



StacksWare

REAL-TIME SOFTWARE INVENTORY & USAGE

Security Briefing

FORTUNE
500

Infrastructure Overview

As detailed in the diagram, StacksWare pulls information from all the machines in your datacenter (be it virtual servers, VDI, or physical workstations) by forwarding data through the StacksWare virtual appliance.

This forwarded data is then processed by your organization's private StacksWare instance (i.e. dedicated hosting) in the Amazon cloud. This instance also provides the helpful dashboards and reports for understanding your software usage.

Context: The StacksWare virtual appliance is a Linux OVA (pre-packaged operating system), which deploys directly through vCenter.

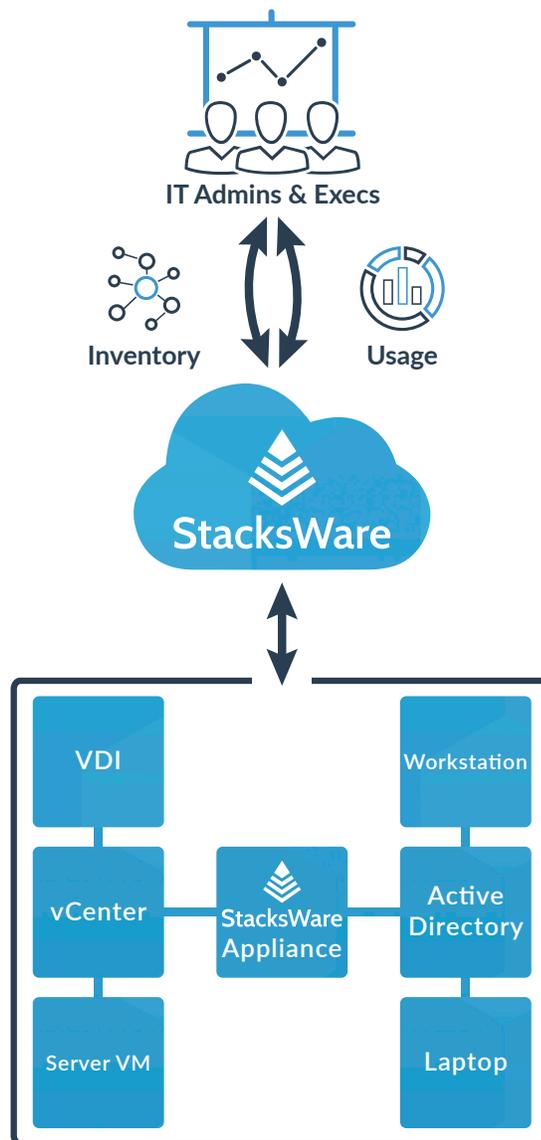
With that high-level explanation of the StacksWare infrastructure, let's drill into the specific security measures that StacksWare provides to protect your data.

Security First

Security should never be an afterthought. With attacks on enterprise organizations increasing each year, environments can lose precious IP, customer trust, and millions of dollars in operational expenditure.

As a SaaS offering with access to sensitive user information, StacksWare ensures that data is protected and secured across the hybrid cloud.

In this document, we detail StacksWare's best-in-class security features, trusted by Fortune 500 companies.



Internet Access

As illustrated from the previous diagram, StacksWare uses a lightweight connector to forward information from the datacenter to a dedicated private instance. Additionally, the connector sends requests to various services for updating and logging purposes. We have detailed each of these services below.

Docker Hub: Since our connector code is written for Docker microservices, StacksWare IM frequently sends download requests to Docker Hub for updates. These updates occur on a rolling basis to provide the best features and patches without the IT headache of redeploying a new virtual appliance.

Loggly: If errors in configuration occur, StacksWare IM pushes error message to Loggly, a popular and trusted logging service. This service allows us to rapidly respond to any issues in data collection that we find your environment.

To ensure data security, we've ensured that all requests to the Internet (i.e. to the private instance or the specified SaaS services) have the following characteristics:

1. All forwarded network traffic to the Internet is SSL encrypted, verified by certificate providers DigiCert, GoDaddy, or RapidSSL.
2. All requests between StacksWare IM and the Internet services are initiated inside the datacenter.



Data Security FAQs

We receive many questions about data storage, collection, and security. We answered the most common questions below.

Question

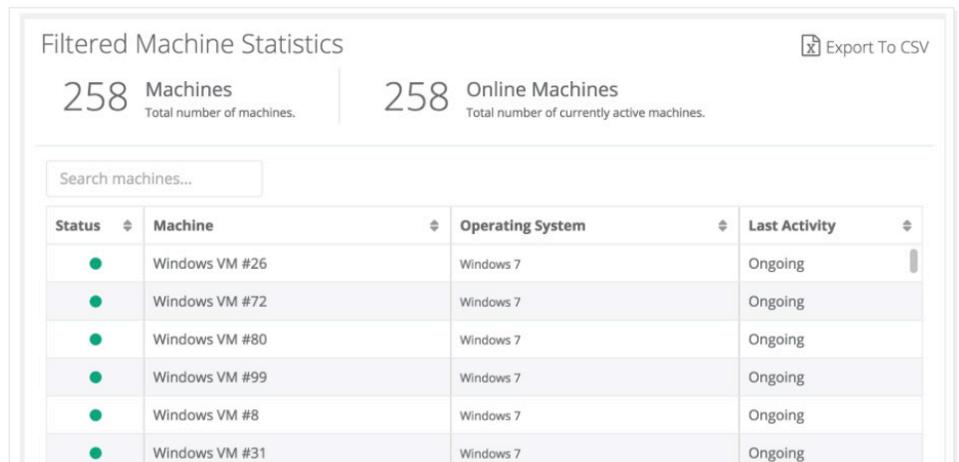
What data is collected?

Answer

StacksWare leverages VMware vSphere APIs to collect infrastructure and application metadata on all supported virtual machines.

Infrastructure Data

StacksWare collects operating system information, machines aliases, and CPU/memory/disk statistics on all virtual machines and underlying hardware.



Filtered Machine Statistics Export To CSV

258 Machines Total number of machines. | 258 Online Machines Total number of currently active machines.

Search machines...

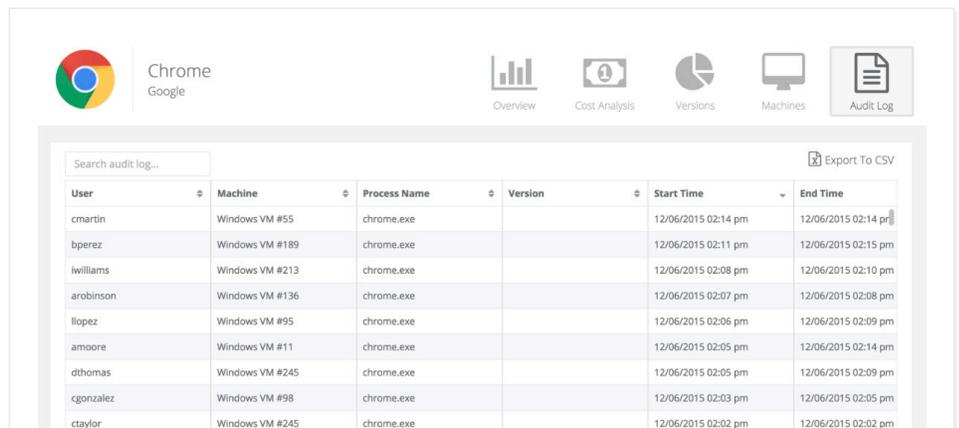
Status	Machine	Operating System	Last Activity
●	Windows VM #26	Windows 7	Ongoing
●	Windows VM #72	Windows 7	Ongoing
●	Windows VM #80	Windows 7	Ongoing
●	Windows VM #99	Windows 7	Ongoing
●	Windows VM #8	Windows 7	Ongoing
●	Windows VM #31	Windows 7	Ongoing

Example view of infrastructure data collected

Application Data

StacksWare collects running process and installed application information, along with their associated usernames.

Content data of desktop or server applications, such as Microsoft Word document information or Exchange Server email information, is not collected.



Chrome Google Overview Cost Analysis Versions Machines Audit Log

Search audit log... Export To CSV

User	Machine	Process Name	Version	Start Time	End Time
cmartin	Windows VM #55	chrome.exe		12/06/2015 02:14 pm	12/06/2015 02:14 pm
bperez	Windows VM #189	chrome.exe		12/06/2015 02:11 pm	12/06/2015 02:15 pm
williams	Windows VM #213	chrome.exe		12/06/2015 02:08 pm	12/06/2015 02:10 pm
arobinson	Windows VM #136	chrome.exe		12/06/2015 02:07 pm	12/06/2015 02:08 pm
llopez	Windows VM #95	chrome.exe		12/06/2015 02:06 pm	12/06/2015 02:09 pm
amoore	Windows VM #11	chrome.exe		12/06/2015 02:05 pm	12/06/2015 02:14 pm
dthomas	Windows VM #245	chrome.exe		12/06/2015 02:05 pm	12/06/2015 02:09 pm
cgonzalez	Windows VM #98	chrome.exe		12/06/2015 02:03 pm	12/06/2015 02:05 pm
ctaylor	Windows VM #245	chrome.exe		12/06/2015 02:02 pm	12/06/2015 02:02 pm

Example view of application data collected

Again: Sensitive information like document data *is not collected*.

Data Security

Question

Where is the data stored?

Answer

Data is stored in two different locations: the StacksWare IM in your datacenter and your virtual private instance.

On the StacksWare IM, we store your encrypted Active Directory and vCenter service account credentials (i.e. sensitive data); this information never leaves your datacenter.

On the virtual private instance, we store all infrastructure and application information in a dedicated virtual machine in Amazon Web Services EC2.

Question

How are service account credentials secured?

Answer

Service account credentials are encrypted and never leave the StacksWare IM in your datacenter. These credentials are secured on the virtual appliance filesystem using industry standard AES-256 encryption. The encryption key for this data is randomly generated and stored exclusively in your organization's virtual private instance. Under no condition is the encryption key written to the StacksWare IM filesystem.

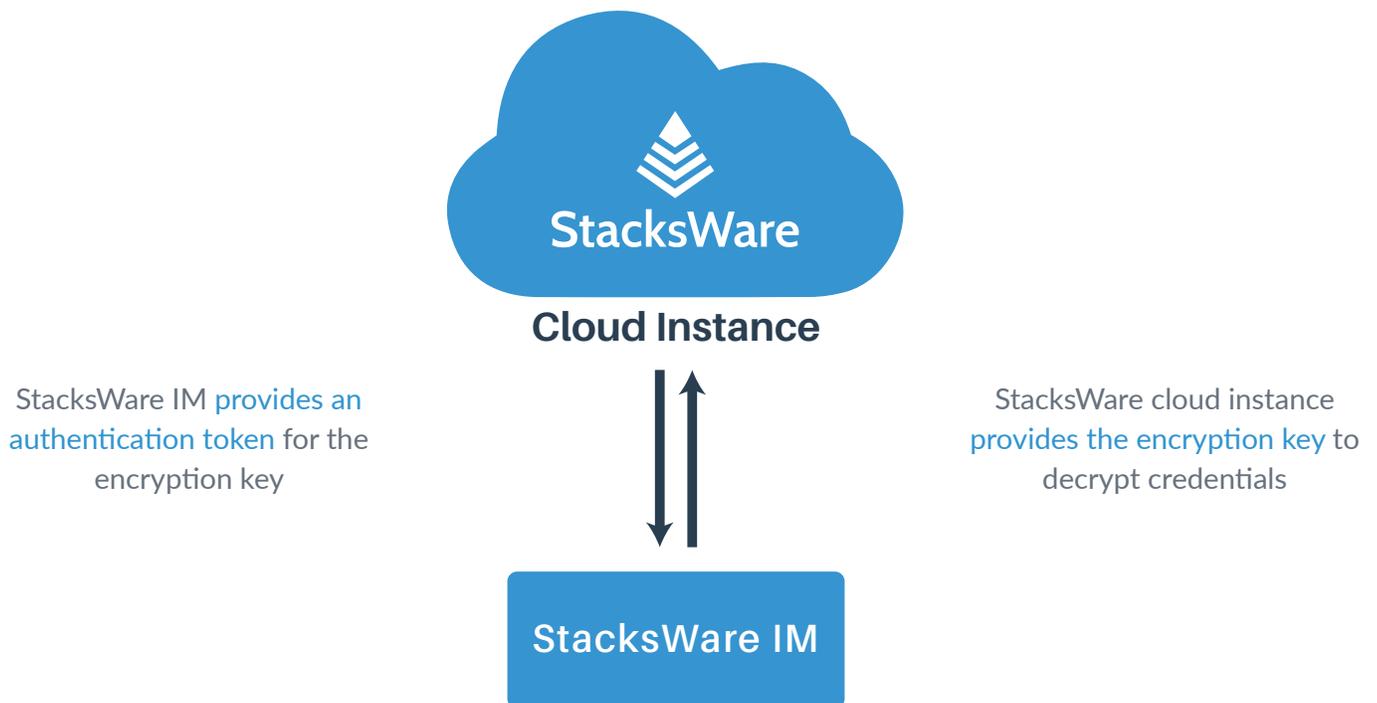
Data Security

Question

How is the encryption key retrieved?

Answer

The encryption key is retrieved from the private instance using an authentication token, which is stored in an obfuscated location on the StacksWare IM filesystem. The permissions for the token can be immediately revoked, if your enterprise environment is compromised. Please contact sales@stacksware.com if you want to revoke your authentication token.



Question

How secure is the virtual private instance?

Answer

Each time we onboard a new organization, we provision an entirely new virtual machine to ensure complete data isolation from other instances. All TCP and UDP ports on this private virtual instance, aside from 80 and 443, are inaccessible to the Internet. If you want to whitelist access to ports 80/443 to custom IP addresses (e.g. your enterprise or departmental modem IP), please contact sales@stacksware.com

About StacksWare

StacksWare Inc. is a Silicon-Valley based technology company committed to preventing enterprises from paying too much for software.

The StacksWare analysis platform was designed for the modern datacenter, and works to control the surging costs of operating a datacenter, making organizations less wasteful and more insightful. Within minutes of installing a simple drag-and-drop virtual appliance, StacksWare customers gain complete visibility into their software assets, and the ability to make immediate cost-reducing decisions.

Virtualization has enabled rapid growth in IT, resulting in enterprise technology that is more effective than ever before. Yet, few enterprises understand their software consumption. The few tools that can monitor software licensing today take months to deploy, resulting in massive capital expenditure and IT frustration.

At StacksWare, our mission is to develop a platform that extracts valuable insight from massive IT environments in minutes. We pride ourselves on shielding IT stakeholders from the complex models underpinning software license analysis, so that they only receive actionable insights that impact their jobs.



StacksWare

+1 855-655-3832

sales@stacksware.com

www.stacksware.com

StacksWare, and the StacksWare logo are registered trademarks of StacksWare, Inc. All other trademarks or service marks are the property of their respective holders and are hereby acknowledged. ©2016 StacksWare, Inc. All rights reserved.