DELL Technologies

Datasheet

ECS Cyber Protection Solution for Object Data

Cyber attacks have become a serious and continuous threat to businesses of all sizes and verticals. A cyber attack is happening every 11 seconds[1] and the average cost of one is $13M[2] and growing. Cyber attacks disrupt operations, damage reputation and can result in law suits related to data protection regulations. While 100% immunity is not practical, IT Organizations can do a lot to significantly improve the cyber resiliency of the systems to protect business-critical data and setup systems for faster recovery of business operations.

In this overview learn what makes Dell ECS Cyber Protection Solution world's most cyber-secure object storage.[3]

August 2022

References:

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[2] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[3] Based on Dell analysis comparing cybersecurity software capabilities offered for Dell ECS vs competitve products, September 2022.

Object data is the new frontier for cyber attacks

Object data can be the next frontier for cyber attackers. In addition to the rapidly growing modern applications that require object stores,a lot of backup data and legal compliance data also uses object storage. Application servers often store the authentication keys on disk making these application hosts obvious targets of attack. To go after this object data all the attackers need is a secret key and a few lines of Python code to gain access to petabytes of data. What makes it worse is the fact that no security tools are monitoring access to object data which makes these attacks go undetected. Dell Technologies in collaboration with Superna is bringing comprehensive zero-trust capabilities to isolate, detect, protect and recover Object storage from cyber attacks.

Cyber attacks happen every

11 seconds[1]

Average cost of a cyber attack for US Federal agencies is estimated to be

$13.7M[2]

Isolate with smart air-gap technology

A robust cyber resiliency strategy involves using all the best practices involved in protecting data: right level of access controls, immutable copies of data, anti-virus and anti-malware. In addition to these capabilities, Ransomware Defender offers the protection of last resort, which is a copy of the data in a cyber vault that is isolated from the production environment. After the initial replication of data to the cyber vault, an air-gap is maintained between the production environment and the vault copy. Any further incremental replication is done only intermittently by closing the airgap after ensuring there are no known events that indicate a security breach on the production site.

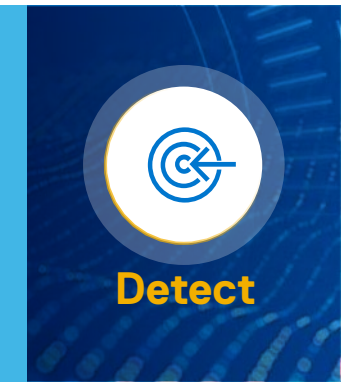
Production Site

Cyber Recovery Vault

References:

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[2] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study



Detect: Real-time detection of suspicious data access activity

Detection and early response is an essential part of any cyber security framework. Ransomware Defender for Dell PowerScale has rapidly become an indispensable tool for IT and Security teams to protect petabytes of business-critical File data with the ability to detect, protect and rapidly recover from Ransomware attacks. Dell Technologies in collaboration with Superna is now bringing this technology to Object storage as an industry first. Eyeglass Ransomware Defender for Dell ECS offers the industry's only S3-native real time data protection by providing customers comprehensive capabilities to detect attack events in realtime. Behavior based analysis of object data access enables zero-trust protection of object data.

Learning mode

Artificial Intelligence and Machine learning are key technologies used in cyber security. Ransomware Defender comes with Learning Mode that can help establish a base line of safe access that may vary from application to application. Over time the system gets more accurate at detecting suspicious data access behavior and minimize false positives.

Application Whitelisting

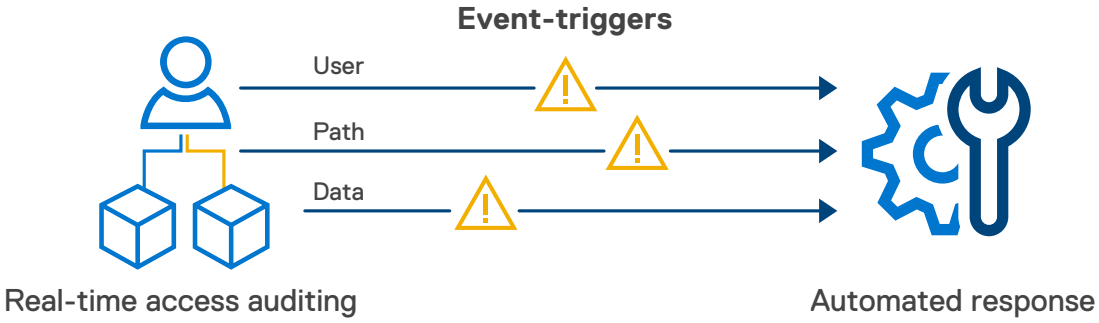
Whitelisting is a key component of a zerotrust based approach where a verified list of applications and and network configurations are allowed exclusive access to data. Ransomware Defender allows the security administrators to keep a list of object buckets, user accounts, server IP addresses that are allowed access to certain object data.

Automated Response

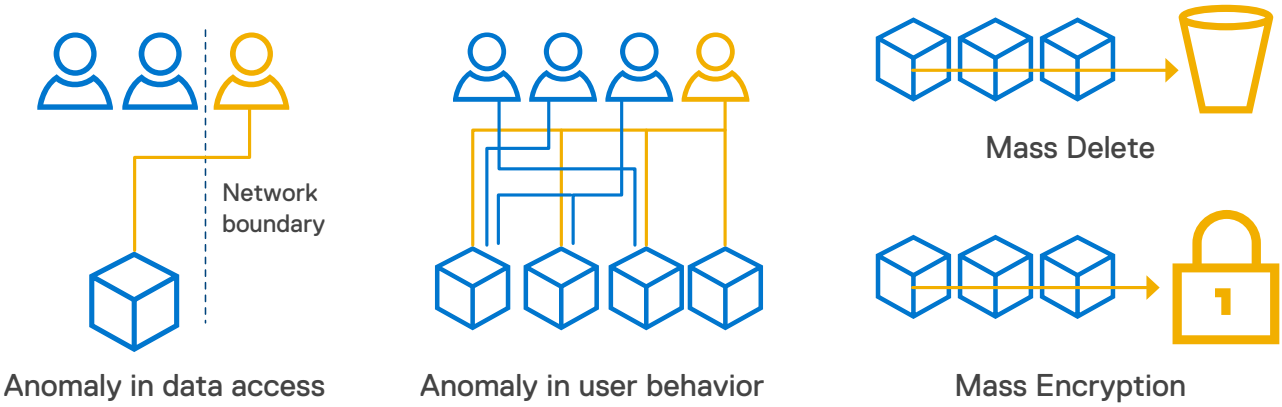
Ransomware Defender offers a range of options to respond to attack events. Administrators are alerted of unusual data access behaviors. The system can be configured to allow a wide range of automated responses from monitor only to immediate user lockout. API Integration with ECS allows access keys to be revoked to stop the attack and speeds up data recovery by tracking compromised objects for administrators to recover from previous versions, using ECS object versioning.

Penetration testing with Security Guard

Penetration testing is a best practice when it comes to check the defenses that are setup against cyber attacks. Ransomware Defender offers automated penetration testing that ensures defenses are operational. Penetration test logs allow administrators to easily see the health of security defenses and generate alerts for failed penetration tests.



Example patterns that can be detected



Operational and Data Recovery

Recovering from a cyber-attack involves identifying the compromised data, users accounts and client IPs where the attack originated. Ransomware Defender provides this information so that admins can quarantine infected object stores and namespaces. Ransomware Defender provides a list of compromised object data and S3 buckets that allows precise data recovery. This accelerates the recovery time to get systems back up and running, while also providing a post mortem sequence of events that allows security gaps to be addressed to harden the environment from future attacks. With the S3-compliant versioning of ECS, a known good version of object data can be used to restore affected data.

Intrinsic S3-compliant security features of ECS

1. S3 Object lock for ECS

Dell EMC ECS supported WORM (write once, read many) based retention, starting with ECS 2.X. To provide more compatibility with more applications, ECS now supports the object lock feature (starting with ECS 3.6.2), which is compatible with the capabilities of Amazon S3 object lock. Object lock is also designed to meet compliance requirements such as SEC 17a4(f), FINRA Rule 4511(c), and CFTC Rule 17.

Object lock prevents object version deletion during a user-defined retention period. Immutable S3 objects are protected using bucket-level configuration of WORM and retention attributes. The retention policy is defined using the S3 API or bucket-level defaults. Objects are locked for the duration of the retention period, and legal hold scenarios are also supported.

Click here to learn more about ECS Object lock

2. S3 identity and access management

ECS Identity and Access Management (IAM) enables you to have fine-grained access to the ECS S3 resources securely. This functionality ensures that each access request to an ECS resource is identified, authenticated, and authorized. ECS IAM allows you to add users, roles, and groups. You can also grant and restrict the access by adding policies to the ECS IAM entities.

Click here to learn more about ECS IAM

3. S3 versioning

S3 Versioning on ECS enables you to keep multiple variations of an object in the same bucket to protect the data and enable rapid recovery in case of unintended loss, including from accidents, disasters or cyber-attacks. If an older version of an object version is needed, you can retrieve or restore it to a previous version through the ECS S3 API. Further, by enabling bucket-level versioning in ECS Object Lock, you can lock object versions for specific retention periods (supporting governance and compliance scenarios) or indefinitely (for legal hold).

Click here to learn more about ECS versioning

Discover more about Dell ECS Enterprise Object Storage

Learn more about Dell ECS Platform

Follow Dell Storage on Twitter

Contact a Dell Technologies Expert for Sales or Support

DELL Technologies