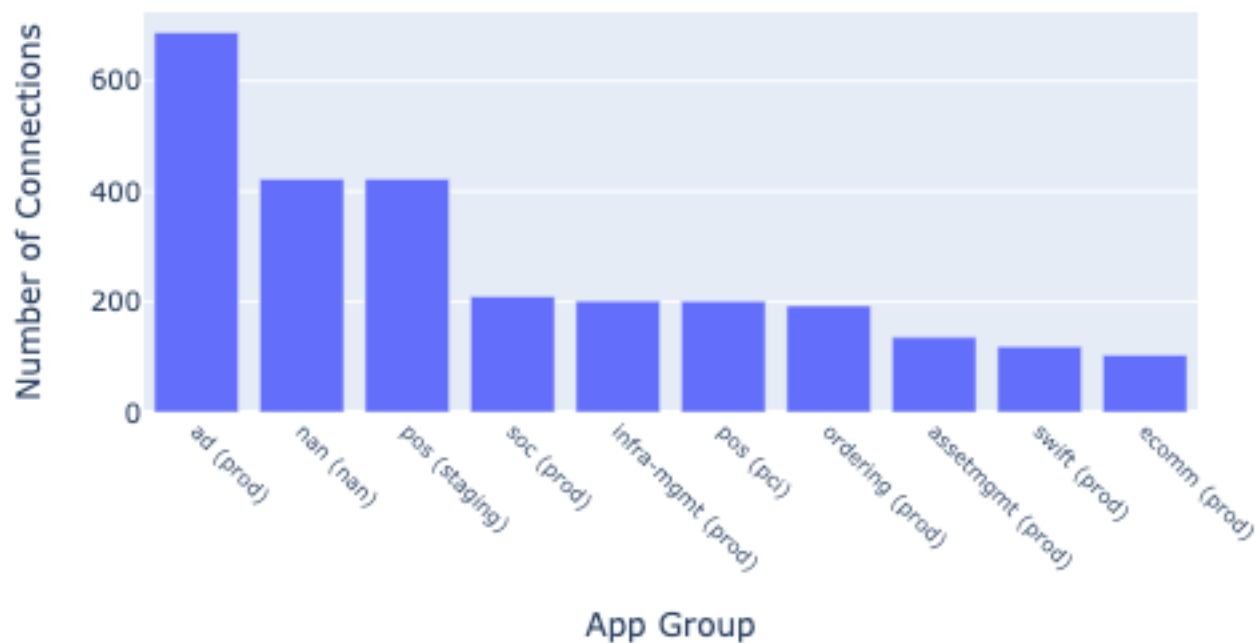
 This section provides an overview of network traffic in the environment, highlighting the top 10 source and destination app groups.

Top 10 Source App Groups: - kubernetes (prod): 391 connections - pos (staging): 370 connections - exchange (prod): 288 connections - monitoring (prod): 286 connections - jump-infra (prod): 271 connections - vdi (users): 258 connections - nan (nan): 236 connections - pos (pci): 224 connections - ordering (prod): 212 connections - ad (prod): 120 connections
Top 10 Destination App Groups: - ad (prod): 688 connections - nan (nan): 423 connections - pos (staging): 423 connections - soc (prod): 210 connections - infra-mgmt (prod): 202 connections - pos (pci): 201 connections - ordering (prod): 193 connections - assetmgmt (prod): 136 connections - swift (prod): 119 connections - ecomm (prod): 104 connections

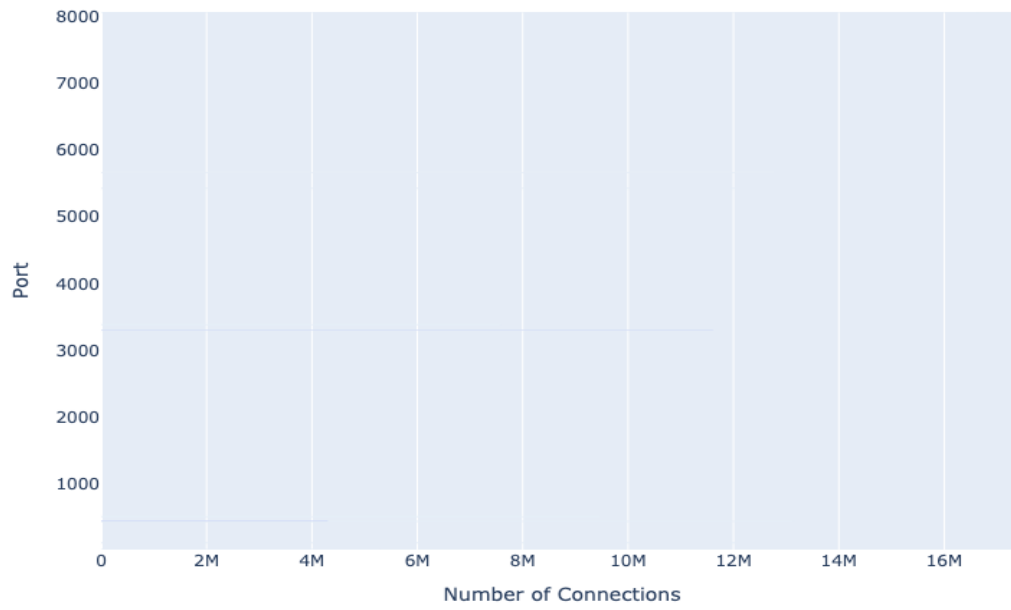
Top 10 Source App Groups



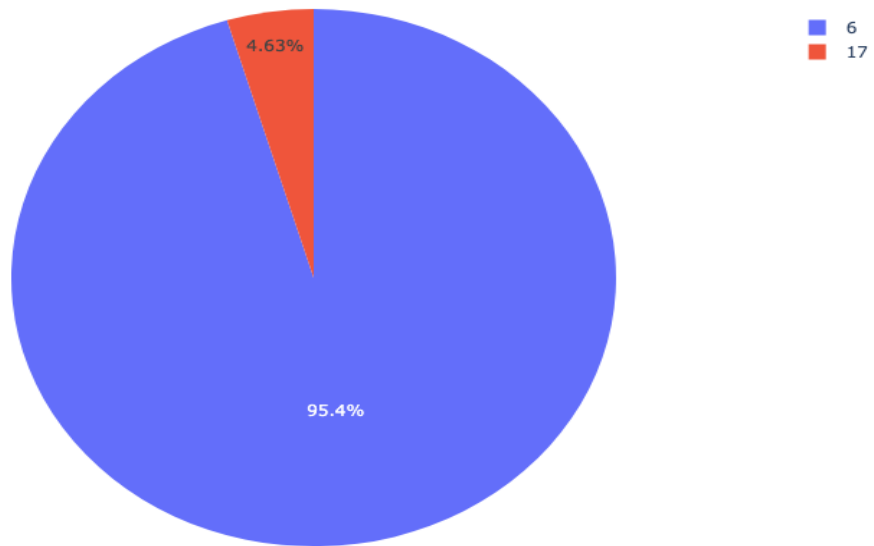
Top 10 Destination App Groups



Top 20 Ports



Protocol Distribution



Process Traffic Summary

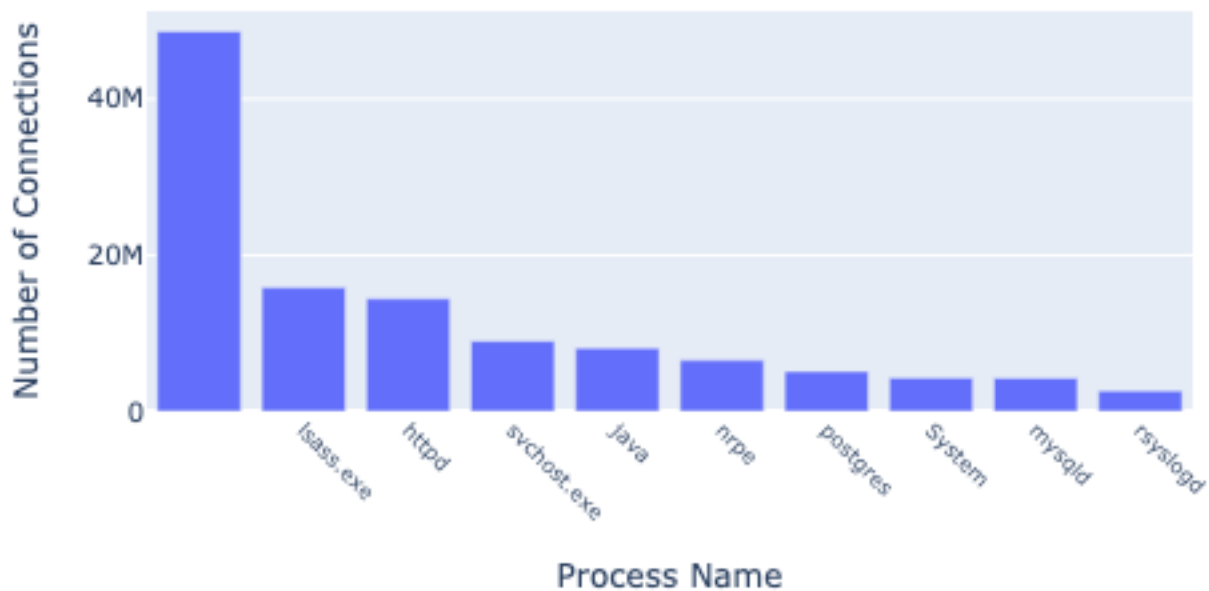


This section provides an overview of network traffic by process name.

Top 10 Processes by Traffic Volume

- : 48674030 connections
- **lsass.exe**: 15849475 connections
- **httpd**: 14432340 connections
- **svchost.exe**: 8996473 connections
- **java**: 8094248 connections
- **nrpe**: 6539188 connections
- **postgres**: 5112670 connections
- **System**: 4294572 connections
- **mysqld**: 4258368 connections
- **rsyslogd**: 2610630 connections

Top 10 Processes by Traffic Volume



AI-Generated Traffic Analysis



This section provides AI-generated analysis and recommendations based on the network traffic data.

Here's an analysis of the provided traffic information with security recommendations, potential issues, insights, and suggestions:

1. Security Recommendations

This section provides key security recommendations based on the observed traffic patterns to enhance the overall security posture of the network.

- **Implement Strict Firewall Rules:**

- Restrict traffic between production and non-production environments (e.g., staging to prod)
- Limit access to sensitive services (e.g., AD, Exchange) from user environments
- Implement application-specific firewall rules to minimize unnecessary connections

- **Enhance Monitoring and Logging:**

- Ensure all critical systems are sending logs to the SOC (port 514)
- Implement additional monitoring for high-volume connections
- Set up alerts for unusual traffic patterns or volumes

- **Secure Remote Access:**

- Implement multi-factor authentication for all remote access (e.g., VDI, jump servers)
- Use VPN for remote connections instead of direct access to production systems
- Regularly audit and review remote access logs
- **Strengthen Authentication Mechanisms:**
 - Implement Kerberos or other strong authentication for AD-related traffic
 - Use certificate-based authentication where possible, especially for inter-service communication
- **Encrypt Sensitive Traffic:**
 - Ensure all database connections (e.g., MySQL on port 3306) use encryption
 - Implement TLS for all HTTP traffic (port 80 to 443)

2. Potential Issues and Anomalies

This section highlights unusual or potentially problematic traffic patterns that warrant further investigation.

- **Cross-Environment Communication:**
 - High volume of traffic from staging to production environments (e.g., pos (staging) to soc (prod))
 - Direct communication between development and production (e.g., ordering (dev) to ordering (prod))
- **Unusual Port Usage:**
 - High volume of connections on non-standard ports (e.g., 49674, 49668) between Exchange and AD
 - Direct RDP access (port 3389) from user environments to production systems
- **Potential Security Risks:**
 - Direct SSH access (port 22) from user environments to production systems
 - High volume of connections from jump servers to multiple environments
- **Unexpected Traffic Patterns:**
 - Large number of connections from POS systems to infrastructure management
 - Direct access from VDI to sensitive systems like payment processing

3. Network Structure and Application Dependencies

This section provides insights into the network architecture and application relationships based on the observed traffic.

- **Centralized Logging:** SOC appears to be the central log collection point for multiple systems
- **Time Synchronization:** infra-mgmt likely hosts the primary NTP server for the network
- **Monitoring Infrastructure:** A dedicated monitoring system checks various services across environments
- **Database Dependencies:**
 - Shared database (shareddb) accessed by multiple applications
 - Mix of MySQL and PostgreSQL usage across different services
- **Active Directory Integration:** Heavy reliance on AD for authentication across multiple services
- **Remote Access:** Combination of VDI, jump servers, and direct connections for remote access

4. Improving Network Segmentation

Suggestions for enhancing network segmentation to improve security and reduce attack surface.

- **Implement Zero Trust Architecture:**
 - Treat all networks as untrusted, even internal ones
 - Require authentication and authorization for all access attempts
- **Create Distinct Security Zones:**
 - Separate PCI-compliant systems into a highly restricted zone
 - Isolate development and staging environments from production
- **Use Network Access Control Lists (NACLs):**
 - Implement strict NACLs between different application tiers
 - Control traffic flow between zones based on least privilege principle
- **Leverage Micro-segmentation:**
 - Implement granular policies at the workload level
 - Use software-defined networking to create dynamic security policies
- **Establish DMZs:**
 - Place public-facing services in a DMZ
 - Create separate DMZs for different types of external access (e.g., partner, customer)

5. Improving Cyber Hygiene

Recommendations for enhancing overall cyber hygiene based on observed and expected traffic patterns.

- **Centralize Time Synchronization:**
 - Ensure all systems use the identified NTP service (infra-mgmt)
 - Implement backup NTP servers for redundancy
- **Standardize Monitoring:**
 - Extend monitoring coverage to all critical systems and applications
 - Implement consistent monitoring ports and protocols across the environment
- **Implement Comprehensive Backup Strategy:**
 - Ensure backup systems have necessary access to all critical data sources
 - Implement network segmentation that allows backup traffic while maintaining security
- **Standardize Remote Access:**
 - Consolidate remote access methods (e.g., VDI, jump servers)
 - Implement consistent authentication and authorization for all remote access
- **Enhance Logging and SIEM Integration:**
 - Ensure all systems are sending logs to the centralized SOC

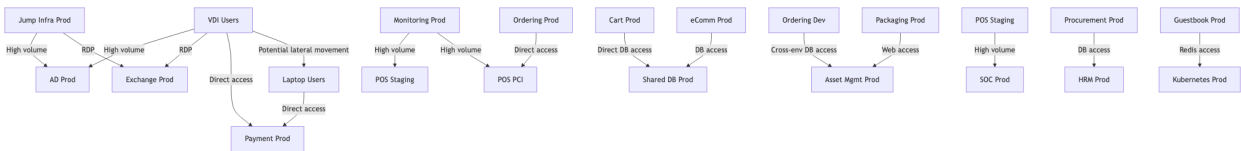
- Implement log forwarding for any systems not currently connected to SOC
- **Implement Patch Management:**
 - Ensure all systems have a clear path for receiving updates
 - Consider implementing a staged patching process across environments

By addressing these areas, the organization can significantly improve its security posture and operational efficiency.

ZTS Advisor findings



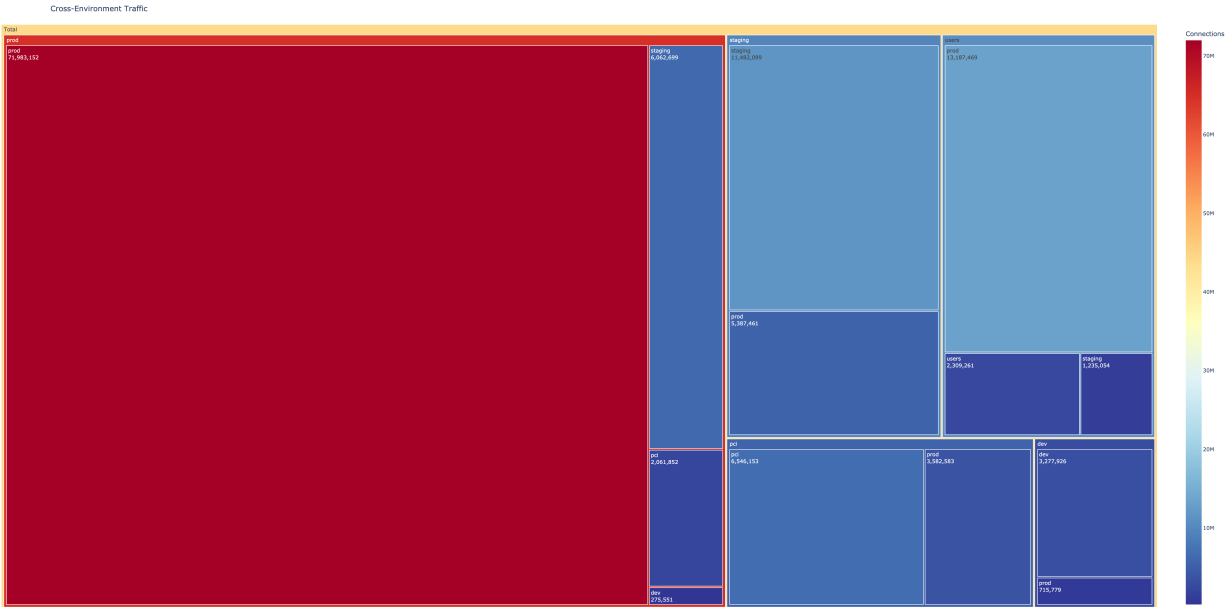
This graph visualizes the network connections, potential issues, and recommendations. The graph is generated using a large language model and using traffic information for augmentend generation.



Cross-Environment Traffic



Cross environment traffic can be an indicator of misconfiguration or malicious activity and should be monitored. Auditors and security teams should review this traffic to ensure that it is compliant and secure. The below treemap visualizes the traffic flow between different environments. The size and color of each box represent the number of connections between environments.



MITRE ATT&CK; Analysis



This section provides an analysis of potential tactics, techniques, and procedures (TTPs) based on the MITRE ATT&CK; framework, given the observed network traffic patterns.

MITRE ATT&CK; Analysis of Network Traffic

1. Identified ATT&CK; Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

2. Potential Techniques

Initial Access

- T1190: Exploit Public-Facing Application
- T1133: External Remote Services

Execution

- T1059: Command and Scripting Interpreter

Persistence

- T1098: Account Manipulation
- T1136: Create Account

Privilege Escalation

- T1078: Valid Accounts

Defense Evasion

- T1090: Proxy

Credential Access

- T1110: Brute Force
- T1003: OS Credential Dumping

Discovery

- T1046: Network Service Scanning
- T1018: Remote System Discovery

Lateral Movement

- T1021: Remote Services
- T1210: Exploitation of Remote Services

Collection

- T1005: Data from Local System
- T1039: Data from Network Shared Drive

Command and Control

- T1071: Application Layer Protocol
- T1043: Commonly Used Port

Exfiltration

- T1048: Exfiltration Over Alternative Protocol

3. Detection Strategies

T1190: Exploit Public-Facing Application

- Monitor for unusual traffic patterns to public-facing applications, especially from `vdi (users)` to `ecomm (prod)` on port 443.
- Implement web application firewalls and regularly review logs for potential exploitation attempts.

T1133: External Remote Services

- Monitor for unusual remote access patterns, particularly from `vdi (users)` and `laptop (users)` to various production environments.
- Implement multi-factor authentication and log all remote access attempts.

T1059: Command and Scripting Interpreter

- Monitor for unusual command execution patterns, especially on `jump-infra (prod)` to various production servers on port 22.
- Implement command logging and alerting for suspicious activities.

T1078: Valid Accounts

- Monitor for unusual account usage patterns, particularly between `vdi (users)` and production environments.
- Implement user behavior analytics to detect anomalous account activities.

T1021: Remote Services

- Monitor for unusual remote service usage, especially between different network segments (e.g., `vdi (users)` to `pos (staging)` on port 22).
- Implement strict access controls and log all remote service usage.

T1210: Exploitation of Remote Services

- Monitor for exploitation attempts on remote services, particularly on commonly exposed ports like 22, 3389, and 443.
- Implement intrusion detection systems and regularly patch remote services.

4. Mitigation Recommendations

T1190: Exploit Public-Facing Application

- Implement strict microsegmentation policies to limit access to public-facing applications from untrusted networks.
- Enforce network policies that only allow necessary traffic between `vdi (users)` and public-facing applications in production.

T1133: External Remote Services

- Use microsegmentation to restrict remote access to specific jump hosts or VPN endpoints.
- Implement network policies that enforce the use of approved remote access methods and restrict direct access to production environments.

T1059: Command and Scripting Interpreter

- Use microsegmentation to limit command execution capabilities to specific administrative hosts.
- Implement network policies that restrict command execution traffic to authorized paths and hosts.

T1078: Valid Accounts

- Implement microsegmentation policies that enforce the principle of least privilege for account access across different network segments.
- Use network policies to restrict account usage to authorized paths and limit lateral movement capabilities.

T1021: Remote Services

- Apply microsegmentation to isolate remote service access, allowing only necessary connections between network segments.
- Implement network policies that enforce the use of secure protocols and restrict unnecessary remote service access.

T1210: Exploitation of Remote Services

- Use microsegmentation to isolate critical services and limit exposure to potential exploitation.
- Implement network policies that restrict access to vulnerable services and enforce strict access controls.

5. Overall Security Posture Improvement

1. Implement strict microsegmentation between different environments (prod, staging, dev) to prevent unauthorized cross-environment access.
2. Review and restrict access from `vdi (users)` and `laptop (users)` to production environments, especially for sensitive services like `pos`, `payment`, and `assetmgmt`.
3. Implement robust logging and monitoring for all inter-segment traffic, particularly focusing on unusual patterns or volumes.
4. Restrict direct access from user segments to production databases (e.g., `shareddb (prod)`) and implement proper application-level access controls.
5. Review and restrict the high volume of connections from `exchange (prod)` to `ad (prod)` on multiple ports, ensuring only necessary traffic is allowed.
6. Implement network-based intrusion detection and prevention systems to monitor for and block potential exploitation attempts.
7. Regularly review and audit all allowed connections, especially those crossing environment boundaries (e.g., `ordering (dev)` to `ordering (prod)`).
8. Implement strong authentication mechanisms, including multi-factor authentication, for all remote access and sensitive service connections.
9. Regularly patch and update all systems, especially those exposed to user segments or external networks.
10. Conduct regular vulnerability assessments and penetration testing to identify and address potential security weaknesses in the network configuration.

By implementing these recommendations and focusing on effective microsegmentation and policy enforcement, the organization can significantly improve its security posture and reduce the risk of successful attacks leveraging the identified ATT&CK techniques.