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.

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 or sales@stratnet.com for more information.

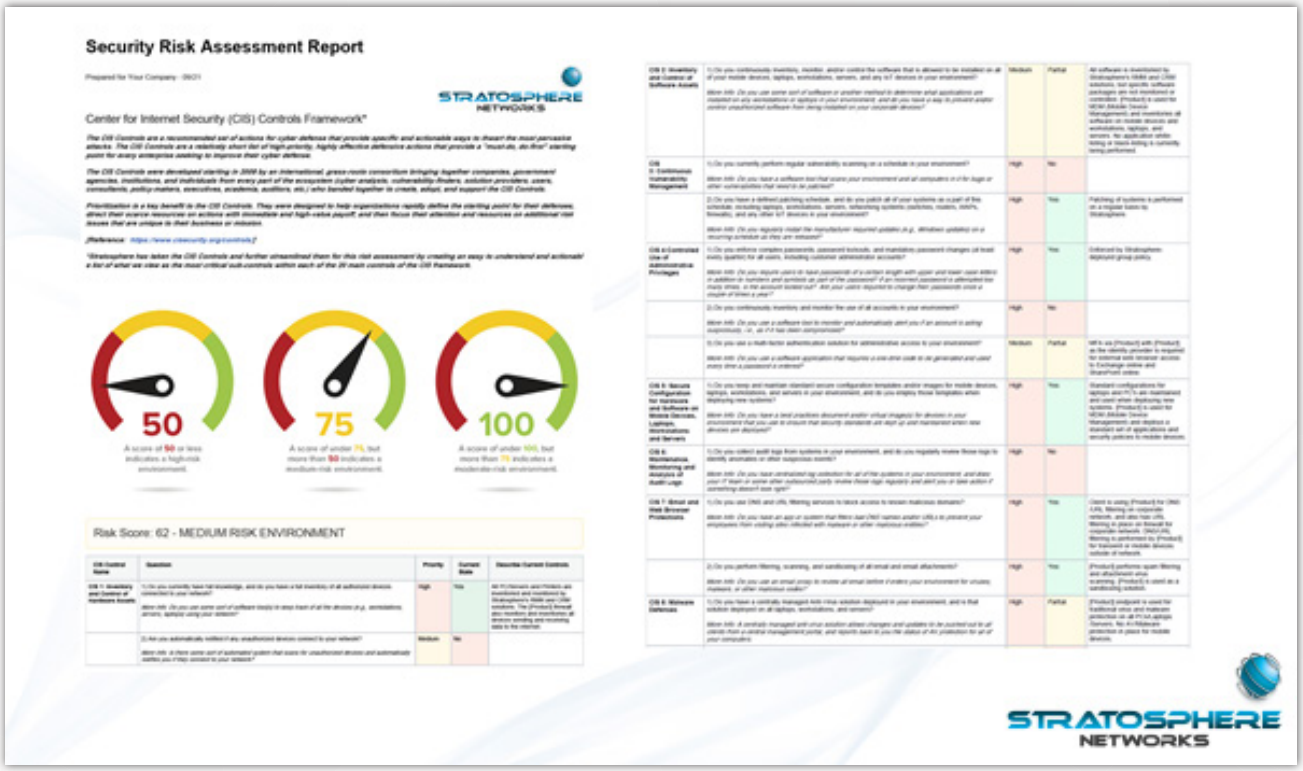
SECURITY ASSESSMENT OFFERING PHASES

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.



DELIVERABLE 1

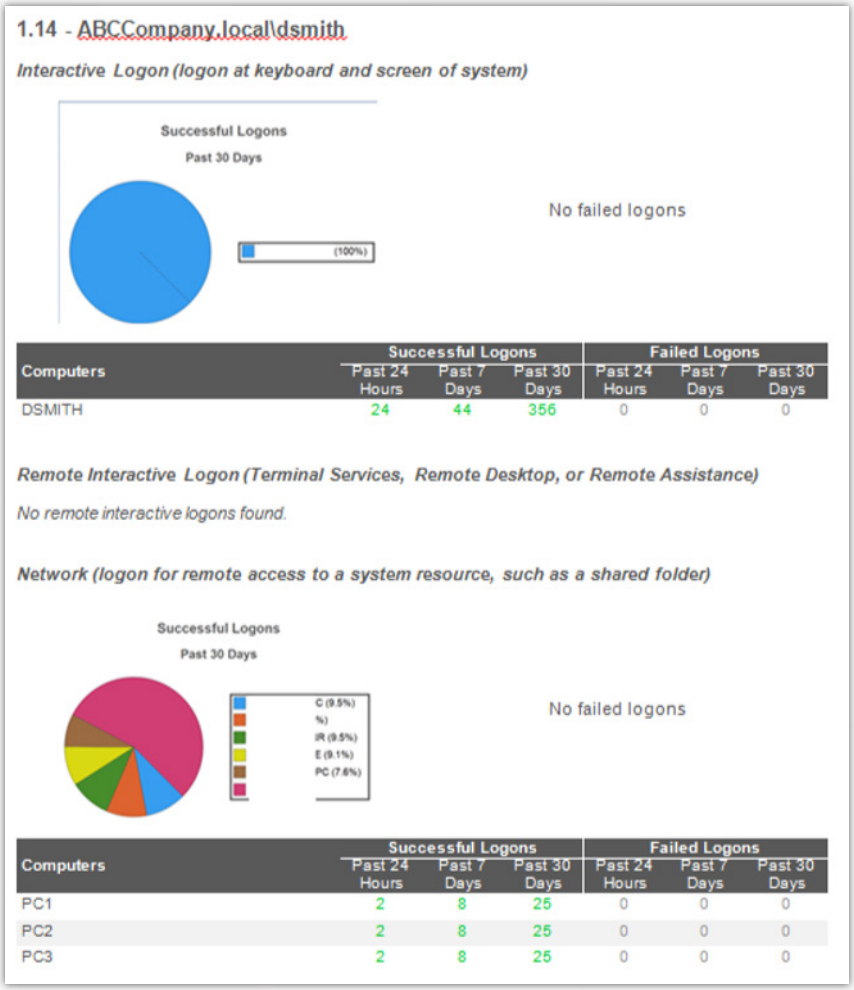
Contact us at: 877-599-3999 or sales@stratnet.com for more information.

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



1.14 - ABCCompany.local\dsmith

Interactive Logon (logon at keyboard and screen of system)

Successful Logons
Past 30 Days

(100%)

No failed logons

Computers	Successful Logons			Failed Logons		
	Past 24 Hours	Past 7 Days	Past 30 Days	Past 24 Hours	Past 7 Days	Past 30 Days
DSMITH	24	44	356	0	0	0

Remote Interactive Logon (Terminal Services, Remote Desktop, or Remote Assistance)

No remote interactive logons found.

Network (logon for remote access to a system resource, such as a shared folder)

Successful Logons
Past 30 Days

C (9.5%)
%)
IR (9.5%)
E (9.1%)
PC (7.6%)

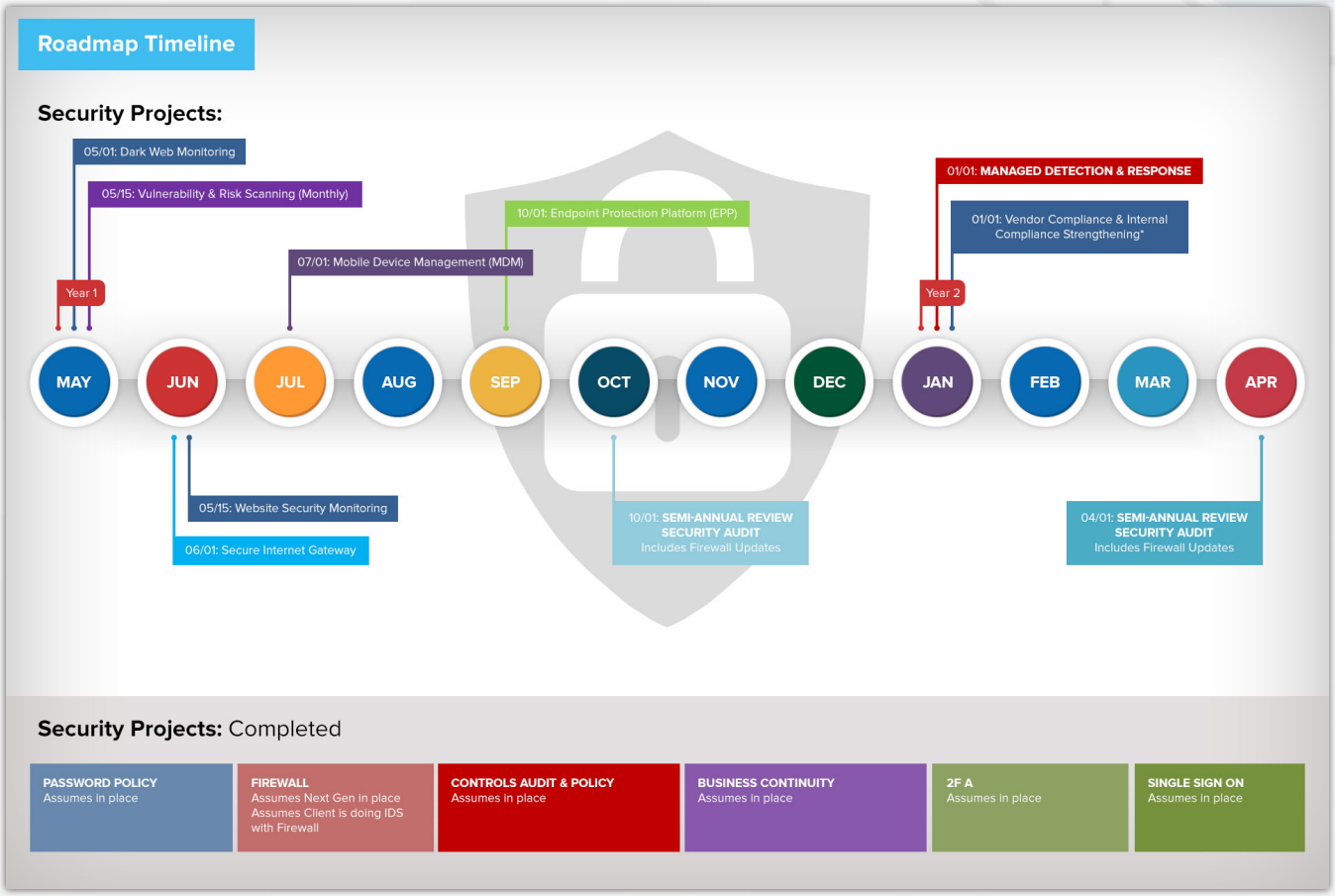
No failed logons

Computers	Successful Logons			Failed Logons		
	Past 24 Hours	Past 7 Days	Past 30 Days	Past 24 Hours	Past 7 Days	Past 30 Days
PC1	2	8	25	0	0	0
PC2	2	8	25	0	0	0
PC3	2	8	25	0	0	0

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