**CSAT Frequently Asked Questions**

**Is CSAT a cloud application?**

No, CSAT is installed on a Windows Server in the customers IT network. All collected data will stay inside the customer network.

**Who has access to the data that CSAT collects?**

Only the customer itself and the service partner that installs and operates the CSAT application have access to the data that is collected. CSAT is installed On Premise at the customer, there is no data sent out to any party or any cloud location. The CSAT installation will be deleted after the assessment.  
In some cases the final report might be shared with Microsoft.

**Does CSAT use my corporate information for other purposes than a Cybersecurity assessment?**

CSAT only uses your data to assess your Cybersecurity status and generate a fact- and risk-based action plan to improve cyber security. It takes a holistic perspective to ensure that all relevant security topics are covered in the assessment, using a questionnaire that is derived from the internationally recognized CIS framework (Center for Internet Security).

**Does CSAT install something on the endpoints?**

CSAT does not install a permanent agent on the endpoint. CSAT will deploy a so-called ‘dissolvable agent’ on the targeted endpoints. This small executable will delete itself from the endpoint after the relevant data is sent back to the CSAT server in the customers network.

**What about network traffic? Does CSAT cause performance issues on the network?**

CSAT does not cause any performance issues. CSAT will only deploy the agent to 20 endpoints at the same time. Making sure the network load is kept to a minimum.

**Is CSAT a monitoring tool?**

No, CSAT takes a snapshot of the current status of your cyber security. It collects relevant information by extracting data from Endpoints (Windows laptops/desktops and Windows Servers), Office 365 services, Azure AD and local Active Directory. Furthermore, CSAT uses a questionnaire to get insights on organizational policies and procedures around Cybersecurity.

CSAT will provide you with a fact-based view on the current cybersecurity status and will recommend action items to improve your security based on these facts. Presenting these facts to the upper Management should improve the follow up security projects.

**We already have a pen-test tool (or other security tools), do I need CSAT?**

These tools are very valuable for your organization and you should keep on using these tools. Monitoring and pen-test tools are reactive, they propose actions based on detected incidents by constantly monitoring certain elements of your systems.  
CSAT takes a different approach than security pen-test or monitoring tools. CSAT will provide you with an action plan to improve security, it is a holistic assessment tool that helps to define the right security improvement projects. Besides checking for windows updates, and some security settings, CSAT collects some Identity Access Management related items, like (stale) accounts and permissions.

**I already have Anti-Virus, do I need CSAT?**

Anti-Virus tools are very valuable for your organization and you should keep on using these tools. Anti-Virus tools act based on detected incidents by constantly monitoring certain elements of your systems.  
CSAT takes a different approach than Anti-Virus tools. CSAT will provide you with an action plan to improve security, it is a holistic assessment tool that helps to define the right security improvement projects. CSAT will identify the AV used on a system and can check the update status of the AV.

**What are the sources CSAT collects information from?**

CSAT collects relevant information by extracting data from Endpoints (Windows laptops and Windows Servers), Office 365 services, Azure AD and local Active Directory. For each source, a different method of data collection is used.

For the endpoints, CSAT uses a ‘dissolvable agent’ on the targeted endpoints. This small executable will delete itself from the endpoint after the relevant data is sent to the CSAT server in the customers network.

For local Active Directory, CSAT uses the Administrator credentials to extract the AD information.

The Microsoft cloud services are being accessed using the API’s.

**How does CSAT collect data from the endpoint?**

CSAT collects data by sending out requests over WMI ports (so these ports should be open on endpoints). Our dissolvable agent is then transferred over WMI and extracted and executed on the endpoints. After extracting the information and sending it back to the CSAT server, executable will dissolve itself from the endpoint.

**All our IT is outsourced, how can CSAT be of value to us?**

CSAT can be used to double check the current security state of the environment. If you out-source your IT, it is still your responsibility to check if the security is in order.

**We use VDI or remote desktop connections/thin clients, is CSAT still helpful for us then?**

CSAT can scan a VDI desktop, and the servers. Still a lot of security issues can be found on these systems. We tend to see VDI systems only patched once every 3 months, due to issues with the business performing acceptance tests. Together with the questionnaire we can cover a lot of topics.

**We already have security projects running, is CSAT still valuable?**

CSAT is not a typical point solution, so there will only be small overlap with existing projects. The end report of CSAT might be of help to get this/other security projects up and running, because the CSAT report can help identify issues to management.

**How do you install the CSAT software on our server? Do you need to be on-site for the CSAT scan?**

We do all the work remotely, via Skype or other means of communication (like TeamViewer if you prefer that)

**What kind of access rights are needed for a CSAT installation and scan?**

CSAT needs to be installed on a fresh Server, so permissions are needed for that.

For a scan the following is needed:

* AD scan: a user account allowed to enumerate all users, accounts, groups, computers, and domain functional levels
* Endpoint scan: Domain admin account with permissions on the endpoint, or a Local Admin account (for example set through a Group Policy) on all the endpoints
* Office 365/Azure AD account: newly created Service principal, needs to be approved by Global Administrator
* SharePoint: Create service principal, approve these with the SharePoint administrator account

**We are too busy for this assessment/How much time of my team is needed for the CSAT scan?**

Your team would spend around half a day in performing the assessment.

* Spin up a freshly installed machine
* Configure the scans
* Take the questionnaire/interview
* Attend the presentation of the results