Architectural Diagram Threat Model & Risk Assessment

Executive Summary

This report presents a security analysis of the provided architectural diagram. A total of 22 components were identified, with 30 potential security threats and corresponding risk assessments.

Identified Components

Component 67 (server)
ID: comp_67

Component 322 (database)
ID: comp_322

Component 324 (database)
ID: comp_324

Component 1023 (server)
ID: comp_1023

Component 1114 (server)
ID: comp_1114

Component 1200 (server)
ID: comp_1200

Component 1263 (database)
ID: comp_1263

Component 1265 (database)
ID: comp_1265

Component 1403 (unknown)
ID: comp_1403

Component 1417 (unknown)
ID: comp_1417

Component 1424 (unknown)
ID: comp_1424

Component 1435 (database)
ID: comp_1435

Component 1437 (database)
ID: comp_1437

Component 1442 (server)
ID: comp_1442

Component 1443 (server)
ID: comp_1443

Component 1545 (unknown)
ID: comp_1545

Component 1554 (unknown)
ID: comp_1554

Component 1570 (server)

ID: comp_1570

Component 1571 (server)
ID: comp_1571

Component 1607 (unknown)
ID: comp_1607

Component 1623 (unknown)
ID: comp_1623

Component 1636 (unknown)
ID: comp_1636

Identified Threats

High Severity Threats

Unpatched Server Vulnerabilities (T001)
Type: Vulnerability
Description: Servers may have unpatched vulnerabilities that can be exploited
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 67
Mitigations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection

SQL Injection (T003)
Type: Injection
Description: Databases may be vulnerable to SQL injection attacks
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 322
Mitigations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users

Sensitive Data Exposure (T004)
Type: Information Disclosure
Description: Databases may expose sensitive data if not properly secured
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 322
Mitigations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments

SQL Injection (T003)
Type: Injection
Description: Databases may be vulnerable to SQL injection attacks
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 324
Mitigations:
- Use parameterized queries

- Implement input validation
- Apply principle of least privilege for database users

Sensitive Data Exposure (T004)
Type: Information Disclosure
Description: Databases may expose sensitive data if not properly secured
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 324
Mitigations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments

Unpatched Server Vulnerabilities (T001)
Type: Vulnerability
Description: Servers may have unpatched vulnerabilities that can be exploited
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1023
Mitigations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection

Unpatched Server Vulnerabilities (T001)
Type: Vulnerability
Description: Servers may have unpatched vulnerabilities that can be exploited
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1114
Mitigations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection

Unpatched Server Vulnerabilities (T001)
Type: Vulnerability
Description: Servers may have unpatched vulnerabilities that can be exploited
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1200
Mitigations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection

SQL Injection (T003)
Type: Injection
Description: Databases may be vulnerable to SQL injection attacks
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1263
Mitigations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users

Sensitive Data Exposure (T004)
Type: Information Disclosure
Description: Databases may expose sensitive data if not properly secured
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 1263
Mitigations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments

SQL Injection (T003)
Type: Injection
Description: Databases may be vulnerable to SQL injection attacks
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1265
Mitigations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users

Sensitive Data Exposure (T004)
Type: Information Disclosure
Description: Databases may expose sensitive data if not properly secured
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 1265
Mitigations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments

SQL Injection (T003)
Type: Injection
Description: Databases may be vulnerable to SQL injection attacks
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1435
Mitigations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users

Sensitive Data Exposure (T004)
Type: Information Disclosure
Description: Databases may expose sensitive data if not properly secured
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 1435
Mitigations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments

SQL Injection (T003)
Type: Injection
Description: Databases may be vulnerable to SQL injection attacks

Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1437
Mitigations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users

Sensitive Data Exposure (T004)
Type: Information Disclosure
Description: Databases may expose sensitive data if not properly secured
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 1437
Mitigations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments

Unpatched Server Vulnerabilities (T001)
Type: Vulnerability
Description: Servers may have unpatched vulnerabilities that can be exploited
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1442
Mitigations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection

Unpatched Server Vulnerabilities (T001)
Type: Vulnerability
Description: Servers may have unpatched vulnerabilities that can be exploited
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1443
Mitigations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection

Unpatched Server Vulnerabilities (T001)
Type: Vulnerability
Description: Servers may have unpatched vulnerabilities that can be exploited
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1570
Mitigations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection

Unpatched Server Vulnerabilities (T001)
Type: Vulnerability
Description: Servers may have unpatched vulnerabilities that can be exploited
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 1571
Mitigations:

- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection

Medium Severity Threats

Denial of Service (T002)
Type: Denial of Service
Description: Servers may be vulnerable to denial of service attacks
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 67
Mitigations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load

Denial of Service (T002)
Type: Denial of Service
Description: Servers may be vulnerable to denial of service attacks
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 1023
Mitigations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load

Denial of Service (T002)
Type: Denial of Service
Description: Servers may be vulnerable to denial of service attacks
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 1114
Mitigations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load

Denial of Service (T002)
Type: Denial of Service
Description: Servers may be vulnerable to denial of service attacks
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 1200
Mitigations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load

Denial of Service (T002)
Type: Denial of Service
Description: Servers may be vulnerable to denial of service attacks
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 1442
Mitigations:
- Implement rate limiting

- Use DDoS protection services
- Scale infrastructure to handle load

Denial of Service (T002)
Type: Denial of Service
Description: Servers may be vulnerable to denial of service attacks
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 1443
Mitigations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load

Denial of Service (T002)
Type: Denial of Service
Description: Servers may be vulnerable to denial of service attacks
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 1570
Mitigations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load

Denial of Service (T002)
Type: Denial of Service
Description: Servers may be vulnerable to denial of service attacks
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 1571
Mitigations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load

Insufficient Network Segmentation (T201)
Type: Lateral Movement
Description: Lack of network segmentation may allow lateral movement in case of breach
Risk: High likelihood, Medium impact (Score: 6)
Affected Components: Component 67, Component 322, Component 324, Component 1023, Component 1114, Component 1200, Component 1263, Component 1265, Component 1403, Component 1417, Component 1424, Component 1435, Component 1437, Component 1442, Component 1443, Component 1545, Component 1554, Component 1570, Component 1571, Component 1607, Component 1623, Component 1636
Mitigations:
- Implement network segmentation
- Use firewalls between segments
- Apply zero trust principles

Single Point of Failure (T202)
Type: Availability
Description: Architecture may have single points of failure affecting availability
Risk: High likelihood, Medium impact (Score: 6)
Affected Components: Component 67, Component 322, Component 324, Component 1023, Component 1114, Component 1200, Component 1263, Component 1265, Component 1403, Component 1417,

Component 1424, Component 1435, Component 1437, Component 1442, Component 1443, Component 1545, Component 1554, Component 1570, Component 1571, Component 1607, Component 1623, Component 1636

Mitigations:

- Implement redundancy
- Use load balancing
- Design for fault tolerance

Risk Assessment

Unpatched Server Vulnerabilities (T001)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

SQL Injection (T003)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

SQL Injection (T003)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Unpatched Server Vulnerabilities (T001)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Unpatched Server Vulnerabilities (T001)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Unpatched Server Vulnerabilities (T001)

Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

SQL Injection (T003)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

SQL Injection (T003)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

SQL Injection (T003)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

SQL Injection (T003)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Use parameterized queries
- Implement input validation
- Apply principle of least privilege for database users
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Unpatched Server Vulnerabilities (T001)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Implement regular patching schedule

- Use vulnerability scanning tools
- Implement host-based intrusion detection
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Unpatched Server Vulnerabilities (T001)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Unpatched Server Vulnerabilities (T001)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Unpatched Server Vulnerabilities (T001)
Risk Score: 9 (High likelihood, High impact)
Recommendations:
- Implement regular patching schedule
- Use vulnerability scanning tools
- Implement host-based intrusion detection
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Sensitive Data Exposure (T004)
Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Sensitive Data Exposure (T004)
Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments
- Prioritize immediate remediation

- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Sensitive Data Exposure (T004)
Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Sensitive Data Exposure (T004)
Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Sensitive Data Exposure (T004)
Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Sensitive Data Exposure (T004)
Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt sensitive data
- Implement proper access controls
- Use data masking for non-production environments
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Insufficient Network Segmentation (T201)
Risk Score: 6 (High likelihood, Medium impact)
Recommendations:
- Implement network segmentation
- Use firewalls between segments
- Apply zero trust principles
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Single Point of Failure (T202)
Risk Score: 6 (High likelihood, Medium impact)
Recommendations:
- Implement redundancy
- Use load balancing
- Design for fault tolerance
- Prioritize immediate remediation
- Implement compensating controls while addressing the root cause
- Consider additional monitoring for early detection

Denial of Service (T002)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load
- Address within normal security improvement cycles
- Implement detection mechanisms

Denial of Service (T002)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load
- Address within normal security improvement cycles
- Implement detection mechanisms

Denial of Service (T002)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load
- Address within normal security improvement cycles
- Implement detection mechanisms

Denial of Service (T002)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load
- Address within normal security improvement cycles
- Implement detection mechanisms

Denial of Service (T002)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load
- Address within normal security improvement cycles

- Implement detection mechanisms

Denial of Service (T002)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load
- Address within normal security improvement cycles
- Implement detection mechanisms

Denial of Service (T002)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load
- Address within normal security improvement cycles
- Implement detection mechanisms

Denial of Service (T002)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement rate limiting
- Use DDoS protection services
- Scale infrastructure to handle load
- Address within normal security improvement cycles
- Implement detection mechanisms