Findings Report

{{ assessment\_name }}



Business Confidential

July 10, 2020

Revision 0.1 - DRAFT



# Assessment Information

|  |  |
| --- | --- |
| Confidentiality Statement | This document is the exclusive property of {{ client\_name }} ({{ client\_short }}) and NorthState. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both {{ client\_short }} and NorthState.  {{ client\_short }} may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance. |

|  |  |
| --- | --- |
| Contact Information | The following table provides key contact information related to this project |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Title | | Contact Data | |
| **{{ client\_short }}** | | | | |
| **{%tr for poc in client\_pocs %}** | | | | |
| {{ poc.name }} | | {{ poc.job\_title }} | | {{ poc.email }} |
| {%tr endfor %} | | | | |
| **NorthState** | | | | |
| Brent Brackin | | Director Business Development | | Office: (727) 773-6516  Email: [brent.brackin@nscom.com](mailto:brent.brackin@nscom.com) |
| Roger Preble | | Client Executive | | Office: (704) 904-3344  Email: roger.prebble@nscom.com |
| Mac Barnhardt | | Account Executive | | Office: (704) 560-5026  Email: [mac.barnhardt@nscom.com](mailto:mac.barnhardt@nscom.com) |
| Matt Lewis | | Account Executive | | Office: (704) 906-8986  Email: [matt.lewis@nscom.com](mailto:matt.lewis@nscom.com) |
| Joedy Glenn | | Sr. Solutions Architect | | Office: (704) 779-4520  Email: joedy.glenn@nscom.com |
| Jonathan Wilson | | Sr. Solutions Architect | | Office: (704) 751-7552  Email: [jonathan.wilson@nscom.com](mailto:jonathan.wilson@nscom.com) |
| Bart Casey | | Solutions Architect | | Office: (864) 809-0752  Email: [bart.casey@nscom.com](mailto:bart.casey@nscom.com) |
| Anthony Ralston | | Sr. Penetration Tester | | Office: (910) 333-4428  Email: [anthony.ralston@nscom.com](mailto:anthony.ralston@nscom.com) |
| Sean Kilbourn | | Sr. Penetration Tester | | Office: (704) 870-7249  Email: [sean.kilbourn@nscom.com](mailto:sean.kilbourn@nscom.com) |
| Christian Campbell | | Sr. Penetration Tester | | Office: (980) 428-6129  Email: [christian.campbell@nscom.com](mailto:christian.campbell@nscom.com) |
| Aaron Williams | | Sr. Penetration Tester | | Office: (910) 635-9008  Email: [aaron.williams@nscom.com](mailto:aaron.williams@nscom.com) |

|  |  |
| --- | --- |
| Revision History | NorthState may update technical inaccuracies and typographic errors in subsequent releases. The following table summarizes previous revisions: |

|  |  |  |
| --- | --- | --- |
| Revision | Date | Description of Change |
| 0.1 | MM/DD/YY | Initial Internal Draft – [INITIALS WHEN COMPLETED] |
| 0.2 |  | Technical QA – [INITIALS WHEN COMPLETED] |
| 0.3 |  | Technical Revisions– [INITIALS WHEN COMPLETED)] |
| 0.4 |  | Business QA – [INITIALS WHEN COMPLETED] |
| 0.5 |  | Business Revisions– [INITIALS WHEN COMPLETED] |
| 0.6 |  |  |
| 0.7 |  |  |
| 0.8 |  |  |
| 0.9 |  | Initial Customer Draft |
| 1.0 |  | Initial Customer Release |

# Contents

[Assessment Information 2](#_Toc45289743)

[Contents 4](#_Toc45289744)

# Executive Summary

|  |  |
| --- | --- |
| Overview | {{ client\_short }} engaged NorthState to evaluate their current information security posture and provide recommendations for improvement.  NorthState tested {{ client\_short }}’s people, processes, and technology controls targeting both internal and external networks.  [-OR-]NorthState measured the current [Application] security control’s effectiveness using standard penetration testing techniques.  [-OR-]{{ client\_short }} engaged NorthState to assess the security of its infrastructure compared to current industry best practices. Based on that assessment NorthState captured recommendations for remediating vulnerabilities and improving {{ client\_short }}’s overall security posture.  [-OPTIONAL-] NorthState identified critical severity issues requiring {{ client\_short }}’s attention.  This assessment will help {{ client\_short }} accomplish the following:   * Gain a real-world perspective on its current security posture. * Gain a real-world perspective on [Application]’s current security posture. * Understand how to strengthen its security program. * Continue promoting security awareness throughout the organization. * Perform an external security assessment of the [Application name] solution and defined IP’s to identify risks. * Define the severity and mitigation strategy for identified risks. * Provide 3rd party documentation proving security testing as a part of {{ client\_short }}’s application management practice. |

|  |  |
| --- | --- |
| Findings Distribution | The following chart illustrates the findings distribution:  A screenshot of a cell phone  Description automatically generated |

|  |  |
| --- | --- |
| Assessment “Report Card” | The following table summarizes NorthState’s rating of the strengths and weaknesses of observed controls. NorthState assigns a summary rating to each component using academic grades. These grades do not reflect risk but compare {{ client\_short }} to similar assessments. |

|  |  |  |
| --- | --- | --- |
| Component | Grade | Details |
| [COMPONENT 1] | **B** | **Strengths**: \_ |
| **Weaknesses**: \_ |
| [COMPONENT 2] | **A** | **Strengths: \_** |
| **Weaknesses: \_** |

|  |  |
| --- | --- |
| Findings  Summary | The following table summarizes the findings identified during the assessment. [-OPTIONAL-if only one component] These findings represent confidentiality, integrity, or availability vulnerabilities.  ***Note****: Severity ratings are based on NIST Special Publication 800-30 Guide for Conducting Risk Assessments*. *See* [*Appendix 2: Finding Severity Ratings*](#_Appendix_2:_Finding) *for additional details.* |

| Finding Title | Severity | Recommendation |
| --- | --- | --- |
| [Component 1] | | |
| {%tr for finding in findings %} | | |
| {{ finding.title }} | {% cellbg finding.color %}{{ finding.severity }} | {{ finding.recommendation }} |
| {%tr endfor %} | | |
| *[Optional based on number of Critical/High]* | **Moderate** |  |
| *[Optional based on number of Critical/High]* | **Low** |  |
| [Component 2] | | |
|  | **Critical** |  |
|  | **High** |  |
| *[Optional based on number of Critical/High]* | **Moderate** |  |
| *[Optional based on number of Critical/High]* | **Low** |  |
| [Component 3] | | |
|  |  |  |

# Assessment Summary

|  |  |
| --- | --- |
| Overview | This section summarizes the approach and results for each assessment component:   * AWS Cloud Architecture Assessment * AWS External Penetration Text * Core Systems Confidentiality, Integrity, Availability (CIA) Review * Endpoint Malware Assessment * External Penetration Test * External Vulnerability Scan * Infrastructure Assessment * Internal Console Assessment * Internal Penetration Test * Internal Vulnerability Scan * Physical Penetration Test * Privileged Identity Management Assessment * Remote Access Assessment * Security Practice Assessment * Security Practice Assessment * Social Engineering Test * Web Application Penetration Test * Wireless Penetration Test |

|  |  |
| --- | --- |
| [COMPONENT1]  Example | Cloud providers offer organizations the capability of quickly deploying new solutions with the scalability of elastic compute resources. NorthState’s Cloud Architecture Assessment identifies misconfigurations in both private and public clouds. Fixing these misconfigurations will minimize service disruptions and mitigate breach risk  NorthState identified multiple misconfigurations in {{ client\_short }}’s AWS accounts. Most issues identified were in the IAM, EC2, and VPC services. None of the findings represented critical risk to the organization. |

## [Component 1] Test (@@@) Findings

|  |  |
| --- | --- |
| [COMPONENT1]  Overview | Cloud providers offer organizations the capability of quickly deploying new solutions with the scalability of elastic compute resources. NorthState’s Cloud Architecture Assessment identifies misconfigurations in both private and public clouds. Fixing these misconfigurations will minimize service disruptions and mitigate breach risk  NorthState found multiple misconfigurations in {{ client\_short }}’s AWS accounts. Most issues identified were in the IAM, EC2, and VPC services. None of the findings represented critical risk to the organization. |

{{p findings\_subdoc }}