SecureCloud Solutions

Confidential Internal Document

# Cybersecurity Posture Overview

Date: June 15, 2023

## 1. Executive Summary

SecureCloud Solutions is committed to maintaining the highest standards of cybersecurity to protect our clients' data and our internal systems. This document provides an overview of our current cybersecurity posture, highlighting our strengths and areas for continuous improvement.

## 2. Network Security

### 2.1 Perimeter Defense

- Implemented Palo Alto Networks PA-5250 next-generation firewalls
- Cisco Firepower 4110 NGIPS for intrusion prevention
- Imperva WAF for web application protection

### 2.2 Network Segmentation

- Implemented micro-segmentation using VMware NSX
- Critical assets isolated in separate VLANs
- Zero Trust Network Access (ZTNA) principles applied

### 2.3 Remote Access

- Cisco AnyConnect Secure Mobility Client for VPN access
- Split-tunnel VPN configuration to optimize performance

## 3. Data Protection

### 3.1 Encryption

- AES-256 encryption for data at rest

- TLS 1.3 for data in transit
- Gemalto SafeNet KeySecure for key management

3.2 Data Loss Prevention

- Symantec DLP suite implemented across endpoints and network
- Regular DLP policy reviews and updates

3.3 Access Control

- Implemented Okta for Identity and Access Management (IAM)
- Role-Based Access Control (RBAC) enforced across all systems
- Quarterly access reviews conducted

4. Incident Response

4.1 IR Plan

- Comprehensive IR plan documented and updated bi-annually
- Clearly defined roles and responsibilities for IR team members

4.2 Detection and Analysis

- Splunk SIEM for log aggregation and analysis
- IBM QRadar for advanced threat detection

4.3 Containment and Eradication

- Automated containment procedures for critical systems
- Partnerships with forensic analysis firms for complex incidents

4.4 Testing and Improvement

- Quarterly tabletop exercises
- Annual full-scale IR simulation

5. Compliance

5.1 Regulatory Compliance

- SOC 2 Type II certified
- GDPR and CCPA compliant
- HIPAA compliance for healthcare clients

5.2 Compliance Monitoring

- Implemented OneTrust for compliance management
- Automated compliance checks using Qualys Policy Compliance

5.3 Audits and Assessments

- Annual third-party penetration testing
- Quarterly internal security audits

6. Endpoint Security

6.1 Endpoint Protection

- CrowdStrike Falcon deployed on all endpoints
- Carbon Black EDR for advanced threat hunting

6.2 Patch Management

- Automated patch management using Ivanti Security Controls
- Critical patches applied within 24 hours of release

6.3 Mobile Device Management

- VMware Workspace ONE for MDM and MAM
- Strict BYOD policies enforced

7. Authentication

7.1 Multi-Factor Authentication

- Duo Security MFA implemented across all systems
- Hardware security keys (YubiKey) for privileged accounts

### 7.2 Password Policies

- Minimum 16-character passwords with complexity requirements
- Password rotation every 90 days
- Password managers provided to all employees

### 7.3 Advanced Authentication

- Piloting FIDO2 passwordless authentication

## 8. Cloud Security

### 8.1 Cloud Service Providers

- Utilizing AWS and Azure with their respective native security tools
- Regular security configuration reviews using CloudCheckr

### 8.2 Cloud Access Security

- Implemented Netskope CASB solution
- Data classification and tagging for all cloud-stored data

### 8.3 Containerization Security

- Aqua Security for container and Kubernetes security
- Twistlock for runtime protection of containers

## 9. Security Awareness

### 9.1 Training Program

- KnowBe4 platform for security awareness training
- Mandatory quarterly training sessions for all employees

### 9.2 Phishing Simulations

- Monthly phishing tests with targeted training for failures
- Phish alert button installed on all email clients

### 9. 3 Security Champions

- Designated security champions in each department
- Quarterly security awareness newsletters

## 10. Conclusion

SecureCloud Solutions is committed to maintaining a robust cybersecurity posture. This document highlights our current security controls and areas for improvement. We will continue to invest in our security infrastructure and employee training to stay ahead of emerging threats.

Confidentiality Notice:

This document contains confidential and proprietary information of SecureCloud Solutions. It is intended solely for internal use and should not be shared with external parties without explicit permission.