COMMVAULT

SOLUTION BRIEF

Improving Risk Management With the Commvault Security Health Assessment Dashboard

Ransomware attacks have increased in sophistication. Cyberattackers pressure organizations by threatening to publish the sensitive data information they have hijacked, known as double extortion.[1] And, bad actors are taking their cyberattacks one step further by demanding ransomware from third-party victims, such as company clients, external colleagues, and service providers – a tactic known as triple extortion.[2] Since cyberattackers continue to expand and evolve, organizations must reevaluate their security posture and define processes and controls to ensure systems and data remain secure and resilient. A systematic approach or framework is the best way to reduce the complexity and help organizations focus on the most impactful security changes.

Commvault's Security Health Assessment Dashboard offers a single pane of glass to identify, monitor, and mitigate risks within the Commvault data protection and management environment. It applies principles of industry-leading risk management frameworks (see Figure 1) to help organizations reduce the attack surface and strengthen their security posture. Most importantly, it helps organizations prioritize and correct high-impact security gaps.

Figure 1: Risk Management Framework

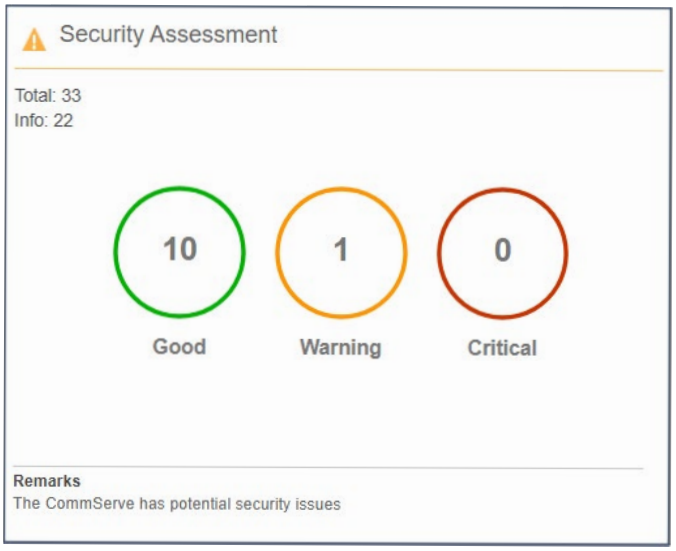

Figure 2: Commvault Security Assessment tile

So what is Commvault's Security Health Assessment Dashboard? This dashboard is available within the Commvault Command Center™ health report.[3] A cloud version is also available to organizations that track CommCell health in the Commvault cloud. Changes to security controls appear daily on the health report to provide continuous monitoring.

You can view the Command Center Dashboard's health report in the Security Assessment tile, Figure 2.

1 Brooke Crothers, February 23, 2022, Venafi, Venafi Survey: Ransomware Evolves—Double and Triple Extortion Now Features in Over 80% of Ransom Demands; https://www.venafi.com/blog/venafi-survey-ransomware-evolves-double-and-triple-extortion-now-features-over-80-ransom.
2 Checkpoint Research, The New Ransomware Threat: Triple Extortion, https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple- extortion/.
3 Available on Feature Release 11.20 and above.

Simplifying risk management

The Security Health Assessment Dashboard allows organizations to Identify, Assess, Mitigate, and Monitor security controls within the Commvault data protection environment (see Figure 3). By design, the dashboard identifies controls available in the Commvault CommCell and provides scoring and remarks to allow organizations to assess the risk properly and continuously monitor security posture.

Not every control fits all organizations. For example, some organizations may use external identity providers with built-in multi-factor controls and password complexity logic. While others may rely on local Commvault accounts to segment access from their primary environment. Either way, the dashboard will provide insights to take the appropriate actions.

To **mitigate** risks, follow the action items for the specific control. Actions range from targeted documentation and more in-depth reports to workflows and software store applications and tools. Applying solutions is simplified and streamlined within the single pane of glass to minimize jumping between the interface windows.

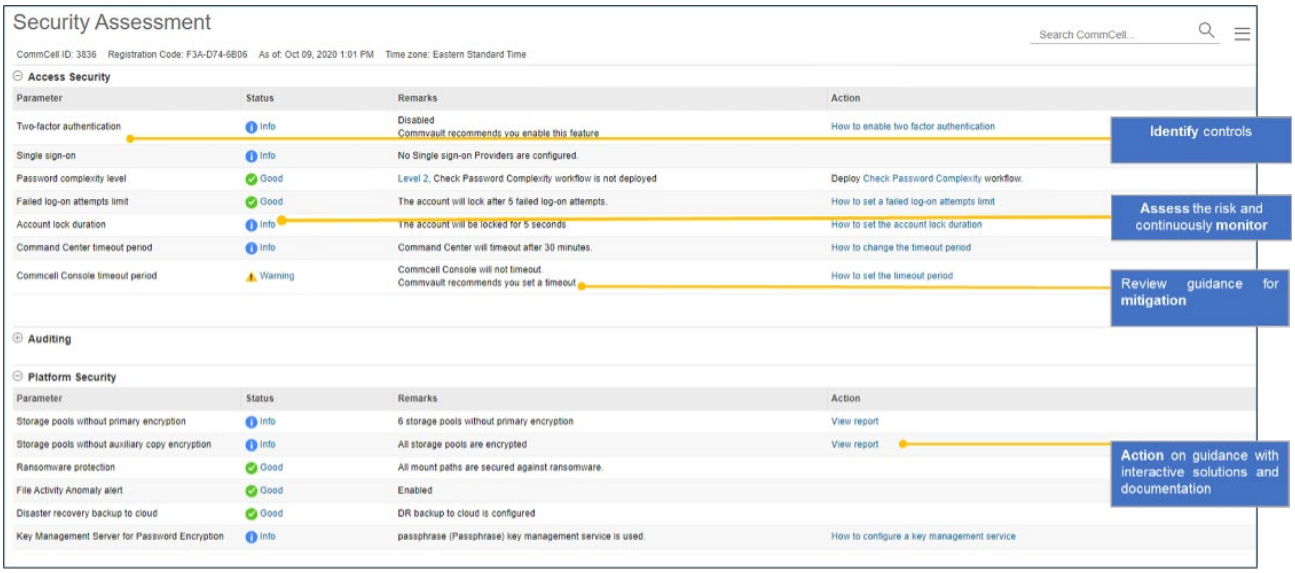

Figure 3: Security Assessment Dashboard

To demonstrate how simple and powerfully interactive this solution is, let's use ransomware protection as an example below.

1. You may see "Ransomware protection" as Critical if data movers (MediaAgents) are not appropriately configured on the dashboard.
2. Click the Enable Protection action in the report to view more details as to what MediaAgents are not protected.
3. At that point, protection can be enabled globally or individually to each MediaAgent without leaving the interface.

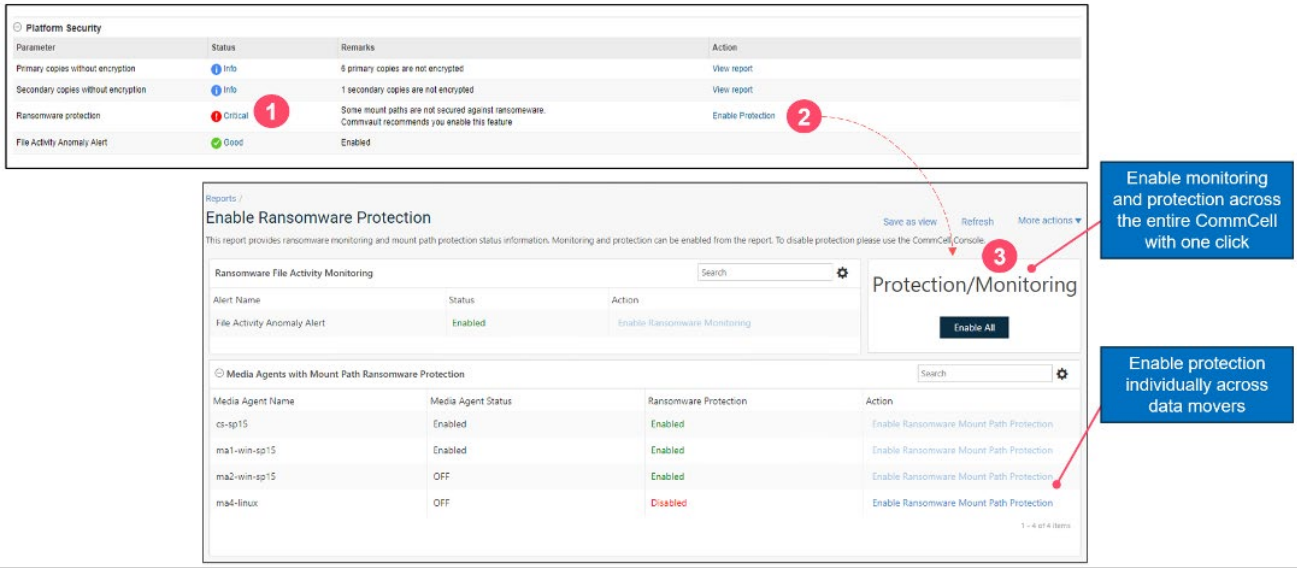

Figure 4: Enabling Ransomware Protection

Zero Trust AAA security controls

Many Security Health Assessment Dashboard controls are part of Commvault's Zero Trust AAA (Authentication, Authorization, Audit) security control framework. Protecting user access levels while auditing events is vital for proper security posture. Building these controls around Zero Trust principles ensures that trust is continuously validated – not just assumed. Home security provides a great example of what zero trust looks like. Our home is our safe zone. We lock the doors and windows, add cameras to monitor in and around our homes, and add alarms and sensors to monitor threats. When we invite guests into our home, we allow our guests a level of access to our safe zone; however, that does not authorize them to read our mail and view our personal information. For this reason, homeowners have locks on their bedroom doors or use safes and lockboxes to keep personal items protected.

Commvault provides controls in the Security Assessment Dashboard that apply zero trust principles. For example, company and owner security features keep data private, segmented, and compartmentalized. The backup administrator should not have access to sensitive corporate data. Enabling privacy locks to keep data locked and private ensures only the data owners can browse and restore the contents while backup administrators can manage backup operations.

Commvault also provides multiple layers of authentication controls to stop malicious actors, insider threats, and even unintentional accidents from deleting backup data. Regardless of your user role within the CommCell, multi-factor controls restrict and block potentially dangerous actions and require elevated authorization every step of the way.

Lastly, the Security Health Assessment Dashboard provides continuous awareness when locks, alerts, and controls are not applied or disabled. This includes any new feature sets that become available in the future that Commvault may recommend.

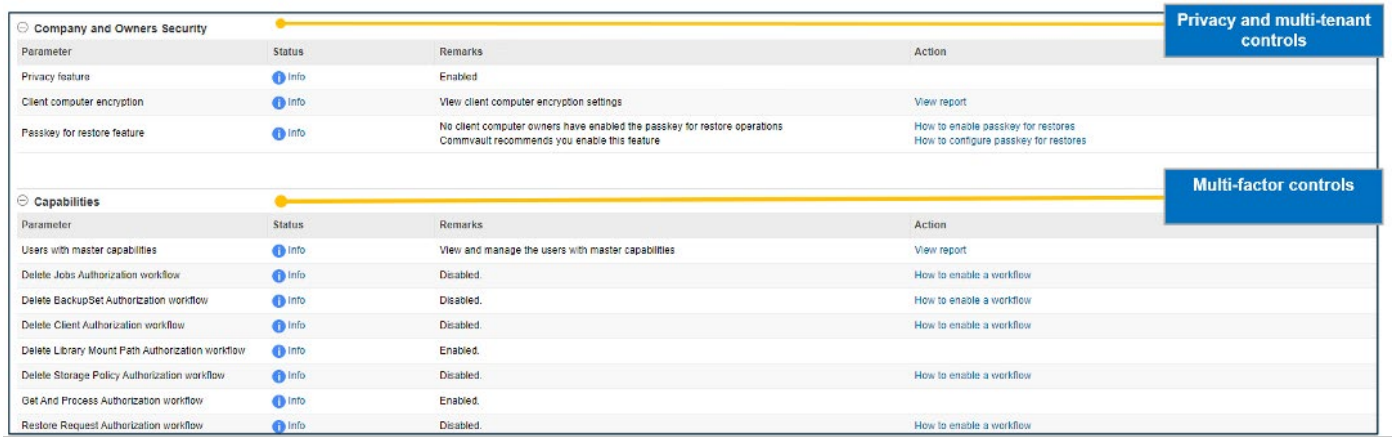

Figure 5: Implementing Multi-tenant and Factor Controls

Conclusion

The Security Health Assessment Dashboard is the starting point for improving security posture within the Commvault data protection and management environment. With its single pane of glass, the ability to automatically provide insights/best practices, and intuitive interactive actions, the dashboard simplifies the complexity of implementing and managing security. To see the dashboard in action, view this Commvault video.

Learn more about Commvault ransomware protection and recovery commvault.com/ransomware >