Things Veeam ONE can tell you that you didn't know

Rick Vanover

RICKATRON

VMware vExpert | Microsoft MVP | Cisco Champion

@Veeam @RickVanover

Veeam ONE in a Tweet

Rick Vanover
@RickVanover

Rickatron quote of the day "I guarantee that Veeam ONE will tell you something about your environment that you didn't know, but need to fix"

12:51 AM - 13 May 2016

London, England

This complete visibility thing

An important sign of maturity to what is going on in the environment:

- VMware vSphere
- Microsoft Hyper-V
- vCloud Director
- **Veeam Backup & Replication**

Complete Visibility

Free Edition of Veeam ONE

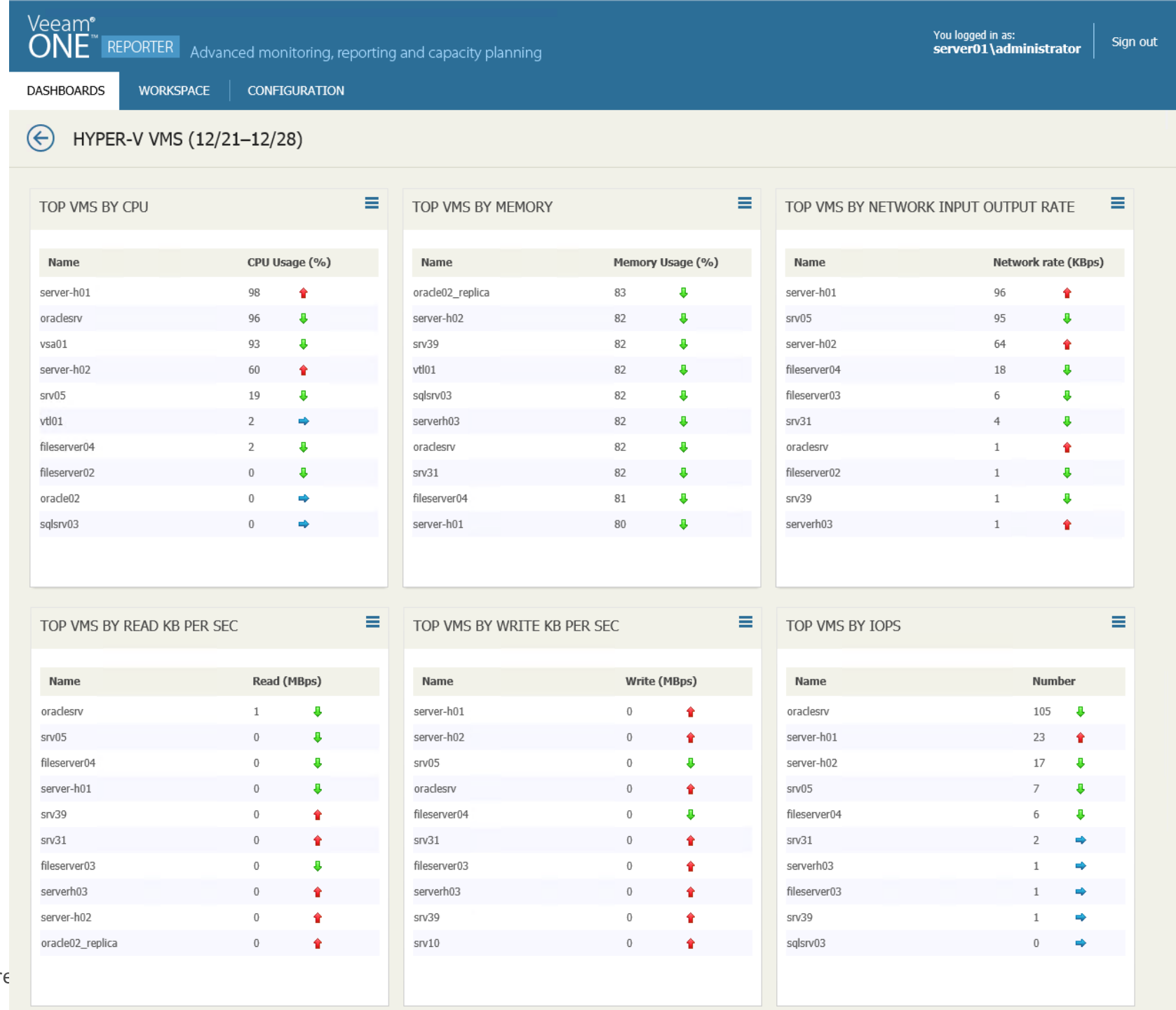
Has a few limitations but still quite usable

Feature	Free Edition Behavior
Data retention	24 hours
Reporting	1 saved report but none of the trending ones
Host inventory	Unlimited vSphere & Hyper-V but no Backup logic
Visio diagram	Free Edition limited to storage and configuration

Questions

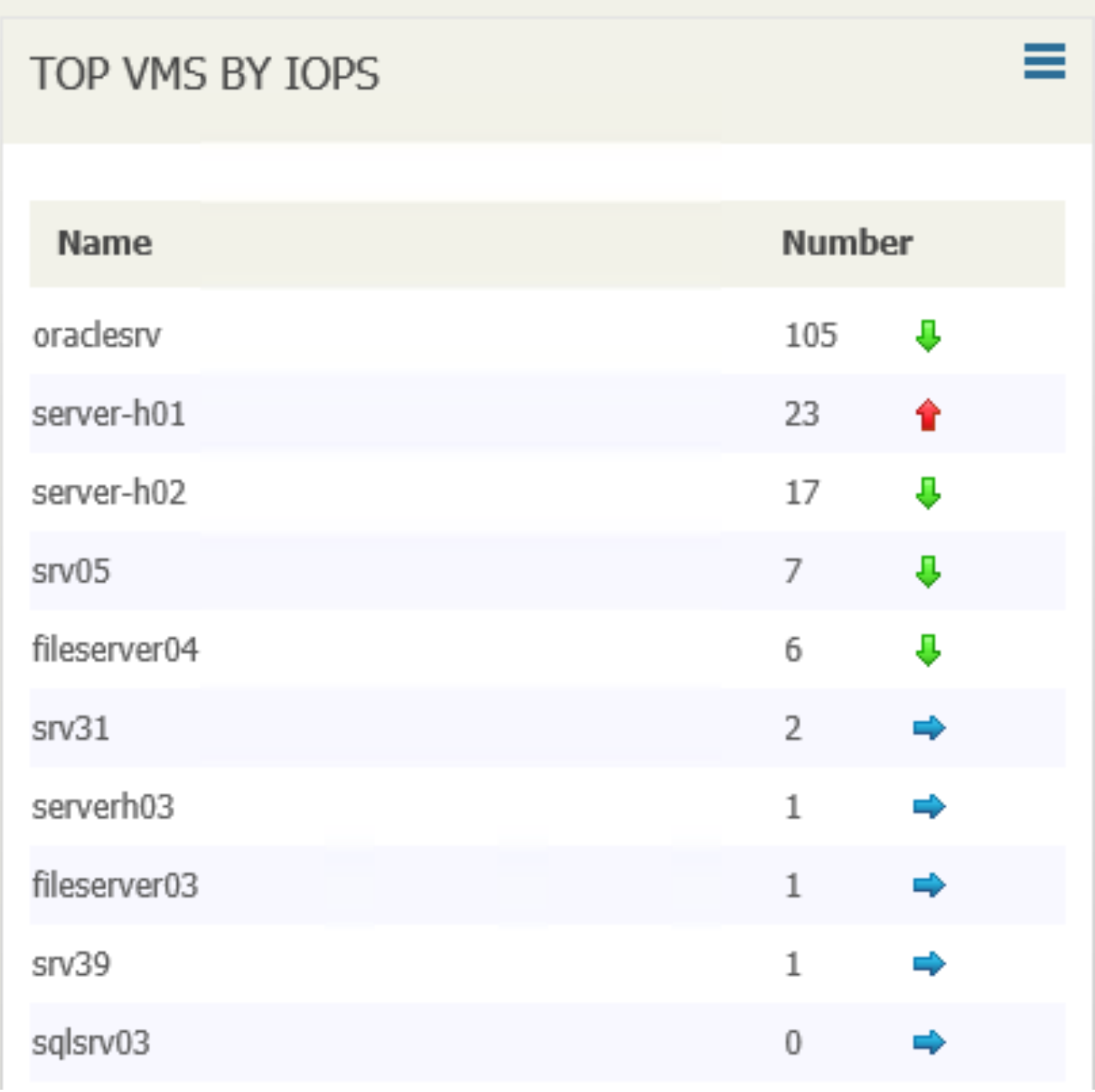
Can you tell how many IOPs are being consumed by each VM?

(Especially in Hyper-V)



More on IOPs

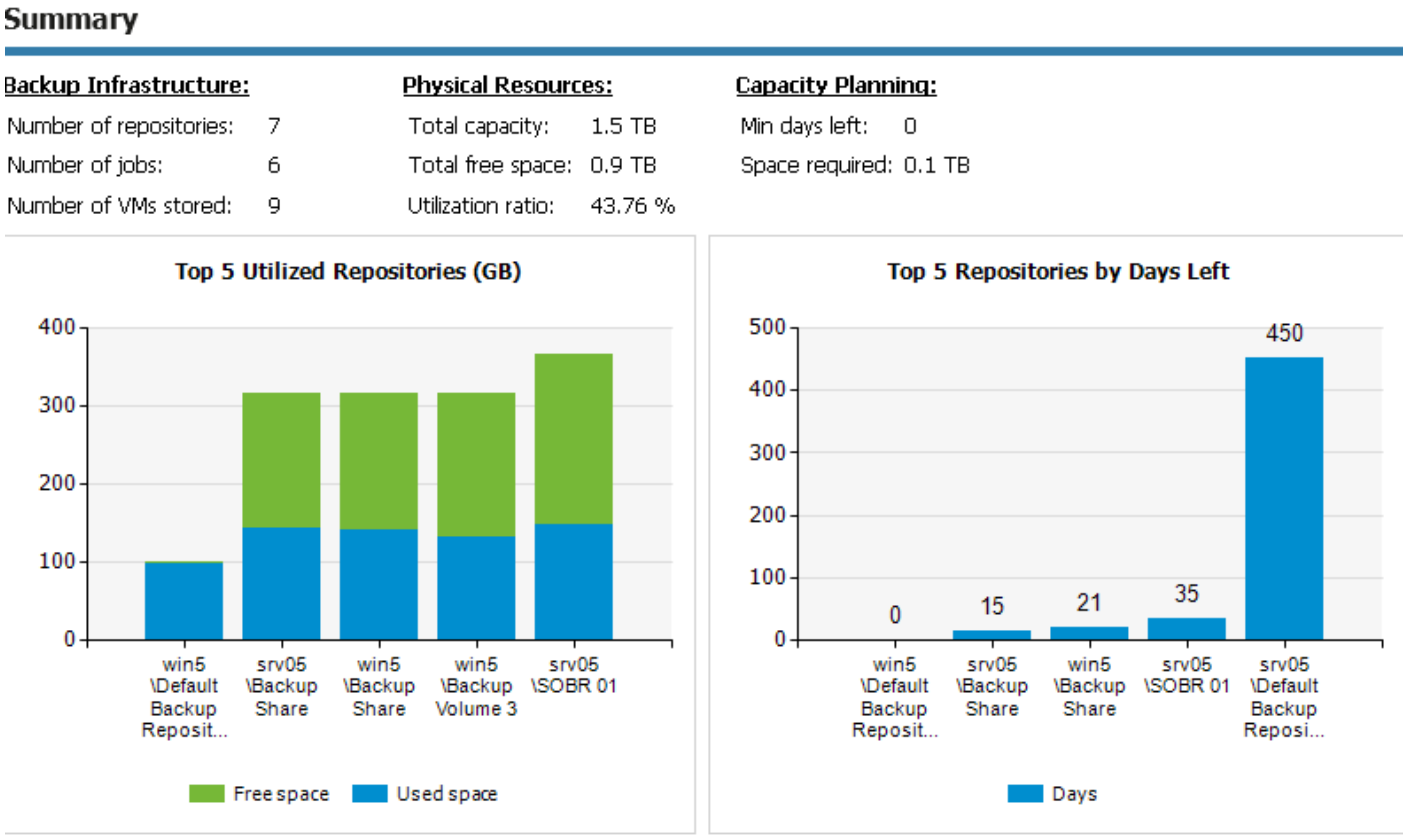
Important information!



More Questions

How much time is left on the backup storage?

Meet the report for
Capacity Planning
for Backup Repositories



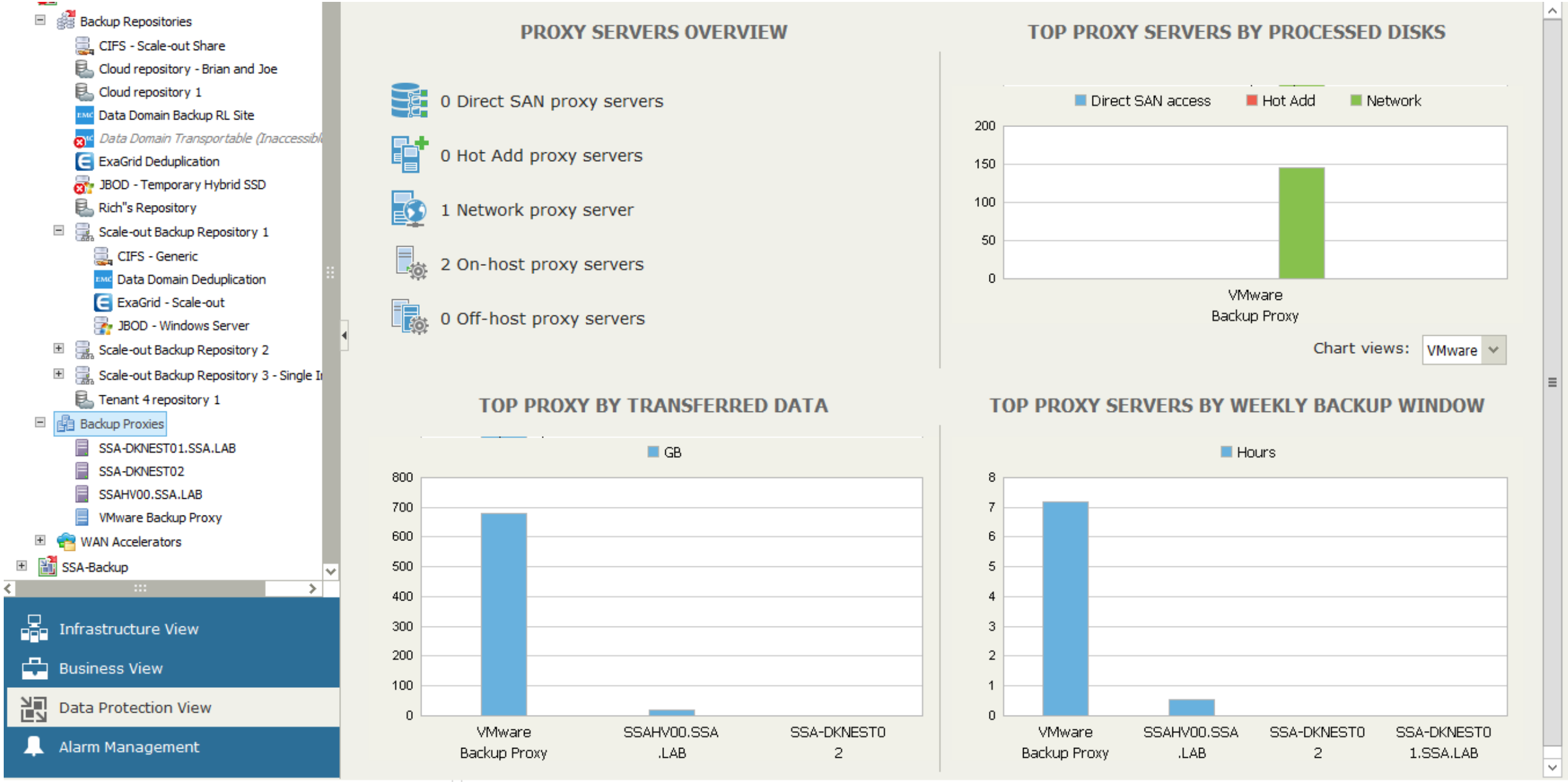
Another Question

Is my backup infrastructure operating as expected?

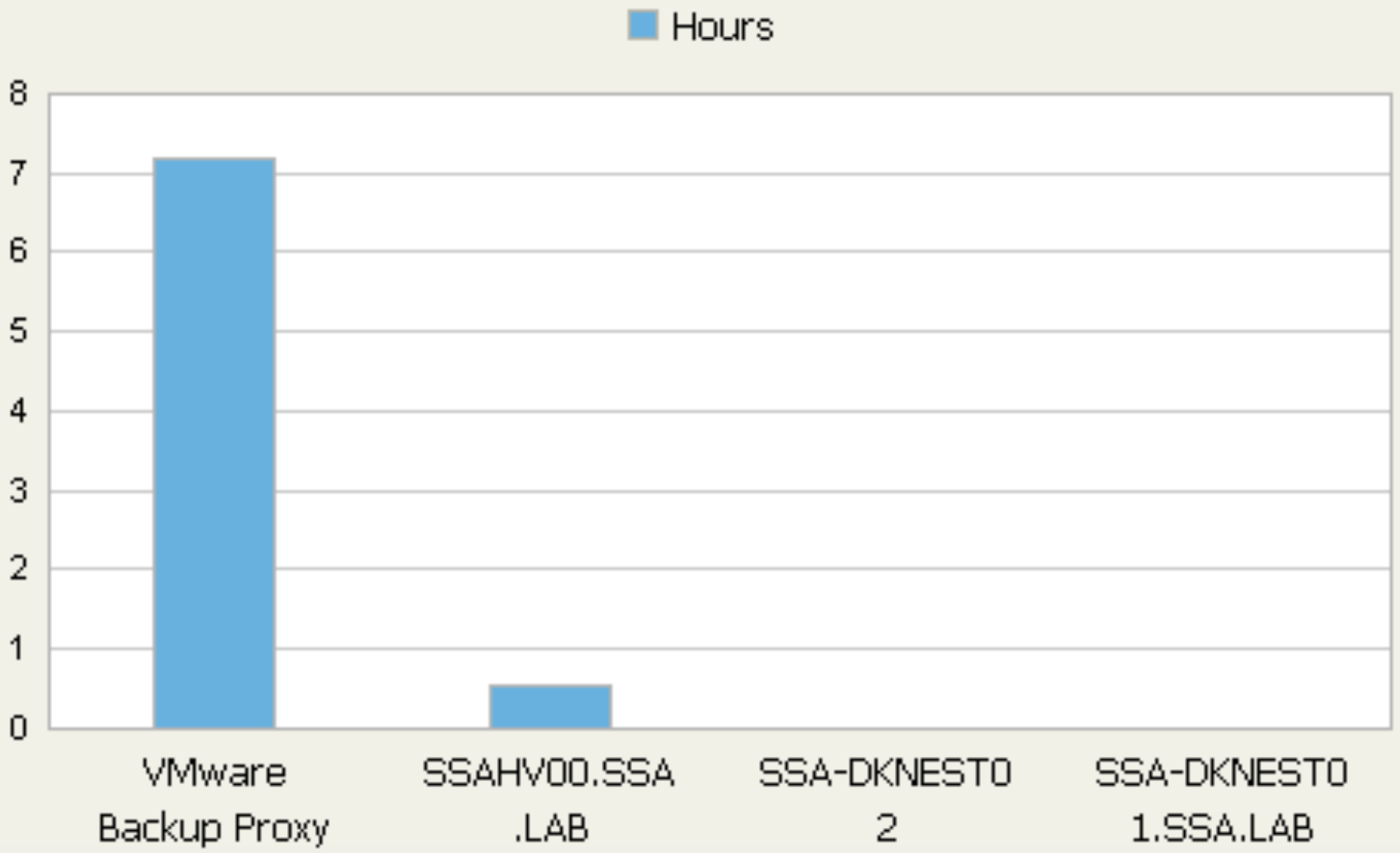
In particular, are the proxies moving as architected?

The Data Protection View is very helpful!

Bonus points: Run the **Unmapped Datastore LUNs** report to see what *can* run as Direct SAN access but isn't.



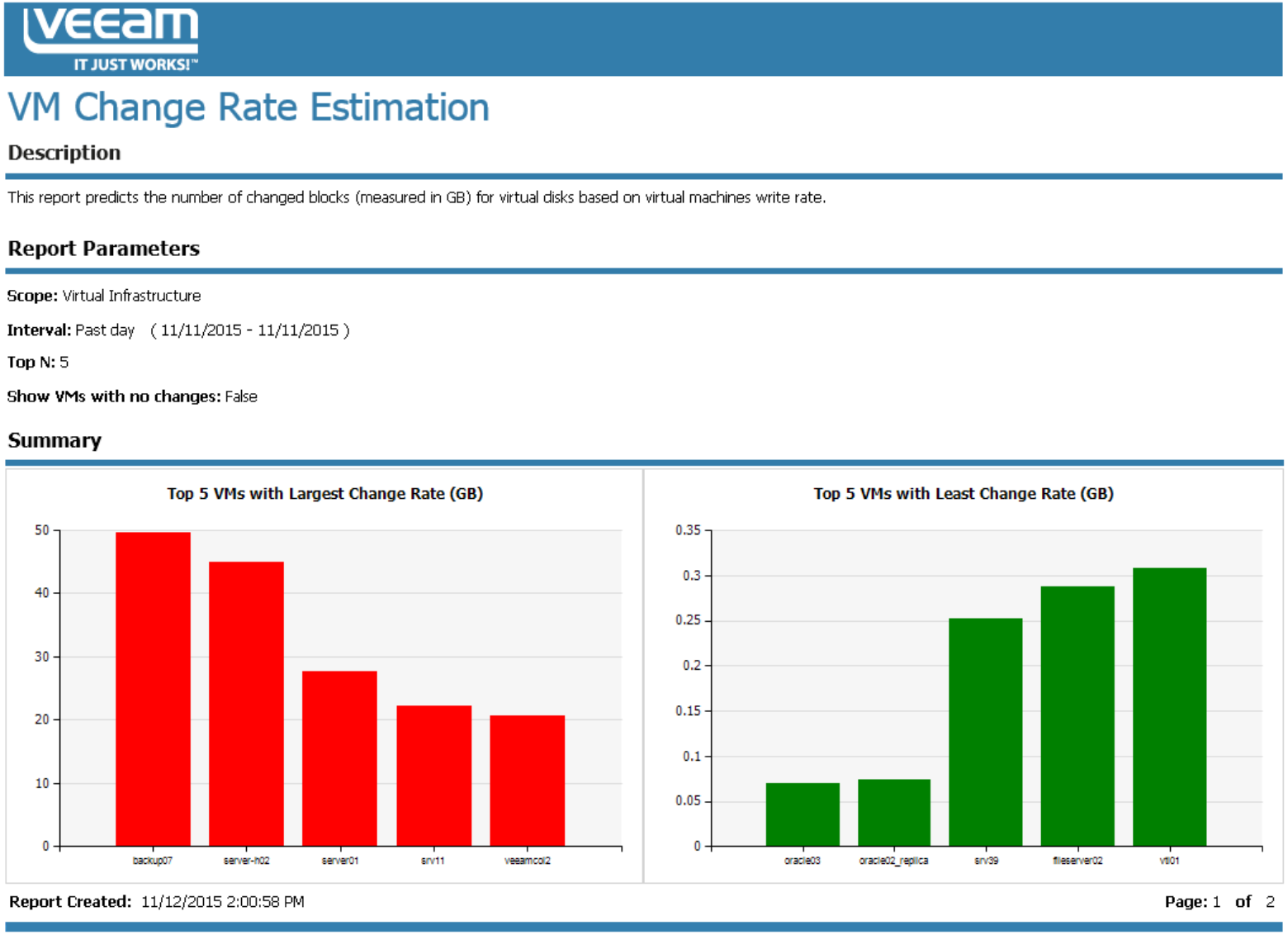
TOP PROXY SERVERS BY WEEKLY BACKUP WINDOW



Questions about storage

What VMs are changing the most and least.

Check the **VM Change Rate Estimation** report.



VEEAM
IT JUST WORKS!™

VM Change Rate Estimation

Description

This report predicts the number of changed blocks (measured in GB) for virtual disks based on virtual machines write rate.

Report Parameters

Scope: Virtual Infrastructure

Interval: Past day (11/11/2015 - 11/11/2015)

Top N: 5

Show VMs with no changes: False

Summary

Top 5 VMs with Largest Change Rate (GB)

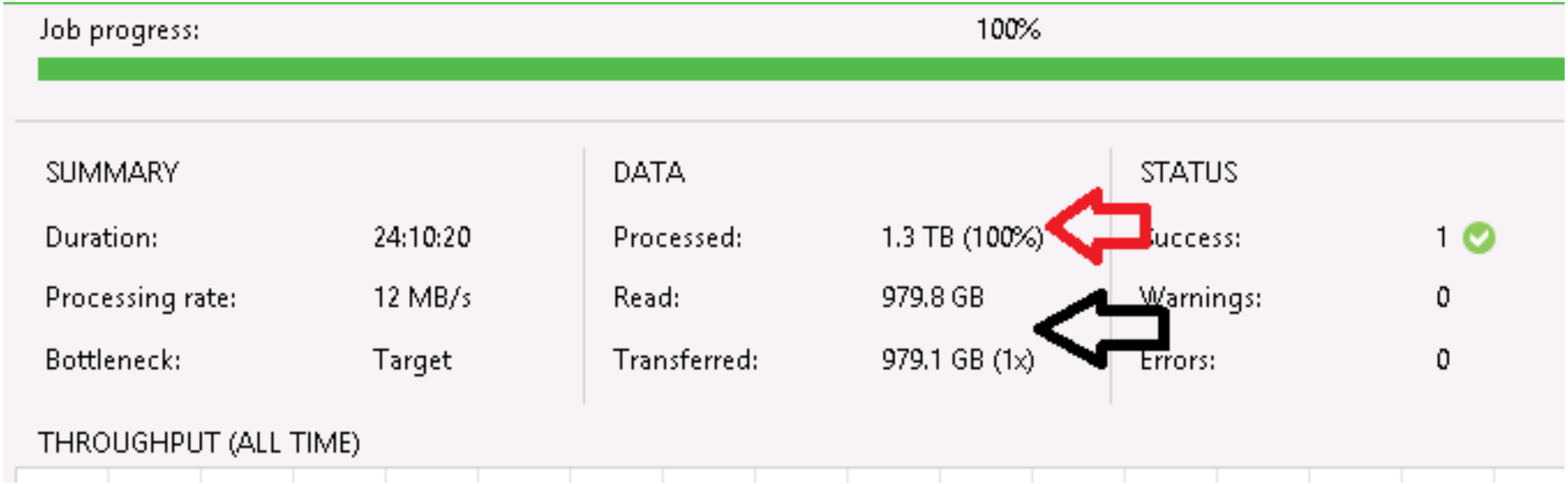
Top 5 VMs with Least Change Rate (GB)

Report Created: 11/12/2015 2:00:58 PM

Page: 1 **of** 2

Question… Can we fix that?

BitLooker!



Veeam ONE & this surface areas

Most security strategies are very clear and strong for running workloads and surface areas.

The data protection strategy has it's own surface area, and it usually incorporates the production systems and more.

Old mindset vs. Reality of today

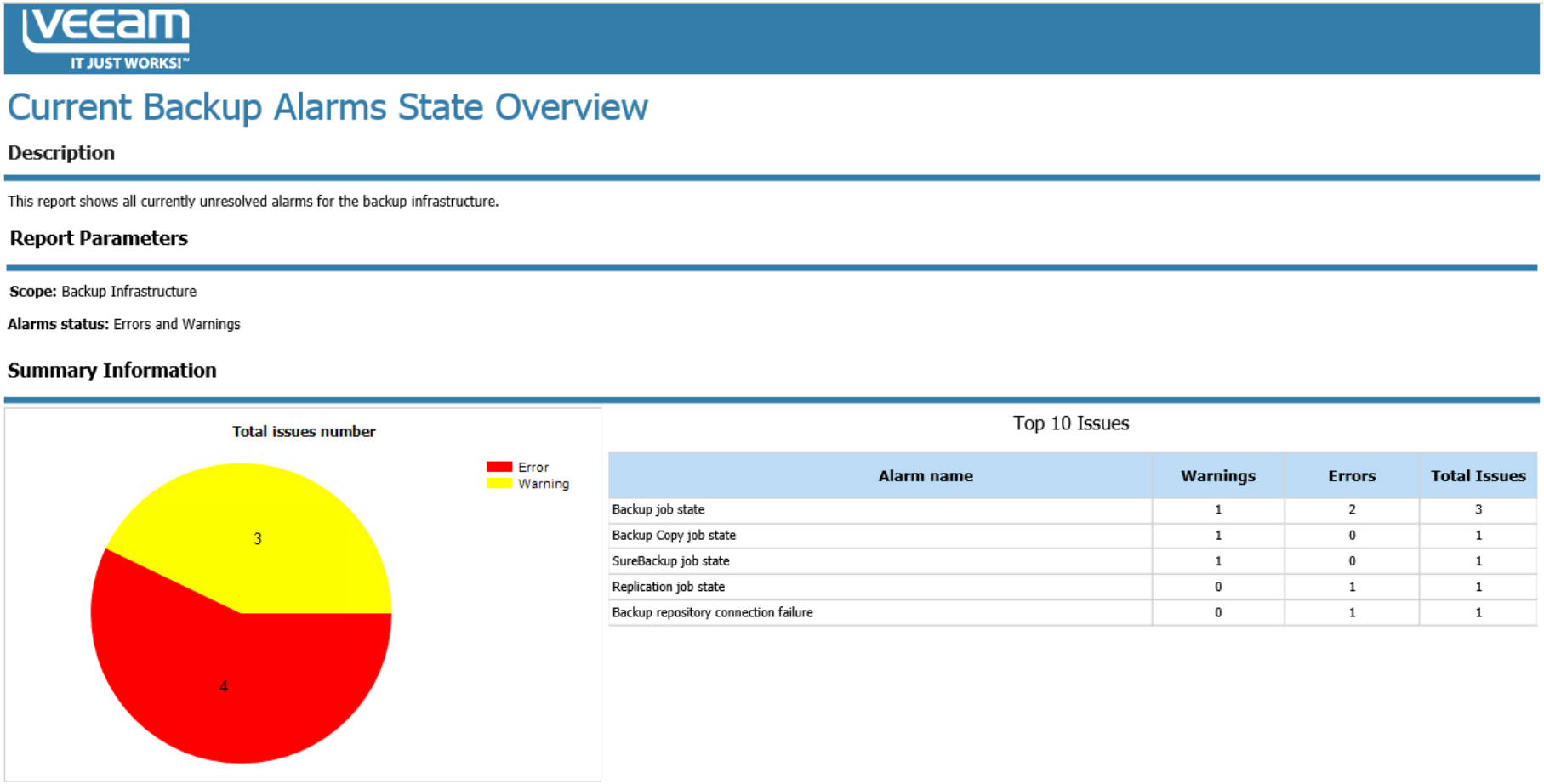
Another question…

In the Backup & Replication UI; what do you look for most:

- Successes **Green**
- Warnings **Yellow**
- Failures **Red**

There is even a report of Alarms

The Current Backup Alarms State Overview report



Current Backup Alarms State Overview

Description

This report shows all currently unresolved alarms for the backup infrastructure.

Report Parameters

Scope: Backup Infrastructure

Alarms status: Errors and Warnings

Summary Information

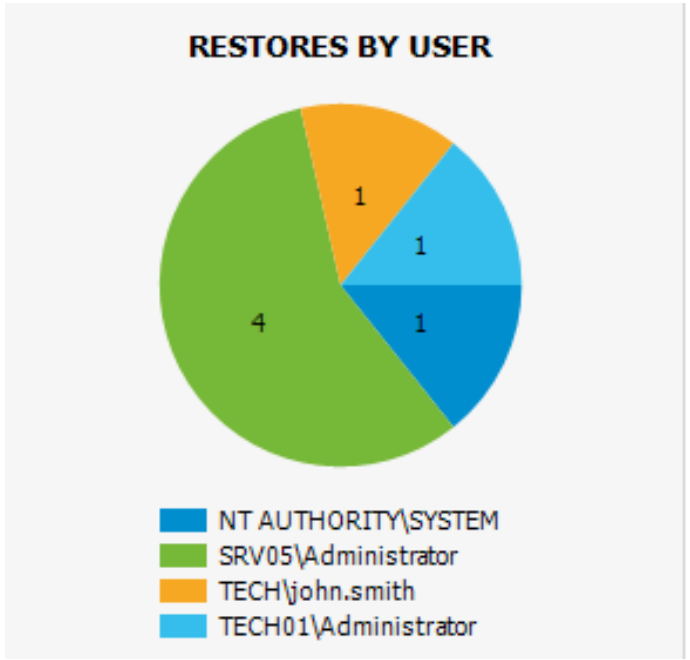
Top 10 Issues

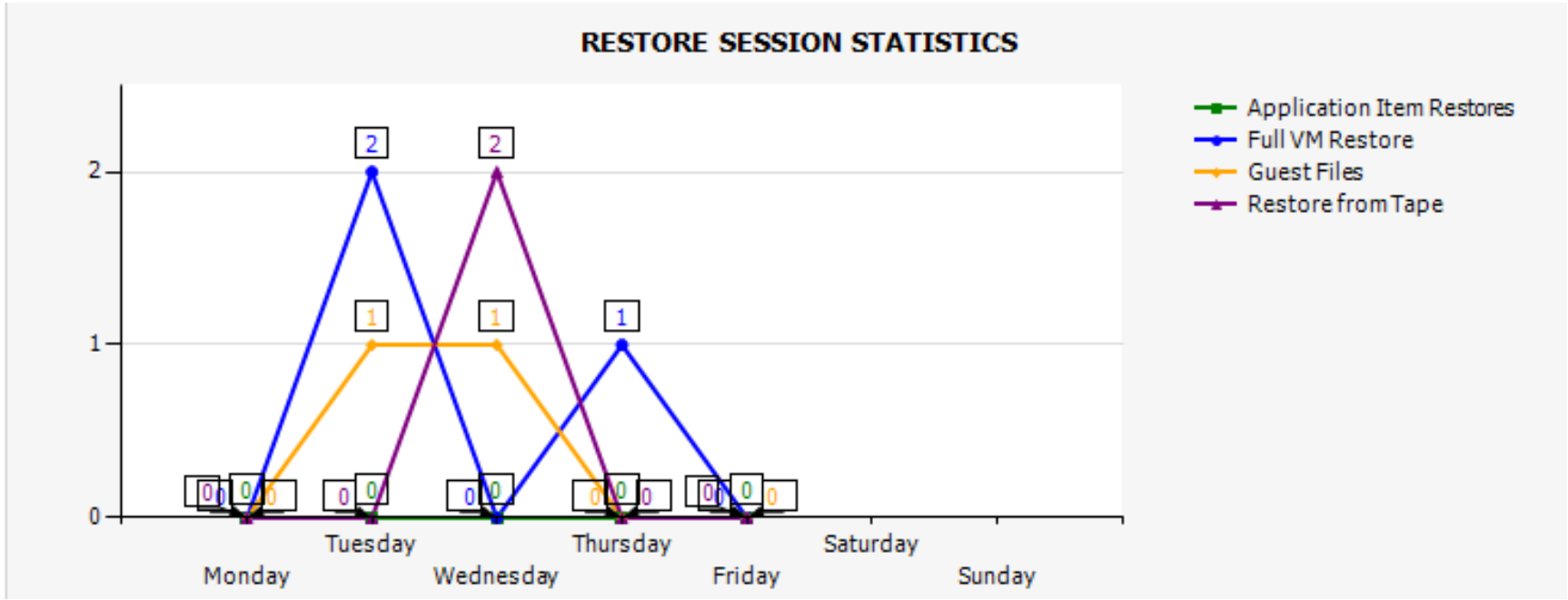
Alarm name	Warnings	Errors	Total Issues
Backup job state	1	2	3
Backup Copy job state	1	0	1
SureBackup job state	1	0	1
Replication job state	0	1	1
Backup repository connection failure	0	1	1

What about successful restores?

Are they authorized, expected, the right “type”?

I love the **Restore Operator Activity Report**





Things to look for and do

- Look for redirected FLR
- Ensure there are no *unplanned* backups
- Do automate critical reports AND have them emailed to supervising groups

Backup jobs visibility

Latest Backup Job Status report

Latest Backup Job Status

Description

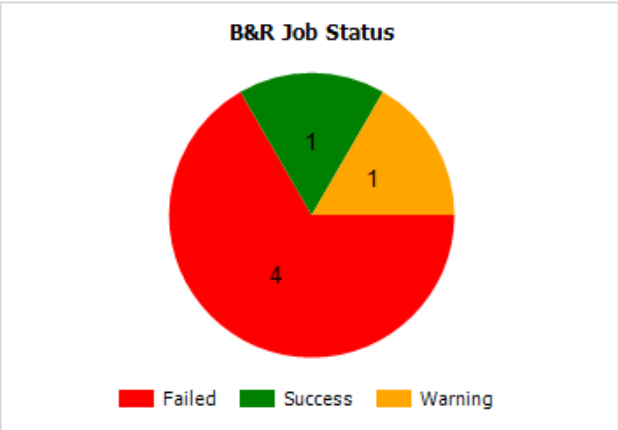
This report provides information about Veeam Backup & Replication jobs status.

Report Parameters

Scope: win5, srv05

Interval: Past Week

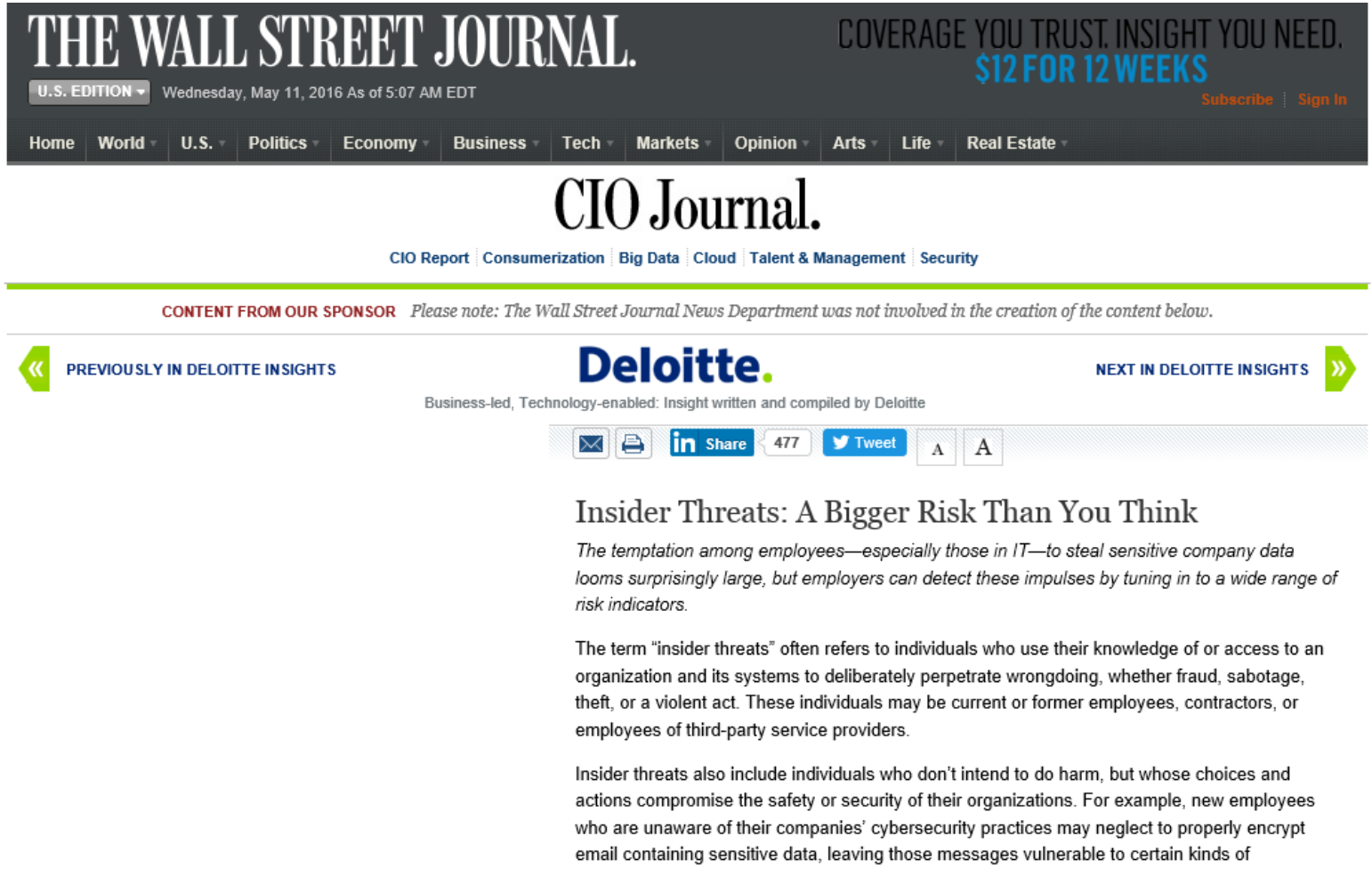
Summary Information



Top 10 Jobs by Duration				
Job Name	Duration (Last Run)	Transferred (GB)	Avg. Duration	Status
win5\SQL DB Backup	00:22:15	0.00	00:22:07	Failed
win5\VDI Replication	00:15:04	0.00	00:12:59	Failed
srv05\DB Backup	00:14:30	0.00	00:14:15	Failed
srv05\VDI Backup	00:14:24	0.00	00:14:11	Failed
srv05\Apache Backup	00:03:37	0.07	00:03:52	Success
win5\Oracle Backup	00:02:45	0.37	00:05:48	Warning

Insider Threats and Backup?

deloitte.wsj.com
http://vee.am/cATUHw



THE WALL STREET JOURNAL.

COVERAGE YOU TRUST. INSIGHT YOU NEED.
$12 FOR 12 WEEKS
Subscribe | Sign In

U.S. EDITION | Wednesday, May 11, 2016 As of 5:07 AM EDT

Home | World | U.S. | Politics | Economy | Business | Tech | Markets | Opinion | Arts | Life | Real Estate

CIO Journal.

CIO Report | Consumerization | Big Data | Cloud | Talent & Management | Security

CONTENT FROM OUR SPONSOR *Please note: The Wall Street Journal News Department was not involved in the creation of the content below.*

PREVIOUSLY IN DELOITTE INSIGHTS

Deloitte.

Business-led, Technology-enabled: Insight written and compiled by Deloitte

NEXT IN DELOITTE INSIGHTS

Share 477 Tweet A A

Insider Threats: A Bigger Risk Than You Think

The temptation among employees—especially those in IT—to steal sensitive company data looms surprisingly large, but employers can detect these impulses by tuning in to a wide range of risk indicators.

The term "insider threats" often refers to individuals who use their knowledge of or access to an organization and its systems to deliberately perpetrate wrongdoing, whether fraud, sabotage, theft, or a violent act. These individuals may be current or former employees, contractors, or employees of third-party service providers.

Insider threats also include individuals who don't intend to do harm, but whose choices and actions compromise the safety or security of their organizations. For example, new employees who are unaware of their companies' cybersecurity practices may neglect to properly encrypt email containing sensitive data, leaving those messages vulnerable to certain kinds of

The Widespread Risk of Insider Threats

97% of insider threat cases studied by Stanford University involved an employee whose behavior a supervisor had flagged, but that the organization had failed to follow up on.

92% of insider threat cases were preceded by a negative work event, such as a termination, demotion, or dispute with a supervisor.

90% of IT employees indicate that if they lost their jobs, they'd take sensitive company data with them.

59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them.

51% of employees involved in an insider threat incident had a history of violating IT security policies leading up to the incident.

25% of employees have used email to exfiltrate sensitive data from an organization.

Network Activity
- Excessively large downloads
- Access request denials

Compliance Cases
- Noncompliance with training requirements
- Policy violations

Data Exfiltration
- Spikes in outbound email traffic volume
- Attachments sent to suspicious recipients
- Removable media alerts

Time & Expense
- Expense violations
- Time entry violations

Access Attributes & Behaviors
- Access levels
- Security clearances
- Privileged user rights

Personnel Management
- Declining performance reviews
- Notice of resignation or termination
- Disciplinary action

deloitte.wsj.com

Source: "Insider threats: What every government agency should know and do," Deloitte Dbriefs, March 2016.

Physical Security
- Physical access request denials
- Physical access anomalies

External Data
- Social media posts
- Financial duress
- Criminal/civil history
- Foreign contacts/travel

Some statistics & characteristics

59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them.

90% of IT employees indicate that if they lost their jobs, they'd take sensitive company data with them.

25% of employees have used email to exfiltrate sensitive data from an organization.

Data Exfiltration

- Spikes in outbound email traffic volume
- Attachments sent to suspicious recipients
- Removable media alerts

Access Attributes & Behaviors

- Access levels
- Security clearances
- Privileged user rights