Introduction
Application owners expect their services to be always available, with no downtime and without any data ever lost regardless of system failure. With modern data protection, this goal can be achieved. However, the ease of cloning virtual machines and the growing number of virtualized applications businesses running today compound the problem of keeping track of which virtual machines have been protected and which have not.

Solution
The Cisco Tetration Analytics™ solution monitors end-to-end data center traffic and automatically identifies virtualized workloads. By integrating Cisco Tetration Analytics with Veeam Backup and Replication (B&R), data protection and compliance operations staff can easily identify which virtual machines have been backed up and which have not.

Use case
You can use Cisco Tetration Analytics to identify endpoints in a data center that are communicating with Veeam and endpoints that aren’t communicating with Veeam. You can then merge the discovered application dependencies with Veeam data to calculate the percentage of virtual machines and hosts that have backup and data protection. You can present the Veeam administrator with a backup-deficit view, or a list of virtual machines that aren’t backed up. Using this identified application access anomaly information, Veeam can take remedial action, issuing an unprotected virtual machine alert to the storage or backup administrator by email.

Solution details
Set up the environment with the following components:
- Veeam Backup and Replication Release 9.5 Update 2
- Veeam Enterprise Manager Release 9.5, using web API for programming integration
- Veeam Backup and Replication Enterprise Plus license installed
- One or more existing virtual machine in the VMware ESXi environment
- One backup job created for those virtual machines with several restore points
Table 1 lists the virtual machine resources required. These resources are expected. They can be adjusted after installation.

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>Cores</th>
<th>RAM</th>
<th>Disk</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam server</td>
<td>8</td>
<td>8 GB</td>
<td>60 GB plus 300 GB for repository</td>
<td>SRV 2016</td>
</tr>
<tr>
<td>(Enterprise Backup Manager run on same server)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Benefits**

Using the open APIs available with both Cisco Tetration Analytics and Veeam B&R, Cisco and Veeam developed an initial integration to prove the ease with which Cisco Tetration Analytics can monitor and notify staff of potential risks. Operations staff can easily see which virtual machines are not being protected and are therefore at risk of potential data loss in the event of a failure. This initial integration can be extended to enforce compliance rules and to identify impending security risks and orchestrate a backup operation before data is compromised.

**Conclusion**

Cisco Tetration Analytics offers powerful and ubiquitous visibility into all traffic in the environment, and Veeam offers a leading data protection solution used by more than 250,000 customers. These two foundational products can be integrated with ease to keep your data center running and protect it from compromise and loss.

**For more information**