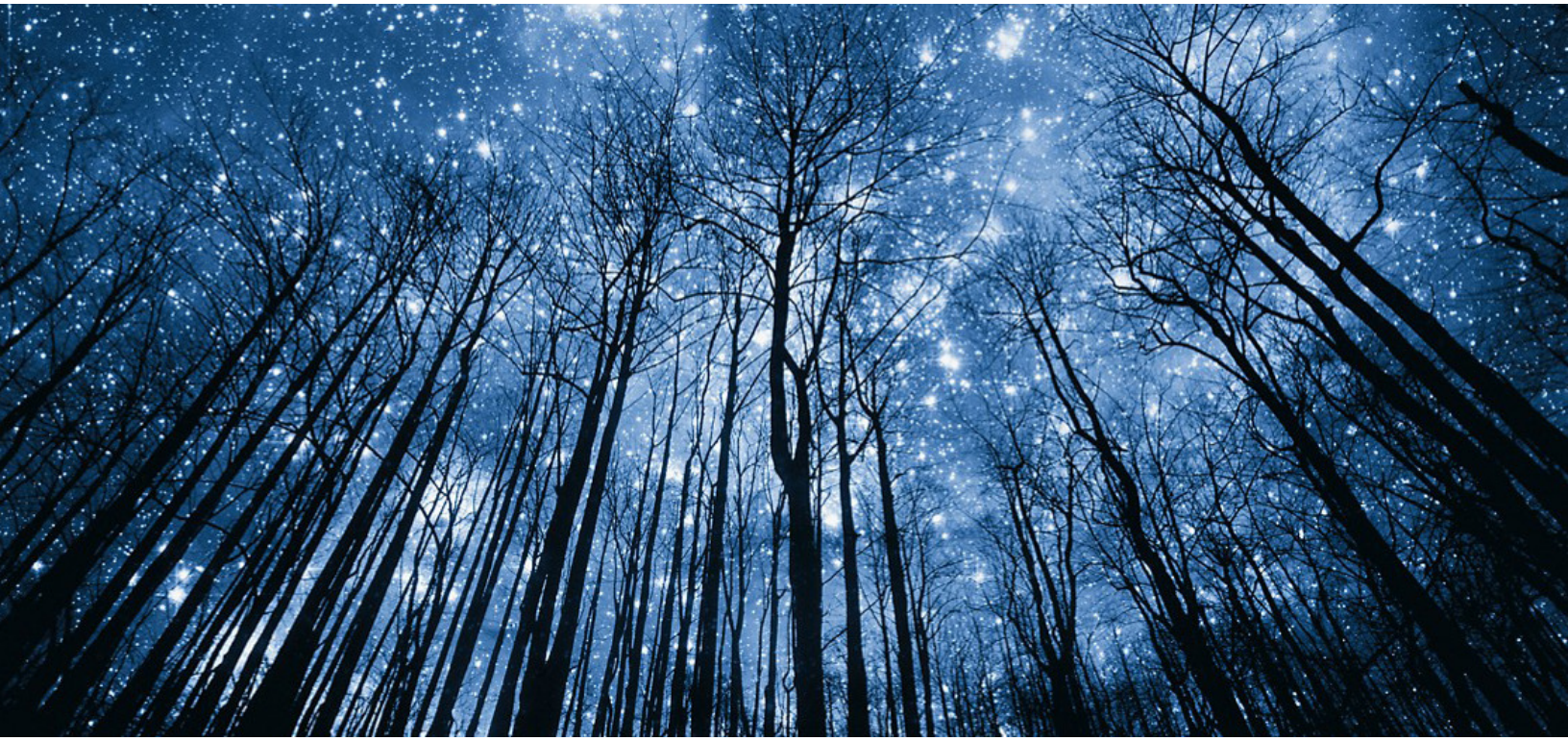
DELL Technologies

REDESIGN ENDPOINTS DATA PROTECTION STRATEGIES



Mohamed Sohail
Advisory Consultant,
Data Center & Business Resiliency

Sameh Gad
Principal Consultant,
DC Modernization & Business Resiliency
Dell Technologies

DELL Technologies
Proven Professional

Knowledge Sharing Article

Contents

Preface

No one nowadays can ignore that digital transformation is changing our lives. The Internet of things, Laptops, Desktops, and even mobiles are playing a vital role in our day-to-day activities, either at home or at work. Cyber threats don't cause only thousands of dollars of loss anymore—the damage is in the trillions. Accenture forecasts over $5T of global value at risk over the next 5 years. [1]

Attacks are usually non-stop and the cost per attack continues to increase, while there is a common misconception that only certain-sized businesses or industries are attacked, the reality is that nobody is protected. Attackers Or the hackers target businesses of all sizes, and across all industries. [2]

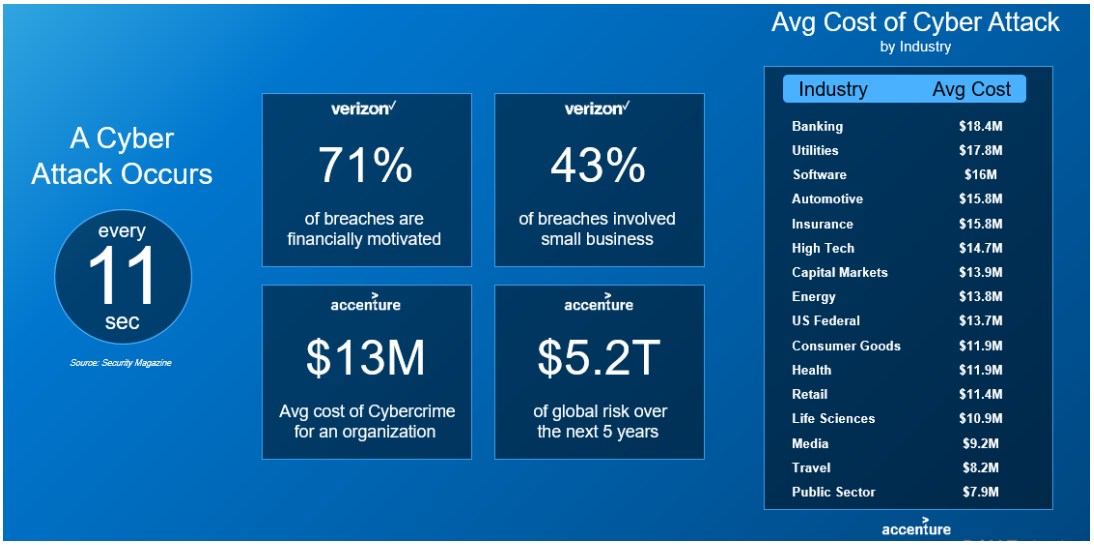


Figure 1: The Evolving Cyber Threat Landscape

Too often, we see organizations focused on guarding against a very specific type of cyber-attack or cyber actor. This narrow focus can put them at risk.

It's important to understand that Cyber-attacks take many different forms, and the attackers may have a variety of motivations, techniques, and even platforms from which to launch their

attacks or work silently in order to have continues access on confidential data. Thus, for example, organizations cannot count on paying a ransom as a last option. While data may be encrypted and look like a ransomware-based attack, it may have been launched from a Nation state as a weapon, an insider with an ax to grind, or a hacktivist whose agenda is ideologically motivated and not financial. There may be nobody to pay to decrypt the data.

One of the most difficult types of cyber-attack to defend against is one launched by an insider (knowingly or unknowingly). They tend to have physical access, full knowledge of the infrastructure and may even have benefitted from privilege creep, giving them access to more systems.

A good cyber recovery strategy takes all of these points into account.

Ransomware attacks can be devastating to your business, they can cause permanent and massive business, data loss and bring down your whole business for weeks. Leading to lost revenue and reputation.

Impending litigation requires a quickly respond to data requests and ensuring that the data is admissible in a court of law. We also need to gather data for internal investigations and to prepare for a case.

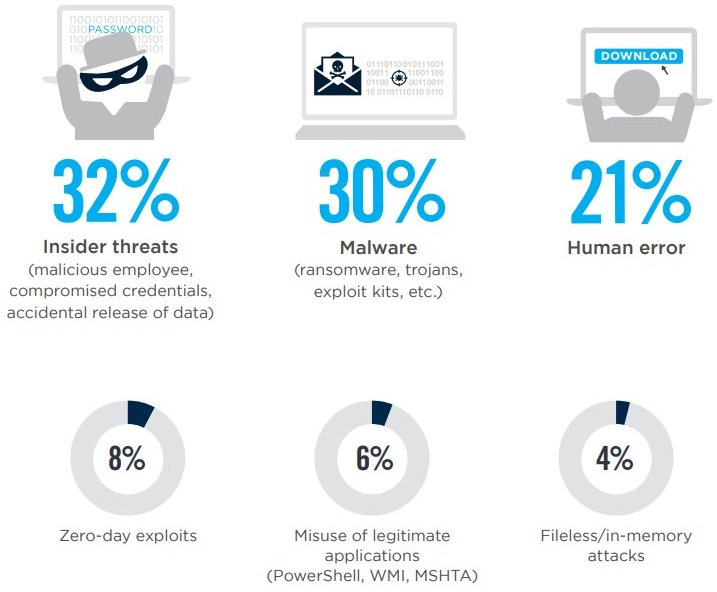


Figure 2: Biggest threats to organizations[3]

Finally, there is a heavy price for non-compliance with privacy regulations like **GDPR** or **CCPA**, leading to big fines and a lost reputation. But the process of auditing, monitoring, and ensuring compliance is costly and complex.

Endpoints include but are not limited to:

a) end-user devices such as desktops and notebooks

b) servers

c) mobile devices, including phones and tablets

d) internet of things (IoT) devices

e) peripherals such as printers and multi-function devices (MFDs).

Endpoint Protection methodologies in the era of Ransomware attacks. [Real-time protection, Backup, Air-Gaping the data]

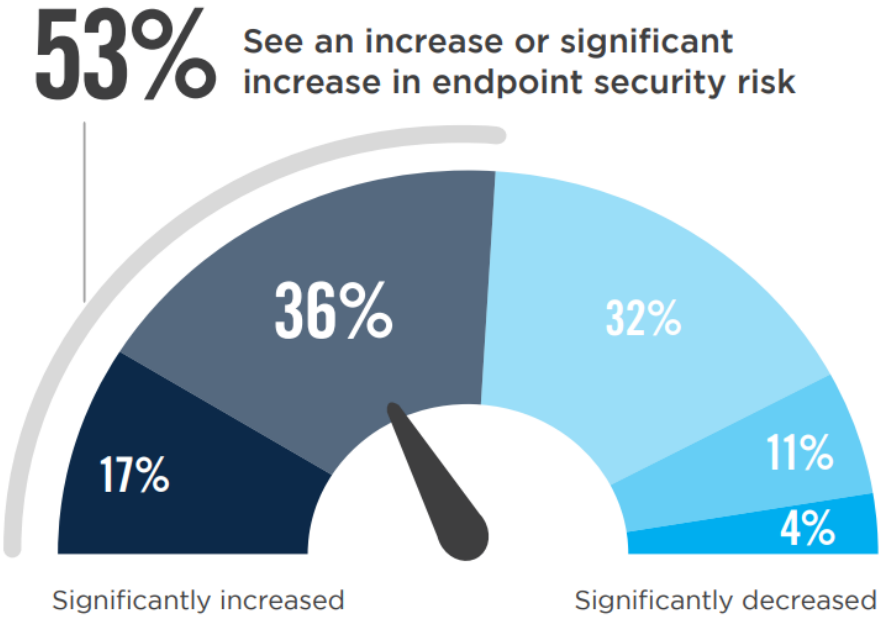


Figure 3: Endpoint security risks

In the above diagram, Accenture study triggered a 53% increase in the Endpoint's security risks which takes us to think of new ways to tackle such challenges. Having this in mind, we need to focus on the following points: -

Prevent:

Not all threats are malware based – the solution can stop 99% of malware

With very low CPU usage and provides the ability to lock and protect USB ports, which can be an easy access point for threats. Traditional antivirus solutions do not provide these capabilities.

Detect:

Solution/platform giving the ability to find malware AND non-malware-based threats quickly and efficiently. With insight, customers can then target the response to get identified threats out of their environment. The main challenge this requires skilled security resources that are focused and trained to respond. This tends to be a gap for many customers.

Respond:

To respond –manage and assist with rapid containment and eradication of threats, remotely or on-site. Work with the key stakeholders, executive and legal teams and this to give independent information and feedback based on evidence presented by risk management team.

Conduct a detailed assessment of the existing risk and incident Response documentation, personnel, and procedures.

Using proprietary technology identifies the presence of compromises and entrenched threat actors operating in your network.

The methodology and the solution should include:

- **Data availability**: Ensuring data is never lost with a reliable backup and recovery that is consistent and allows you to quickly recover from all types of loss
- **Data security**: Protect your backup data in isolated, immutable, and encrypted snapshots that cannot be penetrated or altered by any users or malicious activities so you can rely on it for ransomware recovery. Realizing additional value from your backup data through:
  leveraging the backup solution to proactively collect data, automate legal hold, and pre-cull your data so you can cut costs and quickly submit admissible data
- **Privacy compliance**: Leveraging the backup solution to proactively monitor for compliance violations and remediate them per the available policies.

Endpoint data protection as a service – Dell EMC Avamar as an example

Ransomware and attackers or the bad actors have learned that they have a better chance of achieving their goal – getting paid a ransom or destroying data – if no backup is available for recovery. This has placed the backup under direct attack. Unfortunately, there are several vulnerable points because backups were designed for accessibility, and not necessarily for security:

#1: IT & Backup Admins are the main targets for compromise through a variety of attack vectors because their access is trusted and can easily and rapidly become the effective change agent to carry out an attack.

#2: The master server often contains a catalog of data. Encrypting or deleting this data can make a backup take much longer – and in some cases may even keep the backup from being used for recovery

#3: Any system mounted by the media server can be attacked if the media server is compromised

#4: **File systems**, tape, and the cloud may hold backups but are also being targeted. File systems, especially those accessible via CIFS or NFS are often targeted with data being

encrypted or deleted. Tapes may be offline, but generally require a catalog for a speedy recovery – which is usually online and subject to deletion (see #1 above). Finally, the cloud is not an inherently secure location for backups – it's just different from the production environment. But data there can usually be deleted immediately by anyone with access privileges, and the cloud is always available for access.

There are some important facts about the Endpoints, that we need to put them in mind when thinking of how we protect them.

- End-user machines are an easy target for hackers & disgruntled employees.
- End User Machines are exposed to the Internet & are more vulnerable to malware etc.
- End User machines (Desktops and Laptops) have 25% of organizational data worthy of sitting behind firewalls.

On the other hand, there are basic requirements that Enterprises and End users focus on them to be able to claim that they have a robust Data Protection methodology. We can summarize them into these 2 pillars.

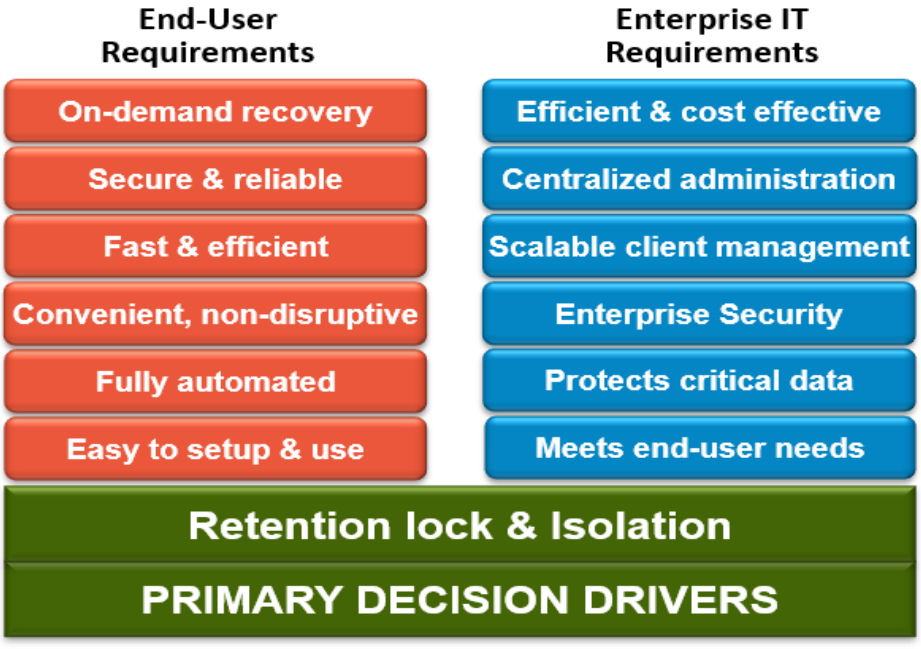


Figure 4: End User & Enterprise IT Requirements

Our checklist of “must have” features for an ideal solution includes, for the end-user:

- **Easy to setup and use** – the easier it is to do, the better; an intuitive, user-friendly user interface will go a long way towards better backup habits
- **Fully automated** – no one remembers to backup up, so a set-it-and-forget-it solution once configured is a must
- **Convenient and non-disruptive** – the ideal solution must be “lightweight,” and run quietly in the background and periodically assure the user that everything is under control – users should be able to continue their work with little or no interruption or delay
- **Fast and efficient** – once the first backup is completed, the ideal solution will monitor the data for changes and backup only the changed parts, saving time; in the case of a data loss, the ideal solution should allow all the data to be restored quickly to a previous good state
- **Secure and reliable** – that’s the data you’re backing up, it’s very important to ensure that the data is encrypted before it leaves the desktop/laptop; and a backup solution is only as good as its ability to restore data, make sure the data is available and recoverable
- **On-demand (self-service) recovery** – that’s what the backup solution is for in the first place – recovery; users need to quickly and easily restore their data (without burdening IT)

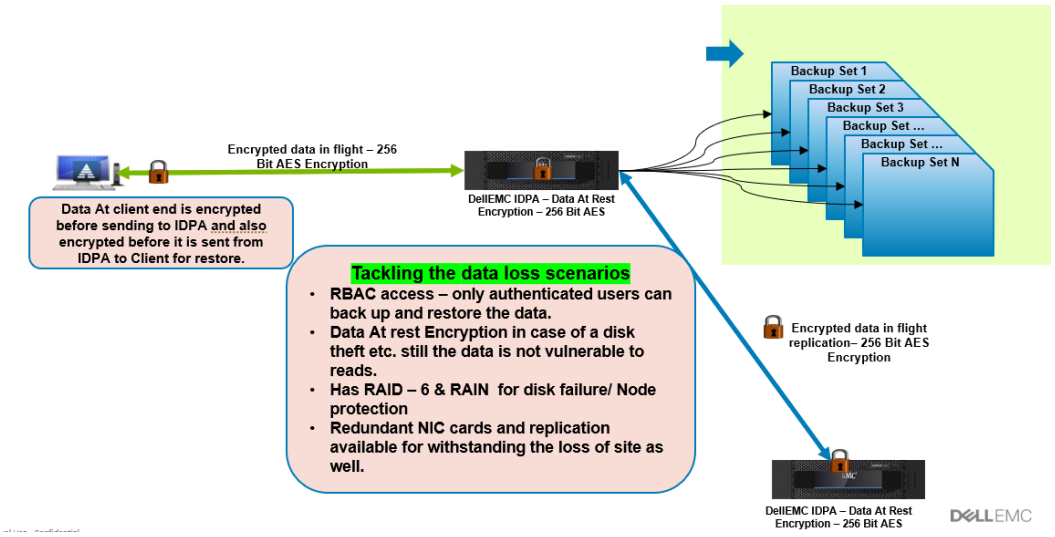


Figure 5: Tackling Data loss scenarios

And IT's checklist of "must have" features for desktop/laptop includes:

- First up, IT must Meet end-user requirements – backups are not the most pleasant tasks anyone wants to comply with (but needs to do), so you must meet the requirements of end-users to encourage good backup behaviors
- Protects mission-critical data – the ideal solution must provide comprehensive data protection for corporate intelligence
- Enterprise integration and scalability – The best practice is avoiding backup solution that places demands for additional infrastructure and look for something comprehensive that works with existing resources; to classify as a true enterprise solution the solution should leverage technologies such as high availability, load balancing, and support thousands of clients
- Scalable client management – the need for centralized visibility into distributed information assets
- Centralized administration – administration and management represent a major component of the total cost of a solution, consequently centralized administration and control are a must; the administration should be able to install, configure, and administer client software from a central location

- Efficient and cost-effective -
    - Bandwidth and storage optimization – the ideal solution must maximize the efficiency of its transmission over the network as well as the storage efficiency of the backup data
    - Replication plus long-term storage flexibility – the solution should replicate to a storage device that is physically separate from the desktop/laptop and is protected, ideally to an offsite location, so it can quickly be recovered from failure; in addition, export to tape for long-term storage would be ideal
    - Cost effectiveness – and of course cost; uses existing infrastructure; take advantage of virtualization

That's quite a list!

The key question is, does the ideal solution exist, that can balance the requirements of both the end-user and IT? The short answer is yes!... Let's have a look.

How can you reuse your Avamar as an efficient Endpoint Data Protection Solution?

In any engagement, we always have some qualifying questions that make us think if we can achieve certain features and be protected from all the above-mentioned threats. Like no standalone enterprise backup system, Avamar can offer this feature of End-point data protection without any extra tuning, since it is self-service, and doesn't require any rework, or custom scripting. Let's take a look on some points, and deep dive on how it can fit into our goal widening its use as an endpoint data protection tool.

Examples of these qualifying questions we need to ask ourselves to check what should be there:-

- How are you protecting your desktop & laptop systems?

- How are you protecting your home user devices?
- Do you need to reduce operational costs for your Data Protection environment?
- Is it important to have a single, integrated data protection solution to protect all your End-Point devices?
- Does your data protection and recovery solution lower your costs and improve efficiency?
- What is your expectation in terms of reliability and NIST compliance?
- How would you recover from a ransomware attack?
- What if your backups are gone?
- How many Data Domains do you have?
- How many can you log into from the conference room right now?
- In the NIST Cybersecurity framework – who owns the Recovery function?
- How do you protect your backup infrastructure?
- Who owns your cyberattack recovery plan?
- How much is your daily revenue?

Use cases. Below are examples of what we can achieve.

- End User machines (Desktops and Laptops) have 25% of organizational data worthy of sitting behind firewalls.
- Desktop Laptop “DTLT” Clients are already enabled, and no limit is enabled on the number of clients.
- Though All Tier -1 applications and databases are protected via various mechanisms from a security perspective – end-user machines are often an easy target for hackers and disgruntled employees.
- End-user machines have business reports, payslips, important passwords, and data that are not always present on servers, hence their protection becomes necessary.

- End user machines are “local” to users and are open to “Internet” hence are more prone to “Phishing” attacks, encryption of data, etc.
- Each End user has around **4-5 GB, with around 5,000 users** resulting in around 25 TB of data, which is not under enterprise data protection focus.

Characteristics

- **Improved SLA:** Daily Full backups – faster restores.
    - BMR backups supported
    - Ability to backup only specific files e.g., *.mp3 exclusion and inclusion possible.
- **Reduce Cost:** Store more copies in much less storage
    - Reduction in bandwidth for replication – as deduplicated data gets replicated
- **Reduce Complexity:** Tapeless
    - Add as many users as required, no need for managing per-client licenses.
    - Each user can have many laptops or machines
    - End User restores supported
- **Improve Resiliency:** Better resilience
- **Site-level protection supported with replication**.
    - Give Data Owner the control & self-service capability with native tools
- **Ease-of-Use:** Data Protection Central new UI improves management and monitoring
- **Lower TCO/ Greater Efficiency:** Dell EMC best deduplication and storage efficiency in the market
- **New investments, new products**: IDPA is an integrated solution and does not require additional components

- **Flexible Deployment:** Dell EMC has flexible deployment options that fit the need of every customer
- **Integration with Endpoint:** Seamless Integration - low system usage

Avamar Capabilities as Backup as a service for Endpoints.

Endpoint Security Solutions

Security and Resiliency Organization (SRO)-Cybersecurity must provide comprehensive and centralized endpoint security solution(s) to prevent, detect and respond to known and unknown threats.

2. Endpoint security solutions include, but are not limited to:

a) Anti-malware software

b) intrusion detection and prevention software (IDS/IPS)

c) endpoint encryption technologies

d) application control/allow list

e) Backup data protection, data loss prevention (DLP), and file integrity monitoring (FIM)

f) URL filtering/content filtering

g) network access control

3. Endpoint security solutions must be:

a) deployed on all endpoints as identified by SRO-Cybersecurity

b) deployed in every environment, as identified by SRO-Cybersecurity, regardless of whether the such environment is hosted on-premises or in the cloud.

Several use cases, including

- Device and data loss, which is addressed through backup and restore

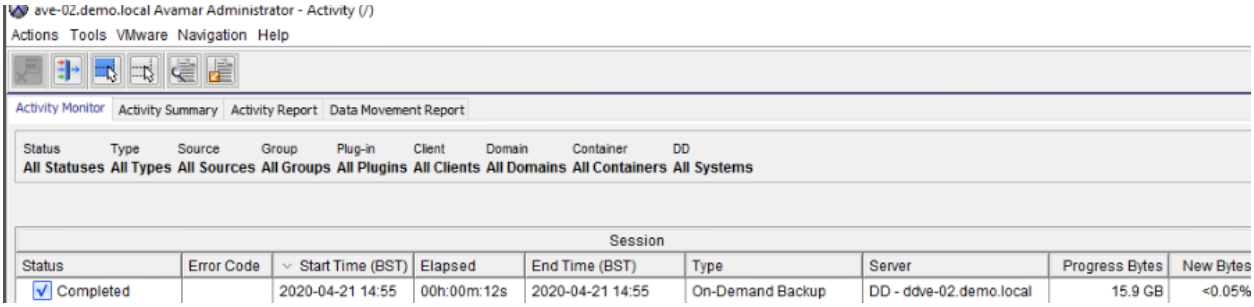
- Data security, including Data loss prevention (DLP) to prevent leaks in the event of device loss or theft and ransomware protection
- Data governance, consisting of eDiscovery and data compliance
- And device lifecycle management, including acceleration and streamlining of key IT processes like OS migration and device refresh
- Monitor and proactively detect anomalies (like the deletion of data or changes to user rights) through alerts based on machine learning (ML) based algorithms. If anything is out of the norm, the customer will see those alerts in their console
- Identify unusual and harmful backup data activity (like the deletion of data or changes to user rights) through alerts that use machine-learned algorithms based on historical activity. If anything is out of the norm, the customer will see those alerts in their console
- The system will then identify which backups have been infected so that the admin can respond by either isolating or deleting that corrupt data to prevent it from contaminating other data sets
- Customers can recover that data quickly using what's called a curated backup which identifies and assembles clean versions into a single "golden snapshot" for recovery.

Avamar Demo

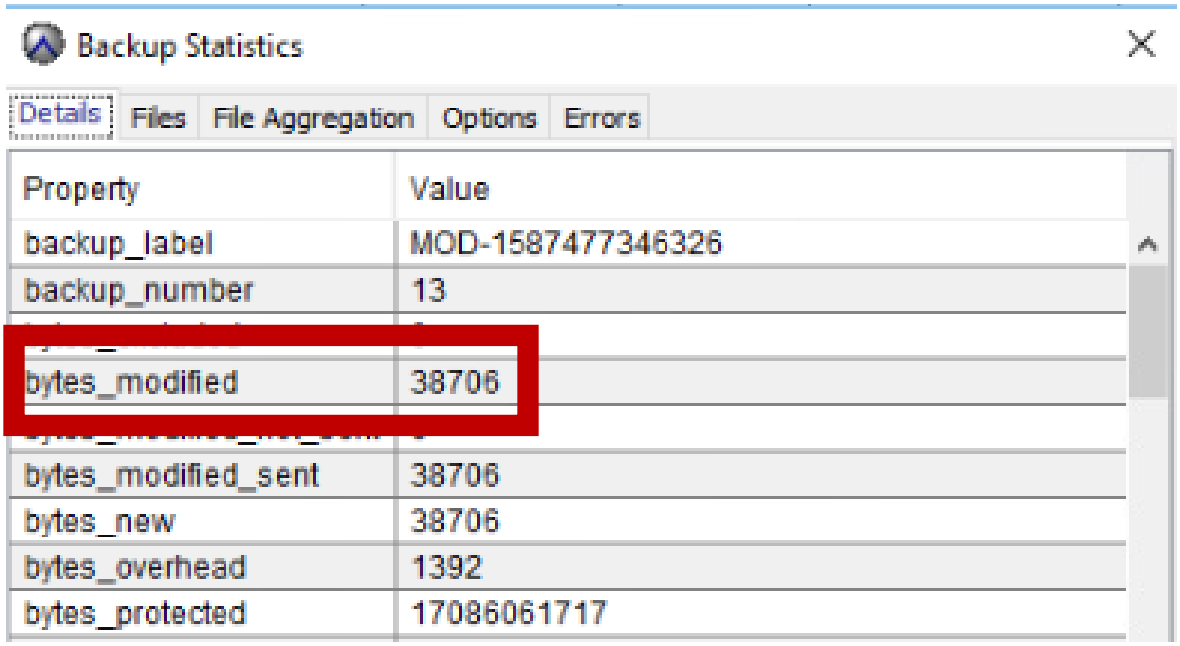
End users can use Avamar as a Backup service solution where they can initiate a backup or restore, or even has this enforced by the system administrator.

Backup

Performing a full backup. Hundreds of endpoints are backed up in parallel in the full backup fashion.

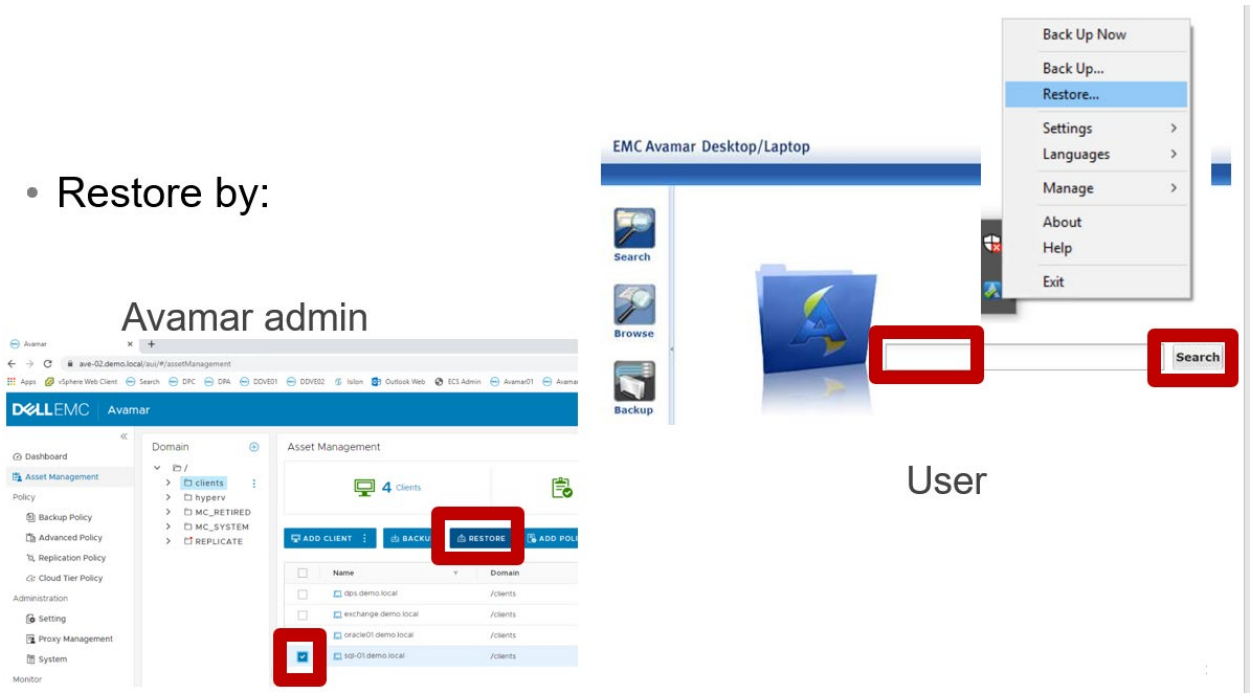


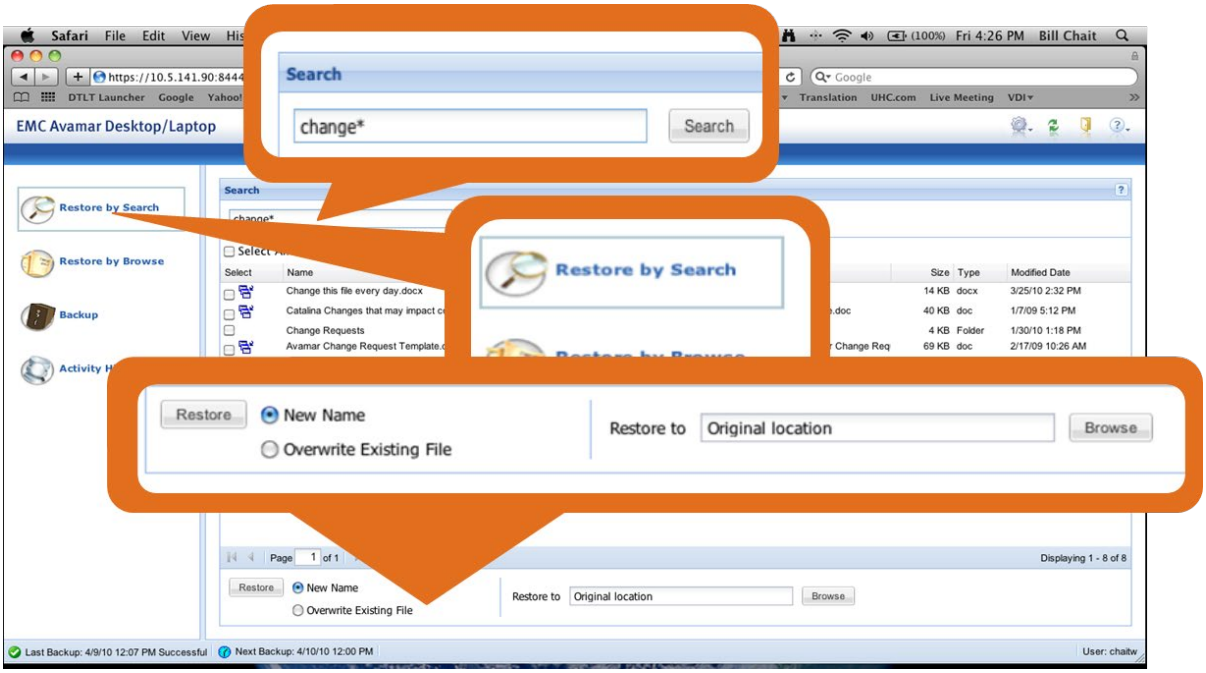
NO network usage during backup!

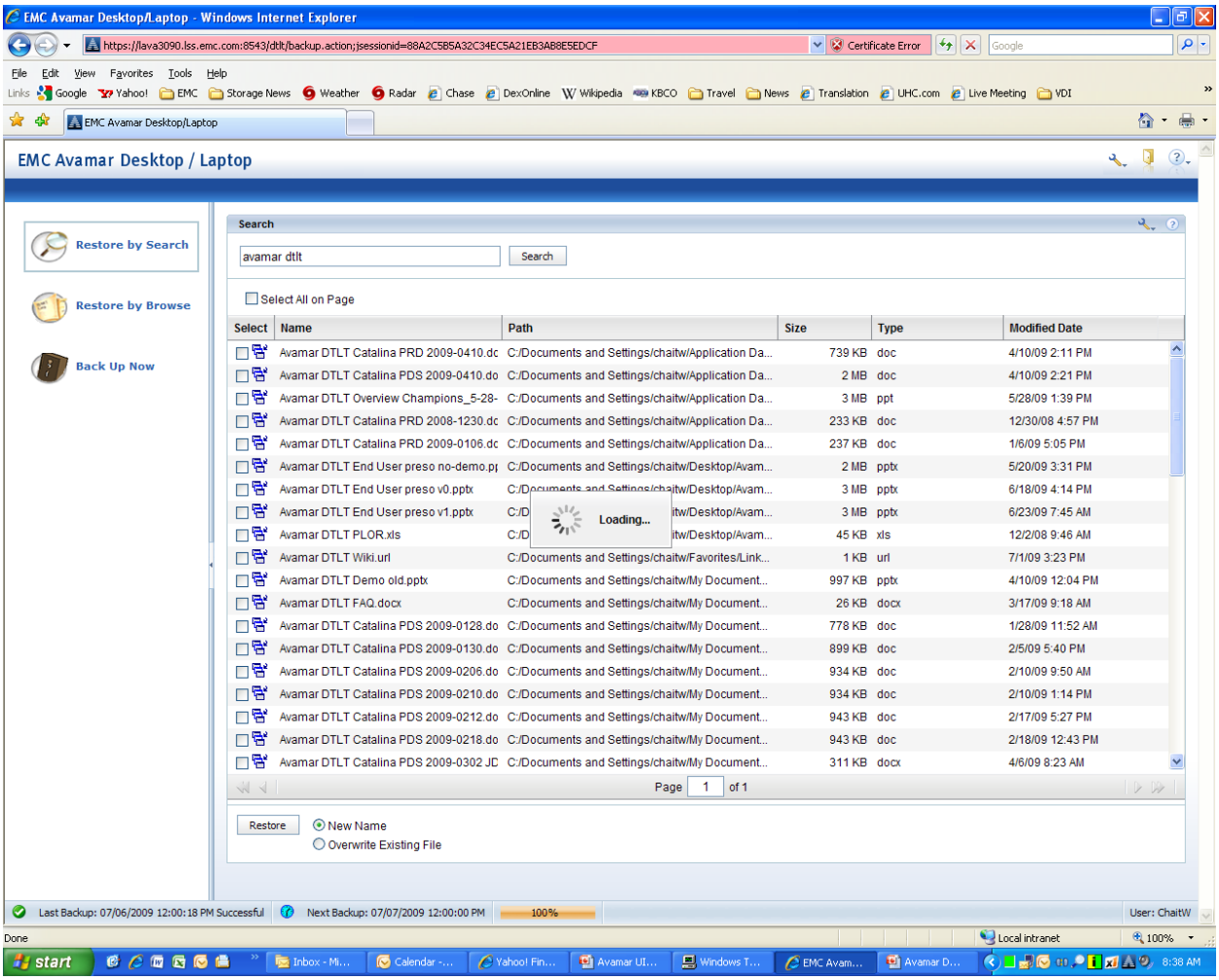


Self-service restore

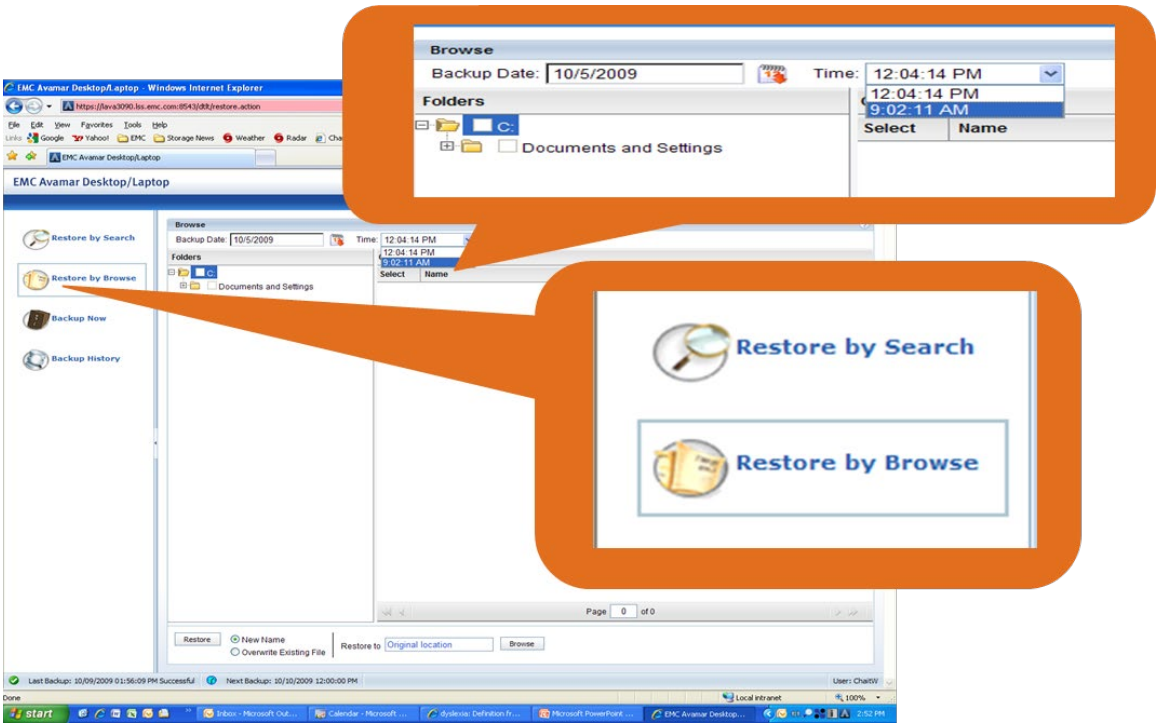
- Restore by:

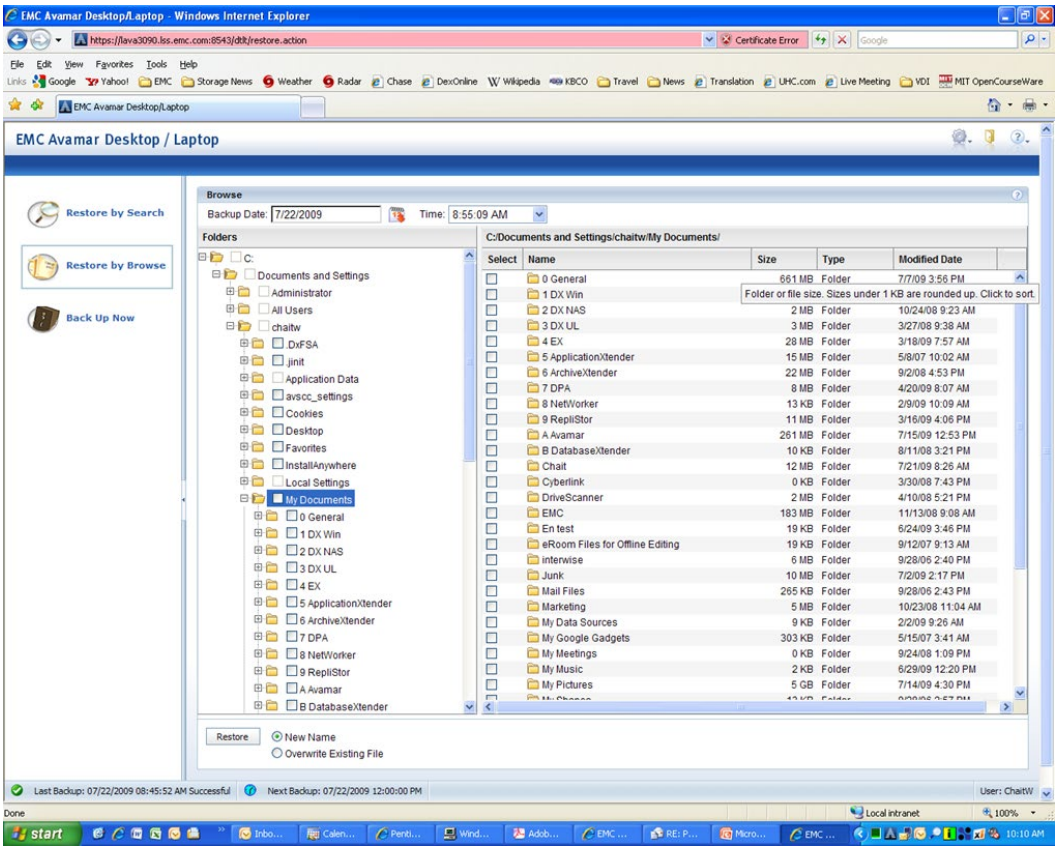

Avamar admin
EMC Avamar Desktop/Laptop
Back Up Now
Back Up...
Restore...
Settings
Languages
Manage
About
Help
Exit
Search
Browse
Backup
Search
User


EMC Avamar Desktop/Laptop
Search
change*
Search
Restore by Search
Restore by Browse
Backup
Restore
New Name
Overwrite Existing File
Restore to
Original location
Browse

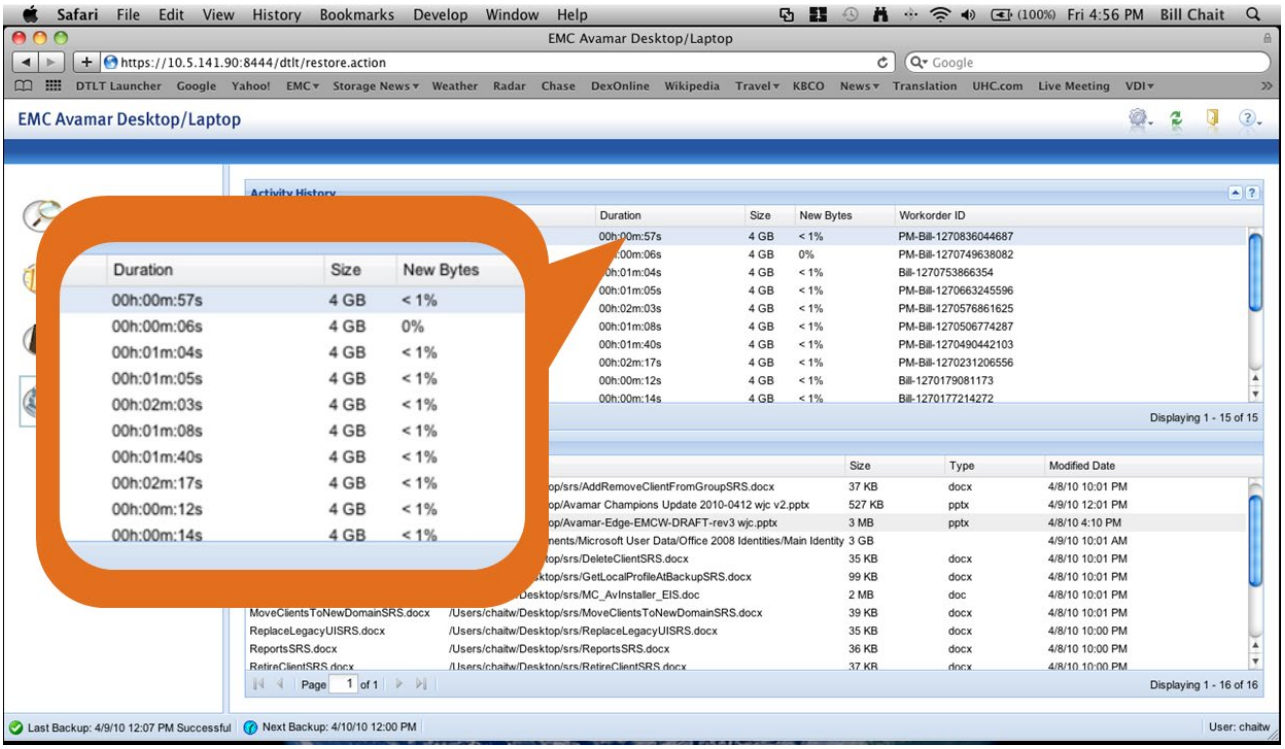


Self-service Recovery - Restore by Browse


Browse
Backup Date: 10/5/2009
Time: 12:04:14 PM
12:04:14 PM
9:02:11 AM
Folders
C:
Documents and Settings
Select
Name
EMC Avamar Desktop/Laptop
Restore by Search
Restore by Browse
Backup Now
Backup History
Restore by Search
Restore by Browse

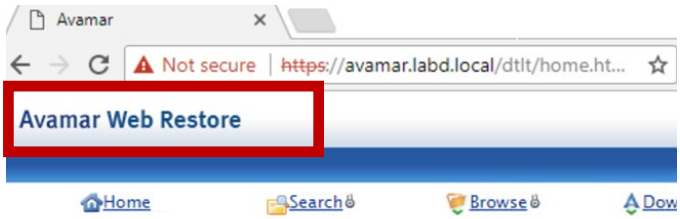

EMC Avamar Desktop/Laptop - Windows Internet Explorer
EMC Avamar Desktop / Laptop
Restore by Search
Restore by Browse
Back Up Now
Browse
Backup Date: 7/22/2009
Time: 8:55:09 AM
Folders
C:/Documents and Settings/chaitw/My Documents/
Select
Name
Size
Type
Modified Date
Restore
New Name
Overwrite Existing File

Activity History



Access to data from any device

- Mobile
- Laptop


Avamar
Not secure
https://avamar.labd.local/dtlt/home.ht...
Avamar Web Restore
Home
Search
Browse
Dow


DELL EMC
Warning: Authorized Users Only
User ID
Password
Domain
AVAMAR
Enter a domain
Client Name
Enter a client
Login
Help
© 2016-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

Achieving Business resiliency by Integrating Avamar with Air Gap & Information security analytics.

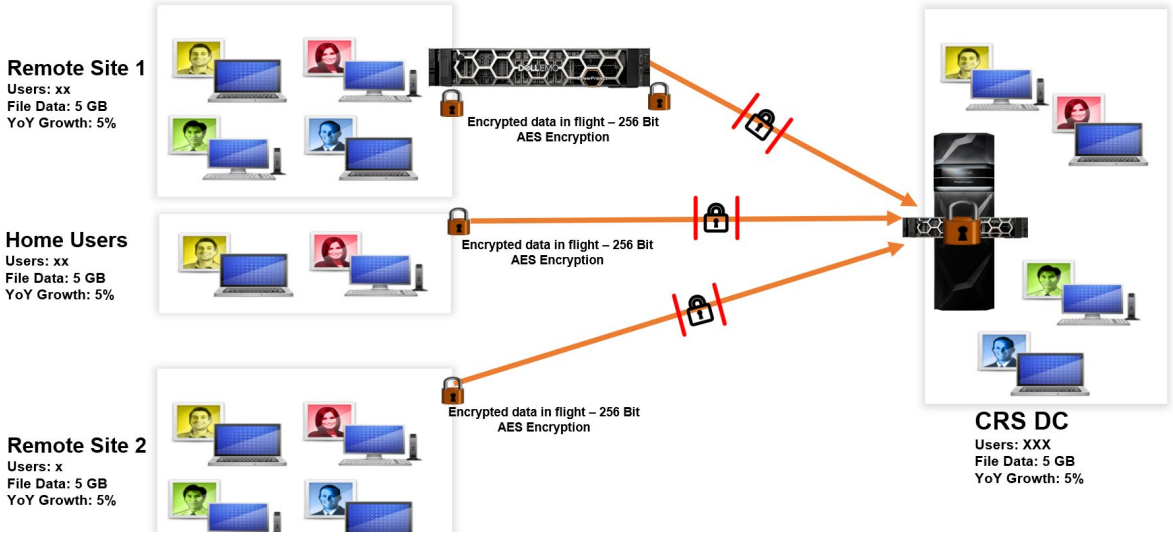


Figure 6: High-Level Architecture of Avamar with Cyber Recovery Vault

The above diagram shows how Avamar can be integrated with Cyber Recovery Vault capabilities with Air-gapping.

Since Avamar is able to apply retention lock to the data as part of its integration with Power Protect Data Domain, this gives it another layer of security.

Backed up data by Avamar can be written to production protection storage and vaulted into an isolated place where is can be analyzed against ransomware, and also create insights from the data to make sure that we are able to recover from encrypted data incident.

The below diagram shows how this integration can happen.

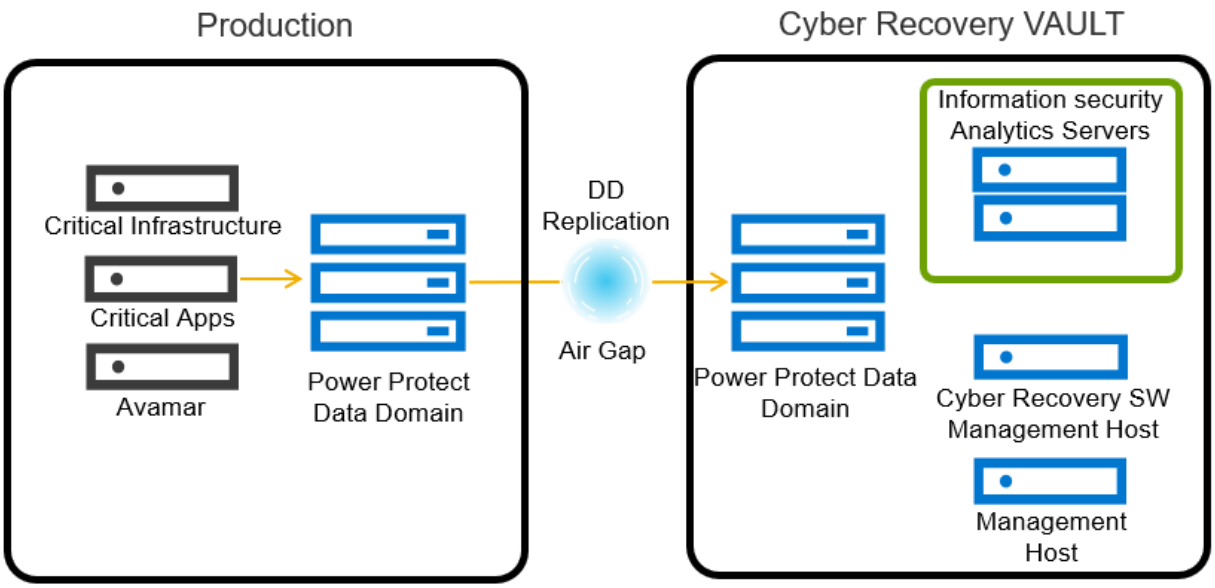


Figure 7: Integration with Isolated Recovery against ransomware attacks

Appendix & References:

1 - External Threats:

Threats are growing at an alarming rate and are more and more sophisticated. A threat can lurk within an environment for an average of 108 days before it is detected. During this time think about all the data it can steal and the harm it can do. And we also know 95% of breaches occur at the endpoint.

2 - User Behavior:

This challenge is compounded by the fact that end users are working and collaborating in more places, with more devices, and sharing information. They sometimes do so indiscriminately. 72% of them will share data externally and half of them will use personal cloud apps to share data. Given the opportunity, 41% of them will go around security.

3 - Limited Security Resources:

if there are not enough security professionals to fill knowledge-based roles. The security industry has a 0% unemployment rate. This means that companies have a hard time staffing and retaining key security personnel… over the next five years, the number of unfilled cybersecurity jobs will rise to a whopping 1.8 million, a 20% increase from 2015 estimates, so the problem is only getting worse each year.

• Couple this with the fact that many medium businesses similar in size to you don't even have a dedicated security department. This role is often shared with IT.

• All these issues are daunting and make security feel like an impossible task.

References

• Source: 95% of security breaches occur at the endpoint. Verizon Data Breach Digest, 2017

• Source: 108 days: The 2018 U.S. State of Cybercrime Survey, in partnership with CSO, U.S. Secret Service, CERT Division of Software Engineering Institute at Carnegie Mellon University, and KnowBe4

• Source: 72% share data externally. Dell End-User Security Survey, 2017

• Source: 50% use personal cloud apps to share data. Dell End-User Security Survey, 2017

• Source: 41% go around security. Forrester TAP report, Evolving Security to Accommodate the Modern Worker, October 2017

• Source: Over the next five years, the number of unfilled cybersecurity jobs will rise to a whopping 3.5 million.

• Source: Cybersecurity Jobs Report 2018-2021, Herjavec Group May 2017, https://www.herjavecgroup.com/wp-content/uploads/2018/07/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf

https://www.accenture.com/us-en/insights/cyber-security-index

https://www.verizon.com/business/resources/reports/2019-data-breach-investigations-report.pdf

https://www.kaspersky.com/about/press-releases/2022_half-of-businesses-53-discarded-new-it-or-business-projects-because-of-cyber-risks

https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds