



**STRATOSPHERE**  
NETWORKS

# STRATOSPHERE SECURITY ASSESSMENT

As hackers get smarter and more dynamic, it's more important than ever for businesses to focus on IT security. No one is immune to hacking and data breaches. Performing security audits and establishing best practices has historically been very expensive and complicated, but Stratosphere now offers an economical way to benchmark and implement a comprehensive security solution.



**HIPAA  
COMPLIANT**

**98%**  
CUSTOMER  
SATISFACTION



**\$80,000+**  
IN CONTRIBUTIONS  
& DONATIONS

**600+**  
HOURS OF  
COMMUNITY  
SERVICE



**99%**  
CLIENT  
RETENTION RATE

**5x**  
BEST  
PLACES  
TO WORK  
IN CHICAGO  
**CRAIN'S**



**IT DEPARTMENT  
OF THE YEAR**

## Sign up for a Stratosphere Security Assessment and receive the following:

- ✦ Introductory meeting with a security analyst to develop security risk audit report.\*
- ✦ Vulnerabilities and risks report\*\*
- ✦ Strategic security road map, including specific cybersecurity solutions\*\*\*
- ✦ Second meeting with a security analyst to review results, reports and road map.

\* Please see the image labeled deliverable 1

\*\* Please see the image labeled deliverable 2

\*\*\*Please see the image labeled deliverable 3

Contact us at: [877-599-3999](tel:877-599-3999) or [sales@stratnet.com](mailto:sales@stratnet.com) for more information.

# SECURITY ASSESSMENT OFFERING PHASES

Our security assessment offering involves the following three

## PHASE 1 Security Risk Audit

During this portion of the process, a security analyst works hand-in-hand with you to collect data and provide an overall summary report. This audit collects data and provides overall summary report(s). We will conduct a background check based on a streamlined version of the CIS controls. This phase will also include the following:

- ✦ **Gap analysis:** Evaluates your overall current cybersecurity program according to industry best practices.

**Security Risk Assessment Report**  
Prepared for Your Company - 06/21

**Center for Internet Security (CIS) Controls Framework**

The CIS Controls are a recommended set of actions for cyber defense that provide specific and actionable steps to thwart the most pervasive attacks. The CIS Controls are a relatively short list of high-priority, highly effective defensive actions that provide a "roadmap" and/or "starting point" for every enterprise seeking to improve their cyber defense.

The CIS Controls were developed starting in 2009 by an international, cross-sector consortium bringing together companies, government agencies, institutions, and individuals from every part of the enterprise (upper, middle, and lower management, security, operations, security, policy matters, executives, academic, academic, etc.) who banded together to create, define, and support the CIS Controls. Prioritization is a key benefit to the CIS Controls. They were designed to help organizations rapidly define the starting point for their defenses, direct their scarce resources to an attack with immediate and high-risk impact, and then focus their attention and resources on additional risk areas that are unique to their business or industry.

Reference: <https://www.cisecurity.org/controls/>

Stratosphere has taken the CIS Controls and further streamlined them for this risk assessment by creating an easy-to-understand and actionable list of what we view as the most critical sub-controls within each of the 20 main controls of the CIS Framework.

**50** A score of 50 or less indicates a high-risk environment.

**75** A score of under 75, but more than 50 indicates a medium-risk environment.

**100** A score of under 100, but more than 75 indicates a medium-risk environment.

**Risk Score: 62 - MEDIUM RISK ENVIRONMENT**

CIS Control Name	Score	Priority	Source	Source Date	Remediation/Current Controls
CIS 1: Identify and Classify Software Assets	50	High	Yes	Yes	All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security.
CIS 2: Implement Software Patch Management	75	High	Yes	Yes	Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security.
CIS 3: Configure and Manage Secure Network Settings	75	High	Yes	Yes	Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security.
CIS 4: Secure Configuration for Servers, Operating Systems, and Software on Mobile Devices, Laptops, Tablets, and Smart Phones	75	High	Yes	Yes	Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security.
CIS 5: Monitor, Detect, and Analyze Malicious Activity	75	High	Yes	Yes	Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security.
CIS 6: Assess and Test System Defenses	75	High	Yes	Yes	Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security.
CIS 7: Perform Patching, Updating, and Patching of All Critical and Essential Applications	75	High	Yes	Yes	Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security.
CIS 8: Monitor Software Assets	75	High	Yes	Yes	Department of Information Systems and Security. All IT systems and IT devices are inventoried and classified by Department of Information Systems and Security.

**STRATOSPHERE NETWORKS**

DELIVERABLE 1

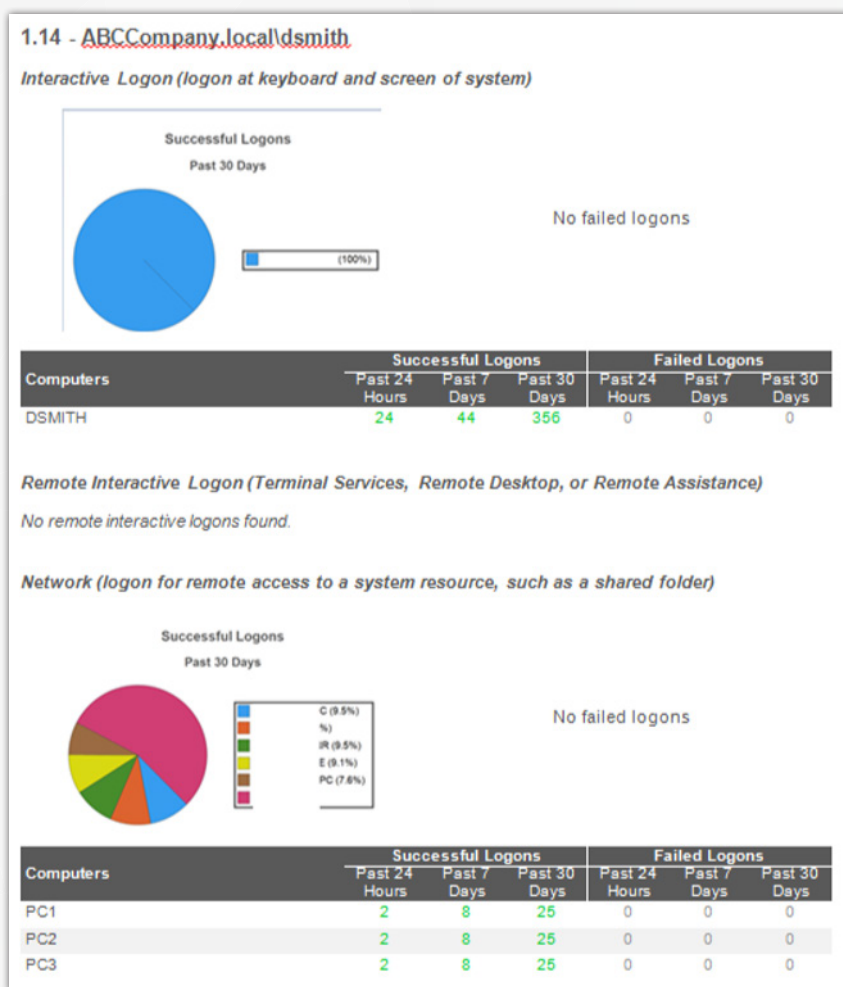
Contact us at: [877-599-3999](tel:877-599-3999) or [sales@stratnet.com](mailto:sales@stratnet.com) for more information.

## PHASE 2

# Internal and External Vulnerability Scans and Reports

A security analyst runs up-to-date vulnerability scans on your network. We use the results of these scans to develop and provide vulnerability reports, to pinpoint risks, and to build a strategic security roadmap to mitigate risks.

- ✦ **Vulnerability scans:** These internal and external scans will identify any vulnerabilities in your network and systems that could potentially lead to a data breach.
- ✦ **Vulnerabilities and risk reports + details:** This will help our team gain visibility into the details of the client's current risks. Examples of those details include the following:
  - ✦ Folders/paths with shared permissions
  - ✦ Password policies
  - ✦ Snapshot of users that recently accessed specific workstations
  - ✦ Windows Updates
  - ✦ Instances of personal identifiable information (PII) within your network that could be targeted.
  - ✦ Potential monetary liability

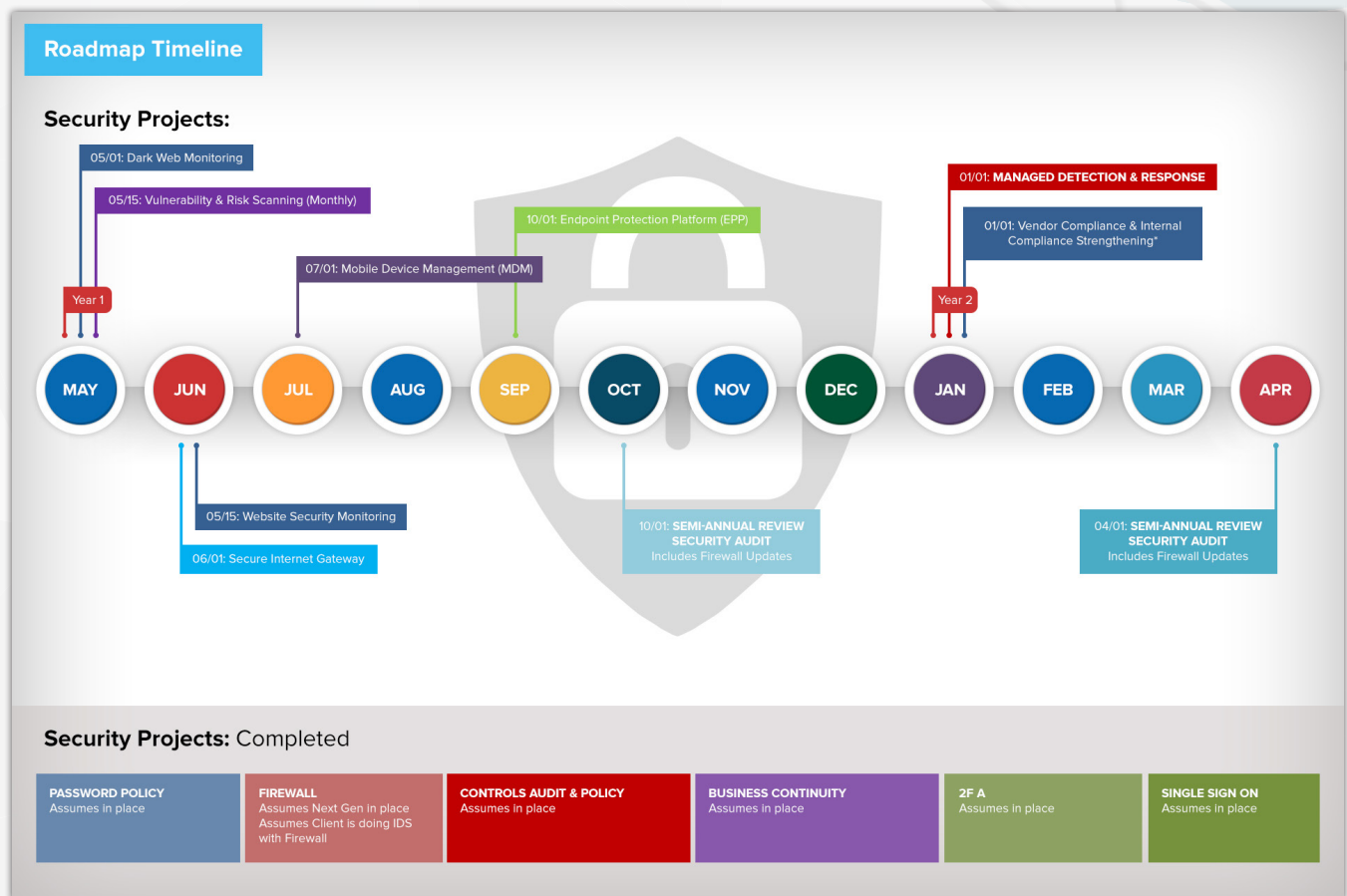


### DELIVERABLE 2

## PHASE 3

# Strategic security road map and advisory meeting

- ✦ Security analyst works to develop a custom plan based on results of the previous two phases.
- ✦ Security analyst reviews the plan with the customer.
- ✦ Final deliverable is provided with formal strategic security road map, which includes the following:
  - ✦ Various best-in-class cybersecurity solutions, customized to fit the client's needs and with the option for Stratosphere to manage them if the client would prefer not to do so
  - ✦ IT security recommendations
  - ✦ Best practices for minimizing risks and maintaining optimal security



## DELIVERABLE 3

Contact us at: [877-599-3999](tel:877-599-3999) or [sales@stratnet.com](mailto:sales@stratnet.com) for more information.