

Bảo vệ và khôi phục dữ liệu trước nguy cơ tấn công mạng: Thách thức và một số giải pháp



Nguyễn Minh Đức

Kỹ sư cấp cao
Veeam Software

Email: minhduc.nguyen@veeam.com

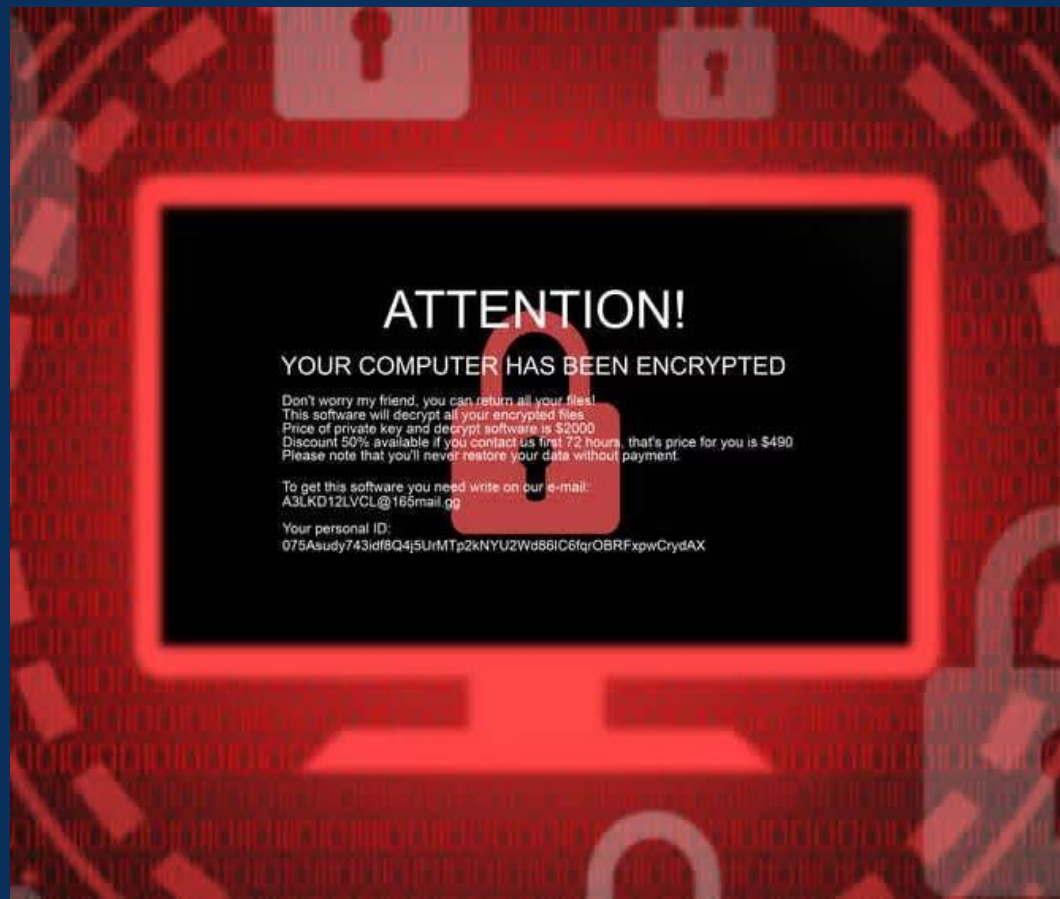
Nội dung

- Cập nhật tình hình các vụ tấn công đòi tiền chuộc (ransomware)
- Bảo vệ và phòng ngừa trước nguy cơ tấn công
- Khôi phục dữ liệu sau khi bị tấn công
Một số ví dụ thực tế từ các tổ chức, doanh nghiệp

Cập nhật tình hình các vụ
tấn công đòi tiền chuộc
(ransomware)

Tấn công đòi tiền chuộc trong bối cảnh hiện nay

**Khi nào
thay cho
Nếu như**



Tấn công vào hệ thống điều hành sân bay EU

Everest ransomware tấn công vào công ty cung cấp dịch vụ IT Collins Aerospace ngày 19-09-2025, gây gián đoạn dịch vụ tại các sân bay lớn nhất châu Âu gồm London Heathrow, Berlin Brandenburg và Brussels.



Nguồn: <https://www.theguardian.com/world/2025/sep/22/flight-delays-europe-cyber-attack-heathrow-brussels-berlin>

© 2026 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

veeam

Tấn công vào hệ thống dịch vụ công Indonesia

Nhóm tội phạm Brain Cipher đã tấn công và mã hóa dữ liệu 282 tổ chức chính phủ tại Indonesia ngày 20-06-2024.



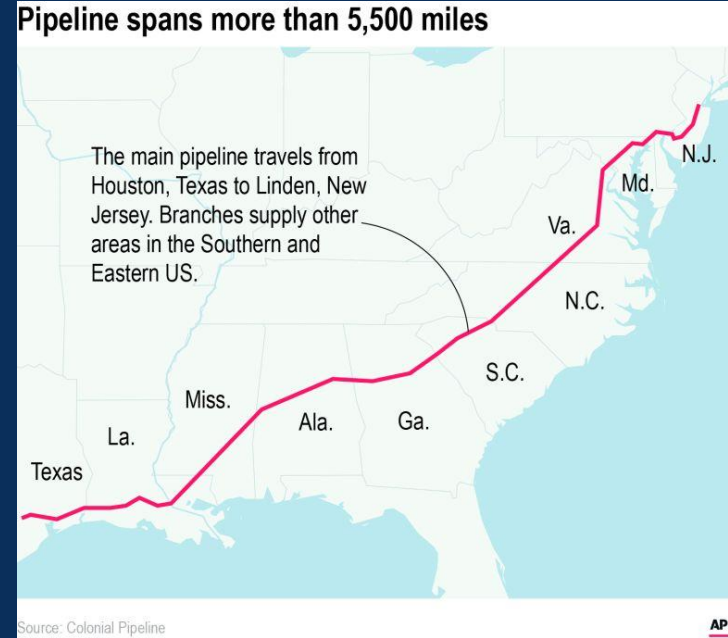
Nguồn: <https://asia.nikkei.com/Spotlight/Cybersecurity/Indonesian-cyberattack-signals-growing-threat-in-Southeast-Asia>

© 2026 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

veeam

Tấn công vào hạ tầng thiết yếu

Colonial Pipeline attack ngày 07-05-2021. Tổng thống Mỹ công bố tình trạng khẩn cấp 09-05 và thống đốc bang Georgia công bố tình trạng khẩn cấp bang vào ngày 10-5.



Nguồn: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

Bảo vệ và phòng ngừa trước
nguy cơ tấn công

Bảo vệ và phòng ngừa tấn công mạng

•**Kế hoạch**: Kế hoạch ứng phó sự cố (IRP) và Kế hoạch dự phòng thảm họa (DRP).

•**Đào tạo người sử dụng, nâng cao nhận thức**

•**Bảo hiểm rủi ro tấn công mạng (Cyber insurance)**

•**Thuê dịch vụ ứng phó sự cố**

•**Phòng ngừa tấn công mạng trong qui trình vận hành:**

- Sao lưu dữ liệu thường xuyên
- Phân lớp mạng
- Cập nhật phần mềm, cập nhật bản vá
- Lập danh sách ứng dụng an toàn (Safelist applications)
- Bảo vệ hòm thư điện tử
- Bảo vệ các điểm đầu cuối (Safeguard your end points)
- Đảm bảo phân cấp, phân quyền (Limit privileges)

Nguồn: "How to protect your organization from ransomware attacks" by JP Morgan Cybersecurity

Nguyên tắc “vàng” trong công tác sao lưu dữ liệu



Ba bản sao dữ liệu



Lưu trữ trên hai phương tiện khác nhau



Một bản dữ liệu lưu ngoài TTDL chính

veeam



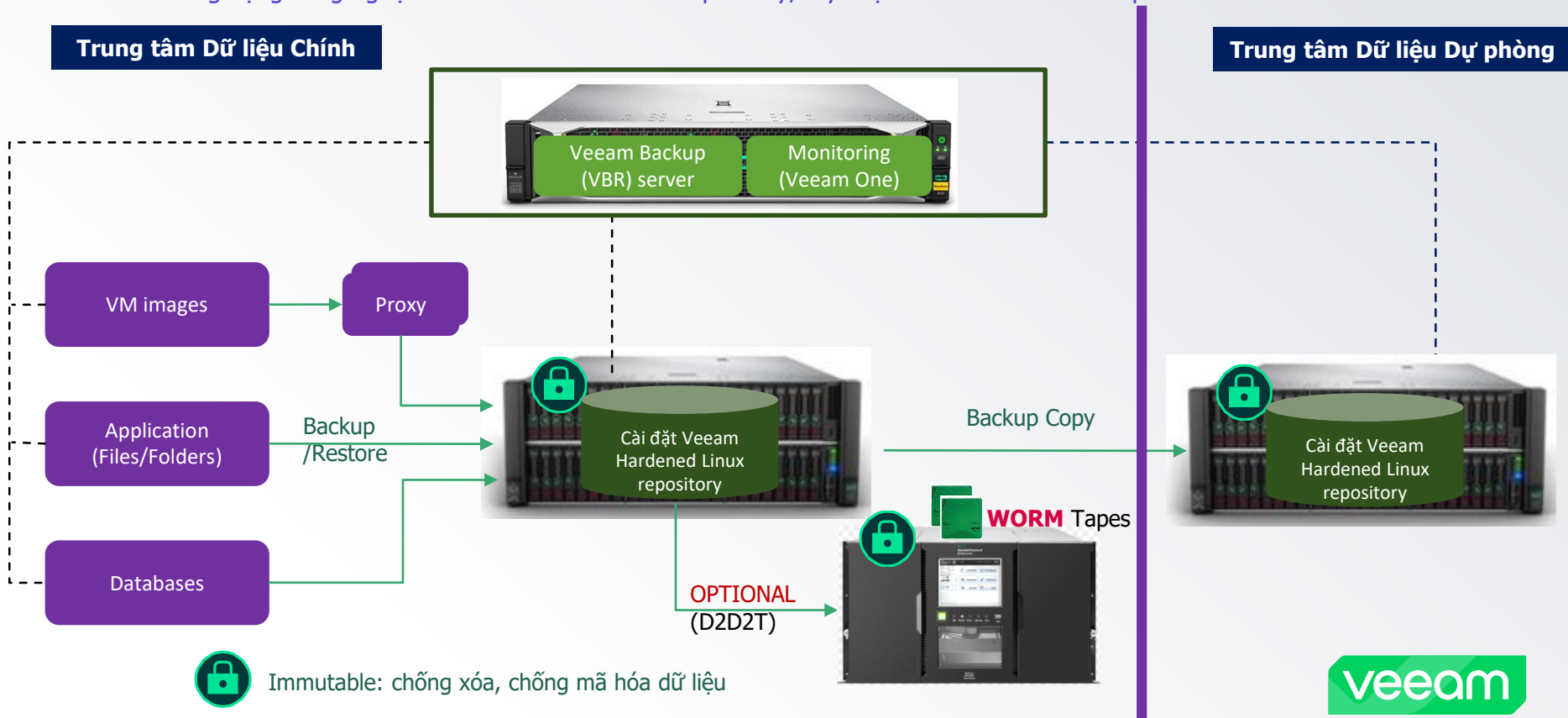
Ít nhất có một bản dữ liệu:
Offline, air-gapped
hoặc chống xóa sửa
(immutable)



Tự động hóa kiểm thử bản sao lưu, đảm bảo không có lỗi

Phòng chống xóa sửa các bản sao lưu dữ liệu: Trung tâm Dữ liệu tập trung cấp tỉnh hoặc tương đương

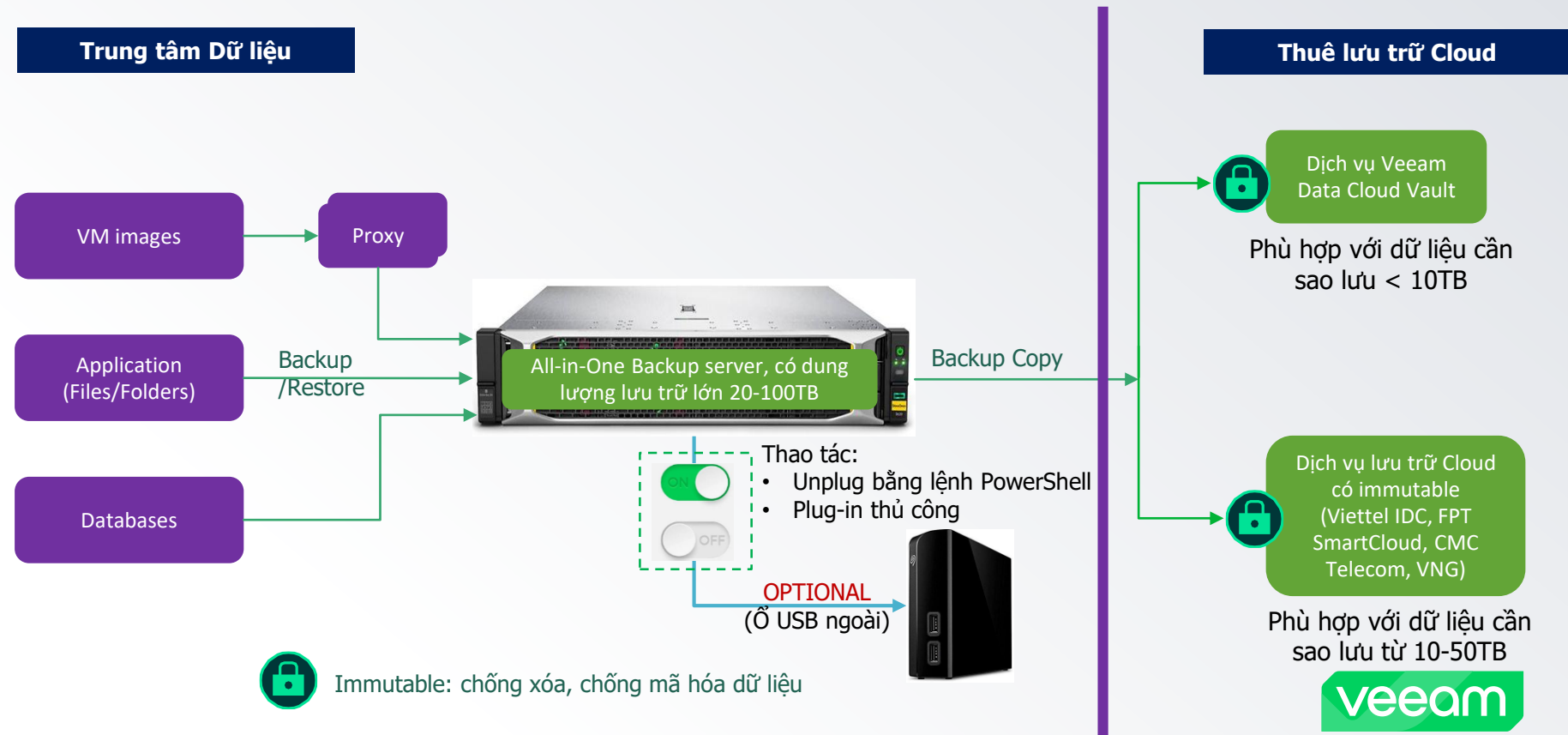
Mô hình 1: Ứng dụng công nghệ Veeam Hardened Linux Repository, tùy chọn sao lưu ra WORM Tape



Phòng chống xóa sửa các bản sao lưu dữ liệu:

Qui mô đơn vị cấp Phường, Bệnh Viện, Trường học

Mô hình 2: Cài đặt máy chủ backup All-in-One, có 1 bản sao lưu lưu trữ trên Cloud chống xóa sửa (immutable)



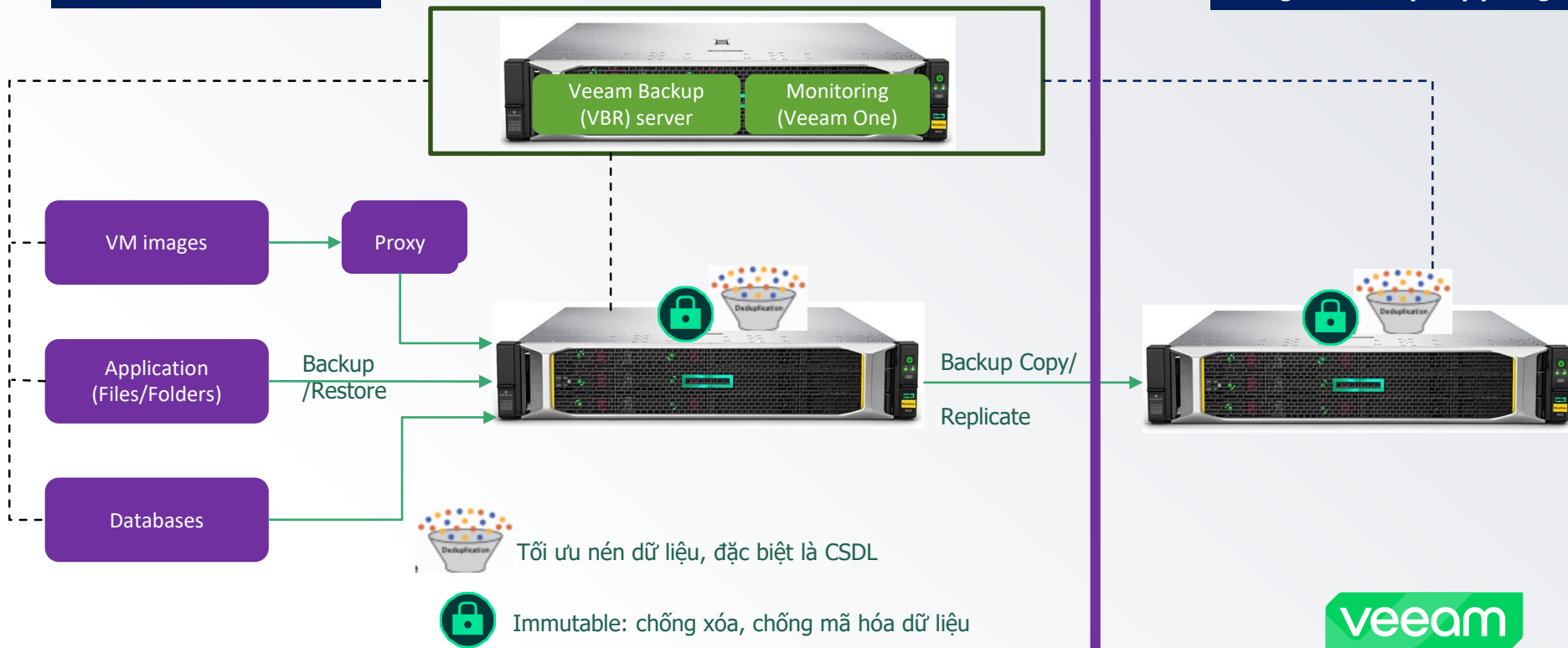
Phòng chống xóa sửa các bản sao lưu dữ liệu: Trung tâm Dữ liệu tập trung cấp tỉnh hoặc tương đương



Mô hình 3: Ứng dụng công nghệ Tủ sao lưu chuyên dụng của các hãng HPE StoreOnce, Dell PowerProtect DataDomain, Exagrid, Quantum

Trung tâm Dữ liệu Chính

Trung tâm Dữ liệu Dự phòng



Khôi phục dữ liệu trong thực tế

Quá trình khôi phục dữ liệu sau tấn công mạng

Với hơn 500,000 khách hàng, giải pháp Veeam giúp các tổ chức, doanh nghiệp khôi phục dữ liệu nhanh chóng. Tuy nhiên quá trình khôi phục bao gồm các yếu tố không chỉ phụ thuộc vào công nghệ...



Bị tấn công

- Thời điểm bất ngờ ví dụ tối Thứ 6 trước kì nghỉ lễ
- Xác định được phạm vi, cô lập vùng lây nhiễm
- Kích hoạt kịch bản Ứng phó sự cố (IRP)



Ứng phó

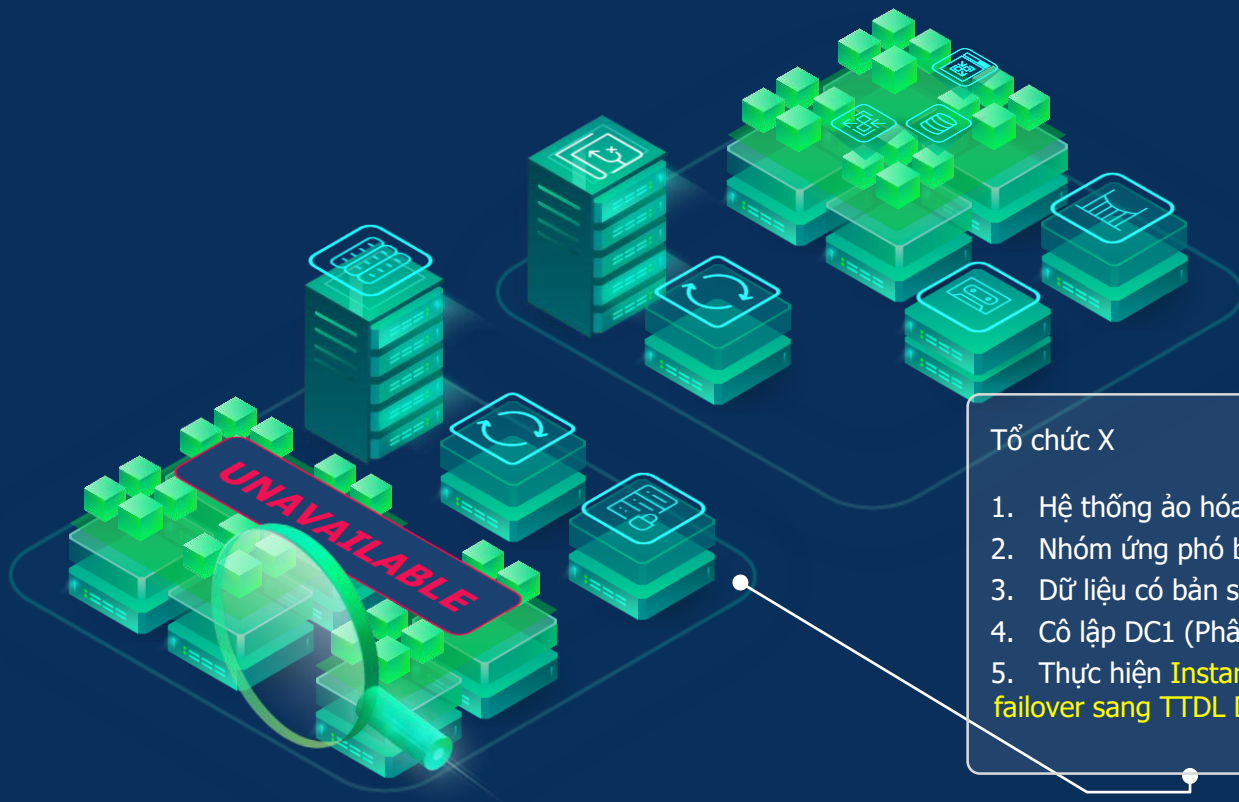
- Nhóm thực thi
- Báo cáo các cơ quan chức năng liên quan
- Thông báo tới đơn vị cung cấp bảo hiểm Cyber insurance



Khôi phục dữ liệu

- Phân tích sâu, truy vết về cuộc tấn công
- Khởi tạo môi trường khôi phục sạch/an toàn (tránh lây nhiễm ngược)
- Tiến trình khôi phục vào môi trường sạch thực hiện song song với quá trình phân tích sâu, truy vết

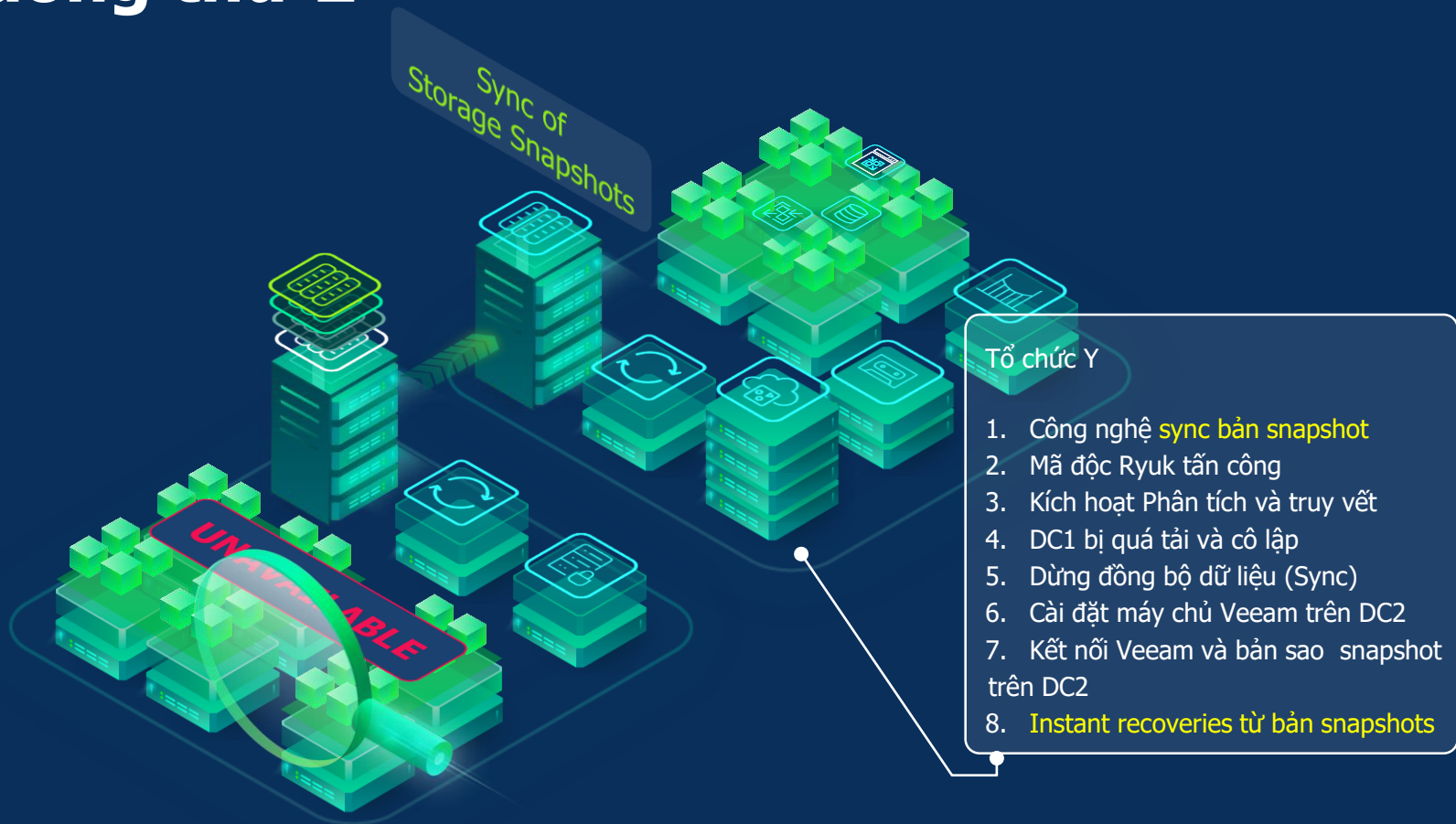
Tình huống thứ 1



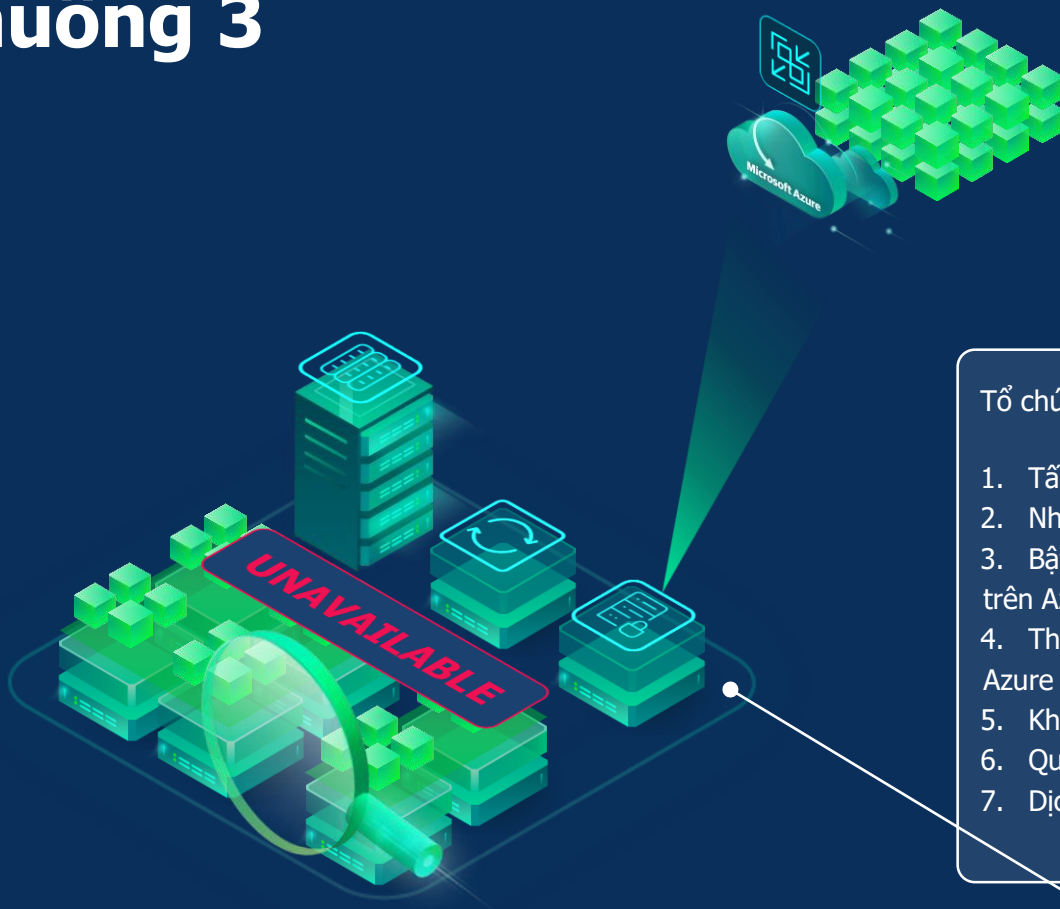
Tổ chức X

1. Hệ thống ảo hóa ESXi bị chiếm quyền
2. Nhóm ứng phó bắt đầu qui trình IRP
3. Dữ liệu có bản sao **không xóa sửa**
4. Cô lập DC1 (Phân tích, truy vết)
5. Thực hiện **Instant VM Recoveries** và **failover sang TTDL Dự phòng**

Tình huống thứ 2



Tình huống 3



Tổ chức Z

1. Tấn công bởi mã độc Conti
2. Nhóm Ứng phó ngắt kết nối TTDL Chính
3. Bật máy chủ Veeam Backup & Replication trên Azure Cloud
4. Thực hiện rescanned các bản sao lưu trên Azure
5. Khôi phục các VMs trên môi trường Azure
6. Quét, tìm kiếm và tiêu diệt malware
7. Dịch vụ online

Thành phố Sarasota



\$34M

Ransom NOT PAID

Veeam has changed our city for the better because backup has become a key component of our incident response strategy ... we finally found a solution that meets the city's data integrity needs. Veeam will be part of the city's lifeline for the foreseeable future.

Herminio Rodriguez

Information Technology Director

Thách thức →

- Giải pháp sao lưu trước đây không đáp ứng được yêu cầu và rủi ro khi cần khôi phục dữ liệu dịch vụ
- Giải pháp sao lưu trước đây không linh hoạt, không hỗ trợ khả năng bảo vệ dữ liệu multi-cloud
- Tỷ lệ backup lỗi cao và ảnh hưởng vận hành dịch vụ

Kết quả (triển khai Veeam) ✓

- Dịch vụ cung cấp đến cư dân vận hành thông suốt
- Đảm bảo chất lượng dịch vụ với cơ chế khôi phục dữ liệu dịch vụ nhanh chóng
- Tỷ lệ sao lưu thành công cao và đảm bảo tuân thủ yêu cầu lưu trữ dữ liệu đối với dịch vụ công

Nguồn: <https://www.veeam.com/success-stories/veeam-city-of-sarasota.html>

veeam

The Veeam logo is displayed in white lowercase letters within a white-outlined rectangular box with rounded corners. The box is set against a green background that features faint, overlapping diamond shapes.

Follow us!



Join the community hub:

