Architectural Diagram Threat Model & Risk Assessment

Executive Summary

This report presents a security analysis of the provided architectural diagram. A total of 11 components were identified, with 14 potential security threats and corresponding risk assessments.

Identified Components

Component 666 (unknown)
ID: comp_666

Component 671 (database)
ID: comp_671

Component 672 (database)
ID: comp_672

Component 911 (unknown)
ID: comp_911

Component 1024 (unknown)
ID: comp_1024

Component 1162 (unknown)
ID: comp_1162

Component 1164 (unknown)
ID: comp_1164

Component 1233 (unknown)
ID: comp_1233

Component 1276 (unknown)
ID: comp_1276

Component 1357 (server)
ID: comp_1357

Component 1360 (server)
ID: comp_1360

Identified Threats

High Severity Threats

SQL Injection (T003)
Type: Injection
Description: Databases may be vulnerable to SQL injection attacks
Risk: High likelihood, High impact (Score: 9)
Affected Components: Component 671
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 671
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 672
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 672
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 1357
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 1360
Mitigations:

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

Medium Severity Threats

Excessive Privilege (T005)
Type: Access Control

Description: Database users may have more privileges than necessary, increasing attack surface
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 671
Mitigations:

- Implement principle of least privilege
- Regularly audit user permissions
- Use role-based access control

Insecure Database Backup (T006)
Type: Information Disclosure
Description: Database backups may not be properly secured, leading to data exposure
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 671
Mitigations:

- Encrypt database backups
- Implement secure backup storage
- Establish backup retention policies

Excessive Privilege (T005)
Type: Access Control
Description: Database users may have more privileges than necessary, increasing attack surface
Risk: Medium likelihood, Medium impact (Score: 4)
Affected Components: Component 672
Mitigations:

- Implement principle of least privilege
- Regularly audit user permissions
- Use role-based access control

Insecure Database Backup (T006)
Type: Information Disclosure
Description: Database backups may not be properly secured, leading to data exposure
Risk: Medium likelihood, High impact (Score: 6)
Affected Components: Component 672
Mitigations:

- Encrypt database backups
- Implement secure backup storage
- Establish backup retention policies

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 1357
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 1360

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 666, Component 671, Component 672, Component 911, Component 1024, Component 1162, Component 1164, Component 1233, Component 1276, Component 1357, Component 1360

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 666, Component 671, Component 672, Component 911, Component 1024, Component 1162, Component 1164, Component 1233, Component 1276, Component 1357, Component 1360

Mitigations:

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

Risk Assessment

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

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

Insecure Database Backup (T006)

Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt database backups
- Implement secure backup storage
- Establish backup retention policies
- 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

Insecure Database Backup (T006)
Risk Score: 6 (Medium likelihood, High impact)
Recommendations:
- Encrypt database backups
- Implement secure backup storage
- Establish backup retention policies
- 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

Excessive Privilege (T005)
Risk Score: 4 (Medium likelihood, Medium impact)
Recommendations:
- Implement principle of least privilege

- Regularly audit user permissions
- Use role-based access control
- Address within normal security improvement cycles
- Implement detection mechanisms

Excessive Privilege (T005)

Risk Score: 4 (Medium likelihood, Medium impact)

Recommendations:

- Implement principle of least privilege
- Regularly audit user permissions
- Use role-based access control
- 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