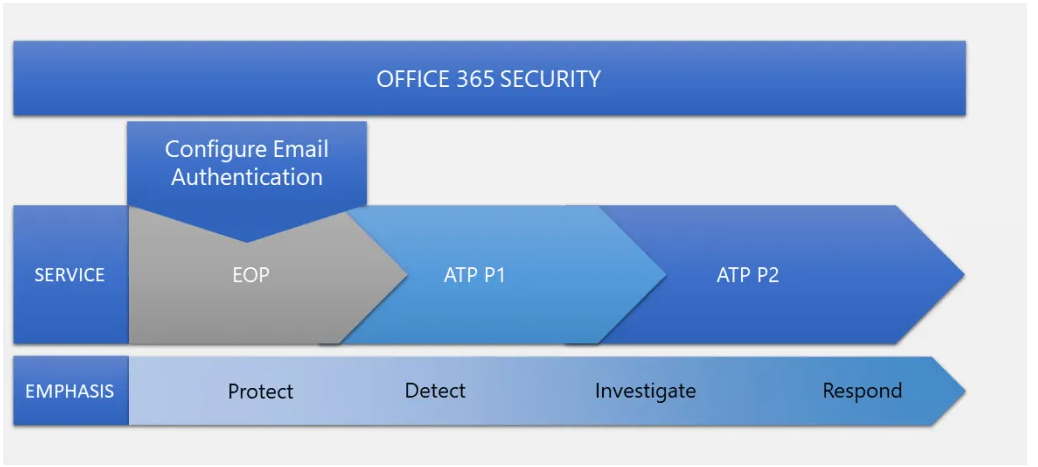
**Office 365 Security:**

Trong Office 365 security, có ba dịch vụ/sản phẩm bảo mật chính với các subscription sau:

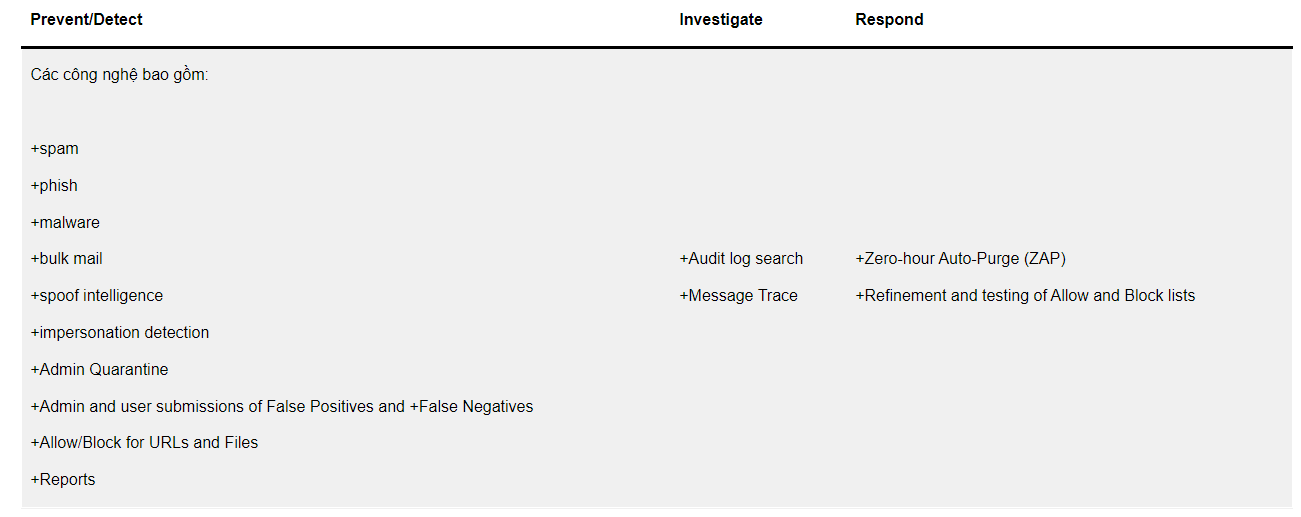
* Exchange Online Protection (EOP)
* Microsoft Defender for Office 365 Plan 1 (Defender for Office P1)
* Microsoft Defender for Office 365 Plan 2 (Defender for Office P2)



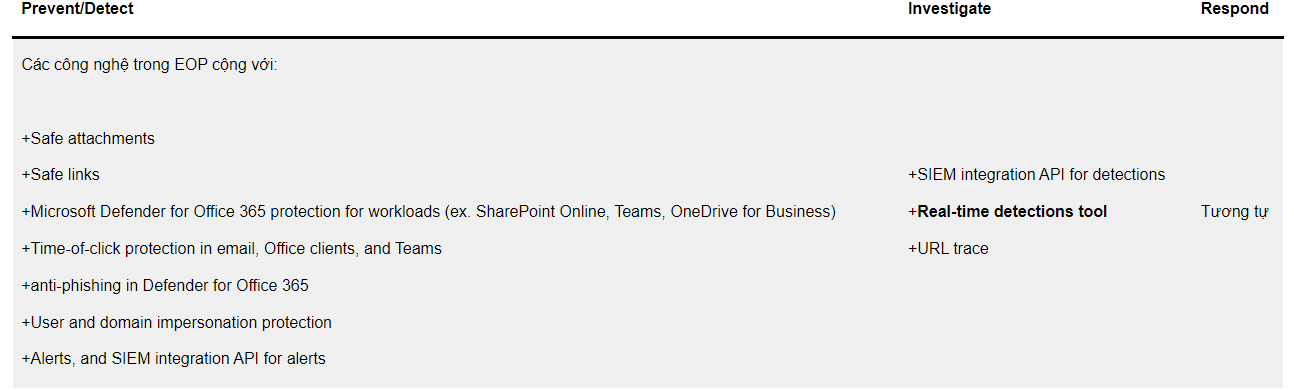
Mặc dù mỗi dịch vụ này đều nhấn mạnh (emphasis) các mục tiêu từ Bảo vệ (Protect), Phát hiện (Detect), Điều tra (Investigate) và Phản hồi (Respond), nhưng tất cả các dịch vụ có thể thực hiện bất kỳ mục tiêu nào trong số các mục tiêu trên.

Cốt lõi của Office 365 Security là bảo vệ EOP (Exchange Online Protection). Microsoft Defender for Office 365 P1 đã bao gồm EOP. Microsoft Defender for Office 365 P2 bao gồm P1 và EOP. Cấu trúc theo tích lũy, khi định cấu hình, bạn cần bắt đầu với EOP và làm việc với Microsoft Defender for Office 365.

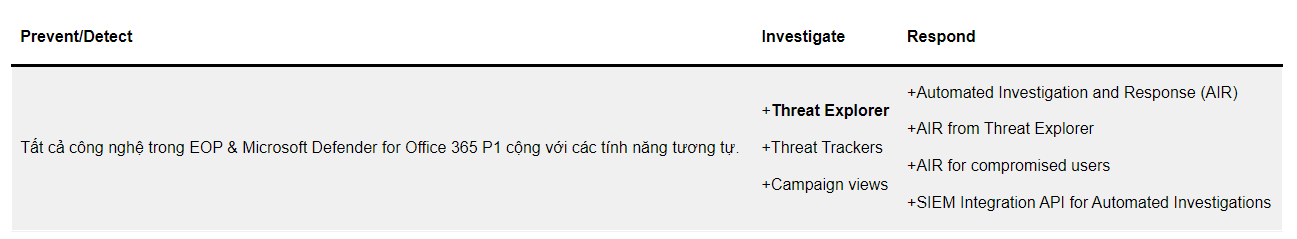
Bắt đầu với **Exchange Online Protection**:



Lợi ích với **Defender for Office 365** Plan 1:



Lợi ích với **Defender for Office 365** Plan 2:



List tính năng:

1. **Anti-malware protection**
2. **Anti-spam protection**
3. **Connection filtering**
4. **Outbound spam protection**
5. **Anti-phishing protection**
6. **Safe Attachments in Defender for Office 365**
7. **Safe Links in Defender for Office 365**
8. **Zero-hour Auto Purge (ZAP)**
9. **Allow and block**
10. **Attack simulation training in Denferder for Office 365**
11. **Advanced delivery policies**
12. **User tags and priority account Email entity page, Teams message entity panel**
13. **Threat Tracker**
14. **Alert policies**
15. **Auditting**
16. **Investigate and Respond**
17. **Threat Intelligence**: Cung cấp thông tin về các mối đe dọa và tấn công hiện tại để tổ chức có thể đối phó với chúng một cách hiệu quả.
18. **Data Loss Prevention (DLP)**: Cho phép bạn kiểm soát và theo dõi dữ liệu nhạy cảm trong Office 365, ngăn chặn việc chia sẻ hoặc mất dữ liệu không được phép.
19. **Data Governance**: Giúp bạn quản lý và bảo vệ dữ liệu trong Office 365 bằng cách thực hiện các chính sách về giữ và loại bỏ dữ liệu, cũng như bảo vệ dữ liệu trong các dịch vụ như SharePoint và OneDrive.
20. **Identity and Access Management**: Bao gồm các tính năng như Multi-Factor Authentication (MFA) và Single Sign-On (SSO) để tăng cường bảo mật xác thực người dùng và quản lý quyền truy cập.
21. **Information Protection**: Cho phép mã hóa dữ liệu và quản lý quyền truy cập dữ liệu theo chính sách.
22. **Security & Compliance Center**: Cung cấp một giao diện quản lý để tạo, theo dõi và tuân thủ các chính sách bảo mật và quản lý rủi ro.
23. **Security and Threat Analytics**: Cung cấp phân tích và báo cáo về tình hình bảo mật và các mối đe dọa tiềm ẩn trong tổ chức.
24. **Mobile Device Management (MDM)**: Cho phép quản lý các thiết bị di động được sử dụng để truy cập dữ liệu và dịch vụ Office 365.
25. **Audit Logging and Reporting**: Cung cấp khả năng ghi lại các hoạt động và tạo báo cáo về quản lý và tuân thủ.
26. **Secure Score**: Đánh giá và cung cấp gợi ý để cải thiện mức độ bảo mật của tổ chức dựa trên cấu hình và hoạt động trong Office 365.
27. **Threat Protection for Microsoft 365 Apps**: Bảo vệ các ứng dụng Office 365 như Word, Excel và PowerPoint khỏi các tấn công và mã độc hại.
28. **Insider Risk Management**: Giúp phát hiện và đối phó với các mối đe dọa nội bộ trong tổ chức.
29. **Communication Compliance**: Theo dõi và quản lý các loại thông tin trong các cuộc trò chuyện và email để tuân thủ các quy định và chính sách.
30. **Security and Compliance Solutions**: Bao gồm nhiều công cụ và tính năng khác nhau để cung cấp bảo vệ đa lớp và quản lý rủi ro trong Office 365

Ref: <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/?view=o365-worldwide>

<https://vinsep.com/kien-thuc/security/tim-hieu-ve-office-365-security/>

**TENABLE:**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

**Tenable Cloud Security - Unified Cloud Native Application Protection Platform (CNAPP)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Với Tenable Cloud Security, bạn có thể dễ dàng tăng cường bảo mật trên tất cả các môi trường AWS, Azure và GCP của mình. Từ việc khám phá toàn bộ tài sản và phân tích rủi ro sâu đến phát hiện và tuân thủ mối đe dọa trong thời gian chạy, bạn có thể giảm độ phức tạp, giảm thiểu khả năng hiển thị trên đám mây và thực thi đặc quyền tối thiểu trên quy mô lớn. Phương pháp tiếp cận toàn diện của Tenable trực quan hóa và ưu tiên chính xác các lỗ hổng bảo mật, đồng thời cung cấp cho bạn kiến thức chuyên môn và công cụ tích hợp mà bạn cần để khắc phục những rủi ro quan trọng nhất.

**Tenable OT Security - OT and ICS Cyber Risk Management: Complete Visibility, Security and Compliance**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Mô tả được tạo tự động

Có được khả năng hiển thị tài sản công nghệ vận hành (OT) chuyên sâu để hiểu rõ hơn, quản lý và giảm thiểu rủi ro mạng của bạn. Tenable OT Security (trước đây là Tenable.ot) là giải pháp bảo mật công nghiệp dành cho doanh nghiệp công nghiệp hiện đại của bạn. Nó có thể giúp bạn xác định tài sản trong môi trường OT của mình, truyền đạt rủi ro, ưu tiên hành động và cho phép các nhóm bảo mật CNTT và OT của bạn phối hợp tốt hơn với nhau.

Với bộ công cụ và báo cáo bảo mật toàn diện, Tenable OT Security cung cấp khả năng hiển thị chưa từng có trong các hoạt động bảo mật CNTT và OT, đồng thời mang lại nhận thức tình huống sâu sắc trên tất cả các trang web toàn cầu và tài sản tương ứng của chúng — từ máy chủ Windows đến bảng nối đa năng PLC — trong một giao diện duy nhất

**Tenable Identity Exposure**

**Secure Active Directory and Eliminate Attack Paths**

Kiểm soát bảo mật Active Directory (AD) và Azure AD của bạn để tìm và sửa lỗi trước khi chúng trở thành sự cố ảnh hưởng đến doanh nghiệp.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Mô tả được tạo tự động

Tenable Identity Exposure (trước đây là Tenable.ad) là một giải pháp bảo mật Active Directory nhanh, không cần tác nhân, cho phép bạn xem mọi thứ trong môi trường Active Directory phức tạp của mình, dự đoán những gì quan trọng để giảm thiểu rủi ro và loại bỏ các đường dẫn tấn công trước khi kẻ tấn công khai thác chúng

**Tenable Vulnerability Management**

**Understand Your Exposures and Know Which Vulnerabilities to Fix First**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, phần mềm

Mô tả được tạo tự động

Có được cái nhìn dựa trên rủi ro về bề mặt tấn công của bạn để nhanh chóng xác định, điều tra và ưu tiên các tài sản cũng như lỗ hổng quan trọng nhất của bạn.

Được quản lý trên đám mây và được cung cấp bởi Tenable Nessus, Tenable Vulnerability Management (trước đây là Tenable.io) cung cấp phạm vi bảo hiểm lỗ hổng toàn diện nhất trong ngành với đánh giá liên tục theo thời gian thực cho tổ chức của bạn. Ưu tiên tích hợp, thông tin về mối đe dọa và hiểu biết sâu sắc theo thời gian thực giúp bạn hiểu rõ mức độ nguy hiểm của mình và chủ động ưu tiên các biện pháp khắc phục. Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

**Tenable Attack Surface Management - Gain Visibility Into Your External Attack Surface**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Mô tả được tạo tự động

Có được khả năng hiển thị toàn diện về tất cả tài sản, dịch vụ và ứng dụng được kết nối internet của bạn để hiểu rõ hơn về dấu ấn kỹ thuật số đầy đủ của tổ chức của bạn cũng như đánh giá và quản lý rủi ro tốt hơn.

Tenable Attack Surface Management (trước đây là Tenable.asm) liên tục lập bản đồ toàn bộ internet và phát hiện các kết nối tới nội dung kết nối internet của bạn để bạn có thể khám phá và đánh giá trạng thái bảo mật của toàn bộ bề mặt tấn công bên ngoài của mình.

**List tính năng:**

1. **Vulnerability Management**: Giúp tổ chức xác định và quản lý các lỗ hổng bảo mật trong hệ thống của họ bằng cách quét và phân tích các thiết bị, ứng dụng và hệ thống.
2. **Asset Discovery**: Tenable giúp bạn tìm ra tất cả các tài sản trong mạng, bao gồm cả các tài sản không được biết đến trước đó, để đảm bảo rằng bạn có thể quản lý và bảo vệ chúng.
3. **Cyber Exposure Analytics**: Cung cấp khả năng thu thập, phân tích và hiểu rõ sự tiếp xúc với nguy cơ trong môi trường của bạn để đo lường mức độ rủi ro.
4. **Container Security**: Đảm bảo tích hợp với quy trình phát triển ứng dụng dựa trên container để đảm bảo rằng các ứng dụng container được phát triển và triển khai một cách an toàn.
5. **Web Application Scanning**: Quét ứng dụng web để tìm lỗ hổng và các vấn đề bảo mật khác trong ứng dụng web của bạn.
6. **Compliance Management**: Hỗ trợ tổ chức đảm bảo tuân thủ với các quy định và tiêu chuẩn bảo mật thông qua việc đánh giá và theo dõi hiệu suất tuân thủ.
7. **Threat Intelligence**: Cung cấp thông tin về các mối đe dọa hiện tại và tiềm ẩn để giúp bạn xác định các yếu điểm yếu trong hệ thống của mình.
8. **Cloud Security**: Hỗ trợ quét và đánh giá môi trường đám mây của bạn, bao gồm cả các dự án đám mây công cộng và riêng tư.
9. **Nessus Scanning**: Sản phẩm Nessus của Tenable là một công cụ quét lỗ hổng nổi tiếng, giúp phát hiện các lỗ hổng bảo mật trong các thiết bị và ứng dụng.
10. **Integrations**: Cung cấp tích hợp với các công cụ và nền tảng khác, giúp tổ chức quản lý rủi ro và bảo mật một cách hiệu quả.

Ref: [https://www.tenable.com/](https://www.tenable.com/%20)

**McAfee**

Các tính năng:

* **ePolicy Orchestrator®** 
  + Quản lý đa sản phẩm: ePO cho phép bạn quản lý nhiều sản phẩm bảo mật McAfee khác nhau từ một nền tảng duy nhất. Bạn có thể cấu hình chính sách, triển khai cập nhật, và theo dõi trạng thái bảo mật từ một điểm duy nhất.
  + Tự động hóa: ePO cung cấp khả năng tự động hóa nhiều tác vụ bảo mật, giúp giảm thiểu công sức quản lý và tối ưu hóa bảo mật.
* **Data Exchange Layer (DXL)** 
  + Giao tiếp tức thì: DXL cho phép các ứng dụng và sản phẩm bảo mật giao tiếp với nhau một cách tức thì, chia sẻ thông tin về các mối đe dọa bảo mật và hoạt động độc hại.
  + Kết nối tới hệ thống bên ngoài: DXL có khả năng kết nối với các hệ thống và ứng dụng bảo mật bên ngoài của McAfee, giúp cải thiện tích hợp với các giải pháp khác.
* **McAfee® Active Response (MAR)** 
  + Phân tích trong thời gian thực: MAR cho phép phân tích và điều tra các mối đe dọa bảo mật trong thời gian thực, giúp tổ chức đối phó nhanh chóng với các cuộc tấn công.
  + Xác định đối tượng độc hại: MAR có khả năng xác định các đối tượng độc hại và cách chúng hoạt động, giúp tổ chức đánh giá và đối phó với các rủi ro.
* **McAfee® Enterprise Security Manager (ESM)** 
  + SIEM mạnh mẽ: ESM là một hệ thống SIEM mạnh mẽ cho phép tổng hợp và phân tích dữ liệu sự kiện từ nhiều nguồn khác nhau để xác định các mối đe dọa và rủi ro.
  + Báo cáo và tuân thủ: ESM cung cấp khả năng tạo báo cáo bảo mật và đảm bảo tuân thủ với các quy định và tiêu chuẩn bảo mật.

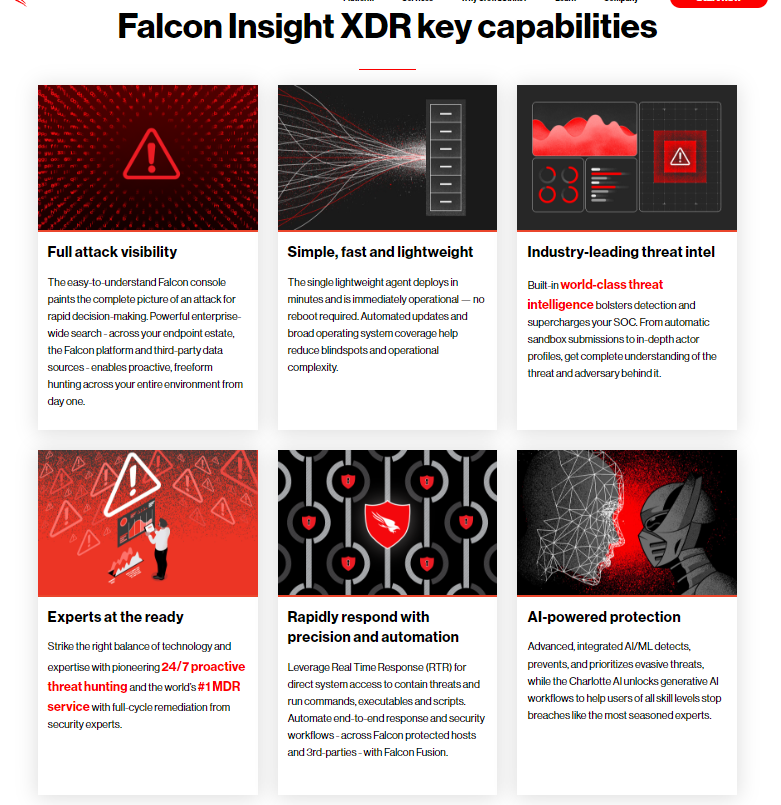
**The McAfee® Data Exchange Layer (DXL)** framework cho phép liên lạc hai chiều giữa các điểm cuối trên mạng. Nó kết nối nhiều sản phẩm và ứng dụng, chia sẻ dữ liệu và điều phối các tác vụ bảo mật bằng cách sử dụng khung ứng dụng thời gian thực được gọi là kết cấu Data Exchange Layer fabric.

DXL nhận và gửi tin nhắn được mã hóa qua kết cấu để theo dõi hoạt động, rủi ro cũng như các mối đe dọa và thực hiện hành động trong thời gian thực.. The DXL framework:

* Rút ngắn quy trình làm việc để tìm kiếm và ứng phó với các mối đe dọa. Việc chia sẻ thông tin gần như tức thời giúp giảm thời gian phát hiện, ngăn chặn và khắc phục các mối đe dọa mới được xác định.
* Sử dụng OpenDXL để kết nối các sản phẩm từ các nhà cung cấp khác nhau với các ứng dụng và công cụ của riêng bạn, giảm bớt những thách thức và sự phức tạp khi tích hợp. Nó cho phép liên lạc giữa nhiều sản phẩm để chúng có thể nhanh chóng chia sẻ dữ liệu về mối đe dọa mà chúng tạo ra, làm tăng giá trị của các ứng dụng bạn triển khai.

**Crowdstrike**

* **Crowdstrike Falcon Prevent Antivirus:**
* State-of-the-art prevention
* Secure your estate in seconds
* Streamline operations and boost productivity
* **Crowdstrike Falcon Insight XDR**



* **Crowdstrike Falcon Firewall Management**
  + Simple firewall policy management
  + Reduced complexity
  + Logging, troubleshooting and compliance
* **Crowdstrike Falcon Device Control**
  + Mitigate USB device risk
  + Achieve automatic threat visibility
  + Streamline policy management
* **Crowdstrike Falcon Sanbox Malware**
  + Visibility into unknown and advanced threats
  + Analysis is expanded to include the entire threat
  + Security teams are empowered
  + Flexible deployment finds the right balance
  + Easily integrate into your workflow

[https://www.crowdstrike.com/products/endpoint-security/falcon-prevent-antivirus/](https://www.crowdstrike.com/products/endpoint-security/falcon-prevent-antivirus/%20)

[https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/](https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/%20)

[https://www.crowdstrike.com/products/endpoint-security/falcon-firewall-management/](https://www.crowdstrike.com/products/endpoint-security/falcon-firewall-management/%20)

[https://www.crowdstrike.com/products/endpoint-security/falcon-device-control/](https://www.crowdstrike.com/products/endpoint-security/falcon-device-control/%20)

[https://www.crowdstrike.com/products/threat-intelligence/falcon-sandbox-malware-analysis/](https://www.crowdstrike.com/products/threat-intelligence/falcon-sandbox-malware-analysis/%20)

**Palo Alto Network**

The Palo Alto Networks next-generation firewalls provide granular control over the traffic allowed to access your network. The primary features and benefits include:

* **Application-based policy enforcement (App-ID**™**)**

Kiểm soát truy cập theo loại ứng dụng sẽ hiệu quả hơn nhiều khi nhận dạng ứng dụng không chỉ dựa trên giao thức và số cổng. Dịch vụ App-ID có thể chặn các ứng dụng có rủi ro cao cũng như hành vi có rủi ro cao, chẳng hạn như chia sẻ tệp và lưu lượng truy cập được mã hóa bằng giao thức Lớp cổng bảo mật (SSL) có thể được giải mã và kiểm tra.

* **User identification (User-ID™)**

Tính năng User-ID cho phép quản trị viên định cấu hình và thực thi các chính sách tường lửa dựa trên người dùng và nhóm người dùng thay vì hoặc ngoài các vùng và địa chỉ mạng. Tường lửa có thể giao tiếp với nhiều máy chủ thư mục, chẳng hạn như Microsoft Active Directory, eDirectory, SunOne, OpenLDAP và hầu hết các máy chủ thư mục dựa trên LDAP khác để cung cấp thông tin người dùng và nhóm cho tường lửa. Sau đó, bạn có thể sử dụng thông tin này để hỗ trợ ứng dụng an toàn có thể được xác định cho mỗi người dùng hoặc nhóm. Ví dụ: quản trị viên có thể cho phép một tổ chức sử dụng ứng dụng dựa trên web nhưng không cho phép bất kỳ tổ chức nào khác trong công ty sử dụng cùng ứng dụng đó. Bạn cũng có thể định cấu hình kiểm soát chi tiết đối với một số thành phần nhất định của ứng dụng dựa trên người dùng và nhóm

* **Threat prevention**

Các dịch vụ ngăn chặn mối đe dọa bảo vệ mạng khỏi vi-rút, sâu, phần mềm gián điệp và lưu lượng độc hại khác có thể khác nhau tùy theo ứng dụng và nguồn lưu lượng truy cập

* **URL filtering**

Các kết nối ra ngoài có thể được lọc để ngăn truy cập vào các trang web không phù hợp

* **Traffic visibility**

Báo cáo, nhật ký và cơ chế thông báo mở rộng cung cấp khả năng hiển thị chi tiết về các sự kiện bảo mật và lưu lượng ứng dụng mạng. Application Command Center (ACC) trong giao diện web xác định các ứng dụng có lưu lượng truy cập nhiều nhất và có rủi ro bảo mật cao nhất

* **Networking versatility and speed**

The Palo Alto Networks firewall có thể tăng cường hoặc thay thế tường lửa hiện có của bạn và có thể được cài đặt minh bạch trong bất kỳ mạng nào hoặc được định cấu hình để hỗ trợ môi trường chuyển mạch hoặc định tuyến. Tốc độ đa gigabit và kiến trúc một đường truyền cung cấp các dịch vụ này cho bạn mà ít hoặc không ảnh hưởng đến độ trễ mạng.

* **GlobalProtect**

The GlobalProtect™ software cung cấp bảo mật cho hệ thống máy khách, chẳng hạn như máy tính xách tay được sử dụng tại hiện trường, bằng cách cho phép đăng nhập dễ dàng và an toàn từ mọi nơi trên thế giới.

* **Fail-safe operation**

High availability (HA) cung cấp khả năng chuyển đổi dự phòng tự động trong trường hợp có bất kỳ sự gián đoạn phần cứng hoặc phần mềm nào

* **Malware analysis and reporting**

The WildFire™ cloud-based cung cấp phân tích và báo cáo chi tiết về phần mềm độc hại đi qua tường lửa. Việc tích hợp với dịch vụ thông tin về mối đe dọa AutoFocus™ cho phép bạn đánh giá rủi ro liên quan đến lưu lượng truy cập mạng của mình ở cấp độ tổ chức, ngành và toàn cầu.

**VM-Series firewall**

A [VM-Series firewall](https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/about-the-vm-series-firewall#:~:text=The%20Palo%20Alto%20Networks%20VM,VM%2DSeries%20Deployments) cung cấp phiên bản ảo của PAN-OS® được định vị để sử dụng trong môi trường trung tâm dữ liệu ảo hóa và lý tưởng cho môi trường điện toán đám mây riêng, công cộng và đám mây lai của bạn.

* **Management and Panorama**

Bạn có thể quản lý từng tường lửa thông qua giao diện web trực quan hoặc thông qua giao diện dòng lệnh (CLI) hoặc bạn có thể quản lý tập trung tất cả các tường lửa thông qua hệ thống quản lý tập trung [Panorama](https://docs.paloaltonetworks.com/panorama)™, có giao diện web rất giống với giao diện web trên tường lửa của Palo Alto Networks.

Ref: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/web-interface-basics/features-and-benefits>

**CyberArk PAM**

PAM (Privileged Access Management) tập trung vào việc bảo vệ và quản lý các tài khoản và quyền truy cập đặc quyền đến hệ thống và dữ liệu nhạy cảm. Các giải pháp PAM của CyberArk được thiết kế để giúp các tổ chức đối phó với các mối đe dọa an ninh, việc xâm nhập vào hệ thống và tấn công từ bên trong bằng cách kiểm soát và theo dõi quyền truy cập đặc quyền và thông tin đăng nhập.

1. **Credential Management:** CyberArk giúp tổ chức lưu trữ, quản lý và xoay các thông tin đăng nhập của tài khoản đặc quyền, chẳng hạn như mật khẩu và khóa SSH một cách an toàn.
2. **Privileged Session Management:** Nó cho phép tổ chức theo dõi, ghi âm và kiểm tra các phiên làm việc liên quan đến các tài khoản đặc quyền, cung cấp thông tin chi tiết về ai đã truy cập điều gì và khi nào.
3. **Access Control:** Giải pháp PAM của CyberArk cho phép tổ chức xác định và thực thi chính sách về ai có quyền truy cập vào hệ thống, ứng dụng và dữ liệu cụ thể, đảm bảo chỉ có những người được ủy quyền mới được truy cập.
4. **Just-In-Time Access:** Tính năng này cung cấp quyền truy cập tạm thời và theo yêu cầu đối với các tài khoản đặc quyền, giảm nguy cơ liên quan đến việc duy trì tài khoản đặc quyền luôn hoạt động.
5. **Multi-Factor Authentication (MFA):** CyberArk hỗ trợ xác minh đa yếu tố để tăng cường bảo mật, đảm bảo rằng ngay cả khi mật khẩu bị xâm nhập, kẻ tấn công sẽ cần một yếu tố xác minh bổ sung để truy cập.
6. **Credential Vault:** Kho thông tin đăng nhập an toàn của CyberArk được sử dụng để lưu trữ, quản lý và xoay mật khẩu và khóa một cách an toàn, giảm nguy cơ truy cập trái phép.
7. **Privileged Threat Analytics:** Tính năng này giúp tổ chức phát hiện và đáp ứng trước hành vi đáng ngờ hoặc bất thường liên quan đến các tài khoản đặc quyền và quyền truy cập.
8. **Compliance and Audit Reporting:** Giải pháp PAM của CyberArk cung cấp khả năng báo cáo và theo dõi để giúp tổ chức chứng minh tuân thủ với các quy định và chính sách an ninh
9. **Integration:** Giải pháp PAM của CyberArk có khả năng tích hợp với nhiều công cụ và công nghệ bảo mật khác để tạo ra một hệ thống an ninh toàn diện..

**AWS WAF**

* **Web traffic filtering**

AWS WAF cho phép bạn tạo quy tắc để lọc lưu lượng truy cập web dựa trên các điều kiện bao gồm địa chỉ IP, tiêu đề và nội dung HTTP hoặc URI tùy chỉnh. Điều này cung cấp cho bạn một lớp bảo vệ bổ sung khỏi các cuộc tấn công web nhằm khai thác lỗ hổng trong các ứng dụng web tùy chỉnh hoặc của bên thứ ba. Ngoài ra, AWS WAF còn giúp bạn dễ dàng tạo các quy tắc chặn các hoạt động khai thác web phổ biến như chèn SQL và tạo tập lệnh chéo trang.

AWS WAF cho phép bạn tạo một bộ quy tắc tập trung mà bạn có thể triển khai trên nhiều trang web. Điều này có nghĩa là trong môi trường có nhiều trang web và ứng dụng web, bạn có thể tạo một bộ quy tắc duy nhất mà bạn có thể sử dụng lại trên các ứng dụng thay vì tạo lại quy tắc đó trên mọi ứng dụng bạn muốn bảo vệ.

* **AWS WAF Bot Control**

AWS WAF Bot Control là một nhóm quy tắc được quản lý cung cấp cho bạn khả năng hiển thị và kiểm soát lưu lượng bot phổ biến và lan rộng có thể tiêu tốn quá nhiều tài nguyên, làm lệch số liệu, gây ra thời gian ngừng hoạt động hoặc thực hiện các hoạt động không mong muốn khác. Chỉ với một vài cú nhấp chuột, bạn có thể chặn hoặc giới hạn tỷ lệ các bot phổ biến, chẳng hạn như máy quét, máy quét và trình thu thập thông tin hoặc bạn có thể cho phép các bot phổ biến, chẳng hạn như trình giám sát trạng thái và công cụ tìm kiếm. Nhóm quy tắc được quản lý Kiểm soát Bot có thể được sử dụng cùng với các Quy tắc được quản lý khác cho WAF hoặc các quy tắc WAF tùy chỉnh của riêng bạn để bảo vệ ứng dụng của bạn.

* **Account Takeover Fraud Prevention**

Account Takeover Fraud Prevention - Ngăn chặn chiếm đoạt tài khoản là nhóm quy tắc được quản lý nhằm giám sát trang đăng nhập ứng dụng của bạn để phát hiện truy cập trái phép vào tài khoản người dùng bằng thông tin xác thực bị xâm phạm. Bạn có thể sử dụng nhóm quy tắc để giúp bảo vệ khỏi các cuộc tấn công nhồi thông tin xác thực, các nỗ lực đăng nhập cưỡng bức và các hoạt động đăng nhập bất thường khác. Với JavaScript và SDK iOS/Android tùy chọn, bạn có thể nhận được dữ liệu đo từ xa bổ sung trên các thiết bị của người dùng cố gắng đăng nhập vào ứng dụng của bạn để bảo vệ ứng dụng của bạn tốt hơn trước các nỗ lực đăng nhập tự động của bot. Ngăn chặn chiếm đoạt tài khoản là một phần của Quy tắc được quản lý dành cho AWS và có thể được sử dụng cùng với Kiểm soát Bot để bảo vệ ứng dụng của bạn một cách hiệu quả trước các cuộc tấn công của bot.

* **Account Creation Fraud Prevention**

Account Creation Fraud Prevention là một nhóm quy tắc được quản lý nhằm giám sát trang đăng ký hoặc đăng ký trong ứng dụng của bạn để phát hiện việc tạo tài khoản giả mạo hoặc gian lận. Bạn có thể sử dụng nhóm quy tắc để giúp bảo vệ khỏi các hành vi lạm dụng như lạm dụng quảng cáo hoặc đăng ký, lạm dụng lòng trung thành hoặc phần thưởng và lừa đảo. Với JavaScript và SDK iOS/Android được đề xuất, bạn có thể nhận được dữ liệu đo từ xa bổ sung trên các thiết bị của người dùng cố gắng đăng ký vào ứng dụng của bạn để bảo vệ ứng dụng của bạn tốt hơn trước các nỗ lực tự động của bot. Ngăn chặn gian lận khi tạo tài khoản là một phần của Quy tắc được quản lý dành cho AWS và có thể được sử dụng cùng với Kiểm soát Bot để bảo vệ ứng dụng của bạn một cách hiệu quả trước các cuộc tấn công của bot.

* **Full feature API**

AWS WAF có thể được quản lý hoàn toàn thông qua API. Điều này cung cấp cho các tổ chức khả năng tạo và duy trì các quy tắc một cách tự động và kết hợp chúng vào quá trình thiết kế và phát triển. Ví dụ: nhà phát triển có kiến ​​thức chi tiết về ứng dụng web có thể tạo quy tắc bảo mật như một phần của quy trình triển khai. Khả năng kết hợp bảo mật vào quá trình phát triển của bạn giúp tránh được sự cần thiết phải chuyển giao phức tạp giữa các nhóm ứng dụng và bảo mật để đảm bảo các quy tắc được cập nhật.

AWS WAF cũng có thể được triển khai và cung cấp tự động với các mẫu mẫu AWS CloudFormation cho phép bạn mô tả tất cả các quy tắc bảo mật mà bạn muốn triển khai cho các ứng dụng web do Amazon CloudFront phân phối.

* **Real-time visibility**

AWS WAF cung cấp số liệu theo thời gian thực và ghi lại các yêu cầu thô bao gồm thông tin chi tiết về địa chỉ IP, vị trí địa lý, URI, Tác nhân người dùng và Người giới thiệu. AWS WAF được tích hợp hoàn toàn với Amazon CloudWatch, giúp dễ dàng thiết lập cảnh báo tùy chỉnh khi vượt quá ngưỡng hoặc xảy ra các cuộc tấn công cụ thể. Thông tin này cung cấp thông tin có giá trị có thể được sử dụng để tạo các quy tắc mới nhằm bảo vệ ứng dụng tốt hơn.

* **Integration with AWS Firewall Manager**

Bạn có thể đặt cấu hình và quản lý tập trung việc triển khai AWS WAF trên nhiều tài khoản AWS bằng cách sử dụng Trình quản lý tường lửa AWS. Khi các tài nguyên mới được tạo, bạn có thể đảm bảo rằng chúng tuân thủ một bộ quy tắc bảo mật chung. Trình quản lý tường lửa tự động kiểm tra và thông báo cho nhóm bảo mật của bạn khi có vi phạm chính sách để họ có thể phản hồi và thực hiện hành động ngay lập tức. Để tìm hiểu thêm về Trình quản lý tường lửa,

[REF: https://aws.amazon.com/vi/waf/features/](REF:%20https://aws.amazon.com/vi/waf/features/)

**SAN**

[**SAN**](https://bizflycloud.vn/tin-tuc/san-la-gi-20210712105534908.htm), viết tắt của Storage Area Network, là mạng chuyên dụng để kết nối các Server và thiết bị lưu trữ nhằm mục đích truyền tải dữ liệu giữa các phần tử lưu trữ với nhau và giữa hệ thống máy tính và phần tử lưu trữ.

Mạng SAN tách biệt hoàn toàn với các mạng LAN và WAN. SAN có khả năng kết nối tất cả các tài nguyên lưu trữ trong mạng với nhau. Vì SAN là mạng tốc độ cao dành riêng cho việc lưu trữ và quản trị dữ liệu, do đó người dùng có thể sử dụng và quản trị tài nguyên lưu trữ hiệu quả hơn, giúp quản lý tập trung các thao tác nhằm tăng độ an toàn, đồng thời sao lưu và khôi phục khi xảy ra sự cố.

**Tại sao nên sử dụng SAN?**

**Khắc phục vấn đề suy giảm băng thông mạng LAN**

Một lợi ích chủ chốt của SAN là cải thiện băng thông. Do dữ liệu thường chiếm lượng lớn băng thông trong mạng, các máy chủ lưu trữ trên mạng LAN thường phải đối mặt với nghẽn đường truyền khiến giảm hiệu năng và tăng độ trễ. SAN giúp chia sẻ gánh nặng băng thông dữ liệu và do đó tăng băng thông tổng thể của hệ thống mạng LAN.

**Tăng cường bảo mật dữ liệu**

SAN lưu trữ và áp dụng các thuật toán bảo vệ một cách nhất quán cho dữ liệu, đảm bảo tính toàn vẹn dữ liệu trong mọi trường hợp. Ngoài ra, SAN giúp giảm thiểu nguy cơ tin tặc tấn công vào mạng LAN và xâm +phạm dữ liệu do mọi thứ đã được lưu trữ trên một hệ thống tách biệt.

**Sao lưu khôi phục dễ dàng**

Sao lưu (backup) luôn là yếu tố chủ chốt khi xét đến hiệu suất mạng dữ liệu. SAN giúp quá trình sao lưu dữ liệu đơn giản hơn khi chỉ cần một máy chủ sao lưu duy nhất để sao lưu dữ liệu từ nhiều vị trí. Dung lượng lưu trữ linh hoạt của SAN cũng giúp bạn không phải chi thêm tiền cho các giải pháp lưu trữ vật lý cho dữ liệu của mình.

Các hệ thống SAN mới hiện nay lưu trữ tập tin tại nhiều vùng vật lý khác nhau (clone), cho phép khôi phục dữ liệu cực nhanh khi một thiết bị lưu trữ bị lỗi hay không truy cập được.

**Tăng khả năng mở rộng**

Bộ nhớ trong SAN được quản lý và cấu hình tập trung, điều đó có nghĩa là việc tăng giảm quy mô lưu trữ có thể được thực hiện linh hoạt và dễ dàng để thích ứng với nhu cầu của doanh nghiệp trong từng giai đoạn.

**Tính năng trong SAN**

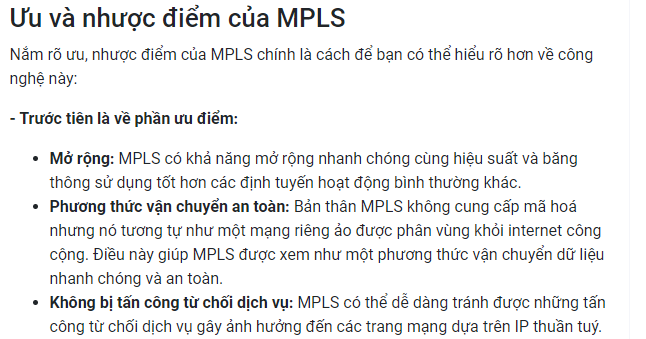
* Hỗ trợ cơ sở hạ tầng đa giao thức bao gồm FC, iSCSI, và FCIP.
* Khả năng nhập xuất với tốc độ cao.
* Tách biệt thiết bị lưu trữ và Server giúp tăng cường bảo mật.
* Cung cấp tính năng xác thực, cấp quyền, điều khiển truy xuất và khả năng quản lý theo vùng.
* Khả năng ứng dụng cao: Với những đặc tính nổi trội như khoảng cách kết nối được mở rộng, hỗ trợ IP và các thiết bị mạng, SAN cho phép cấu hình các mạng phức tạp để quản lý lưu trữ nâng cao và áp dụng kỹ thuật clustering cho server-storage.
* Dễ dàng chia sẻ lưu trữ cũng như quản lý thông tin nhờ tính chất tập trung.
* Mở rộng lưu trữ dễ dàng bằng cách bổ sung bộ nhớ mà không cần cấu hình lại các thiết bị khác.
* Cho phép nhiều máy chủ có thể cùng chia sẻ một thiết bị lưu trữ.
* Bảo trì và nâng cấp dễ dàng với khả năng năng sao lưu dữ liệu nội bộ. Tiết kiệm băng thông mạng LAN khi thực hiện các thao tác backup (LAN-free backup).
* SAN có thể dựa trên một số loại giao diện kết nối tốc độ cao. Nhiều mạng SAN ngày nay cũng sử dụng phối hợp nhiều giao diện khác nhau (Ví dụ: giao diện FC - Fibre Channel).
* Đặc biệt thích hợp với các ứng dụng cần tốc độ cao (Ví dụ: các ứng dụng xử lý giao dịch trong ngành ngân hàng, tài chính…).

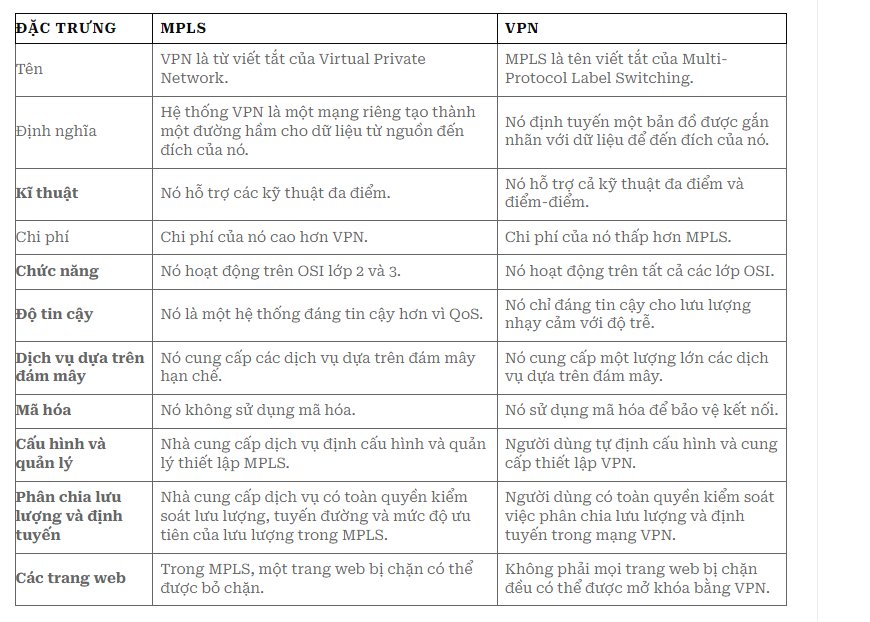
**MPLS**

[**MPLS**](https://bizflycloud.vn/tin-tuc/mpls-la-gi-202204281143151.htm) (Multiprotocol Label Switching) là một loại công nghệ chuyển tiếp dữ liệu có khả năng thông qua các đường dẫn mạng được định sẵn trong kỹ thuật MPLS để gia tăng tốc độ kết nối mạng internet và kiểm soát luồng lưu lượng mạng. Thay vì yêu cầu tra cứu phức tạp hơn trong bảng định tuyến tại những nơi mà các dữ liệu dừng lại thì chúng sẽ được truyền dẫn qua các label với MPLS.

Hiểu đơn giản, mạng internet sẽ thực hiện việc chuyển ngẫu nhiên các packet từ router này sang router khác và đến packet cuối cùng để các dữ liệu mạng có thể hoạt động được. Điều này sẽ gây tốn rất nhiều thời gian khi người dùng thực hiện truy xuất.

Với MPLS, công nghệ này đã xác định được trước đường truyền và packet đích để chuyển dẫn theo đường dẫn. Do đó, các router tiết kiệm được nhiều thời gian hơn trong việc đưa ra quyết định nơi mà các gói tin chuyển phát đến và đảm bảo các gói tin này sẽ luôn đi theo một đường dẫn. Như vậy, tốc độ mạng sẽ được tăng tốc đáng kể.





REF: https://bizflycloud.vn/tin-tuc/mpls-la-gi-202204281143151.htm

**VMware vSphere**

Các tính năng của VMware vSphere bao gồm:

* Hypervisor: VMware vSphere sử dụng hypervisor để tạo ra môi trường ảo hóa và quản lý phân bổ tài nguyên giữa các máy chủ ảo.
* vCenter Server: Giúp quản lý các máy chủ ảo, tài nguyên ảo và mạng ảo trên một giao diện đồng nhất. Nó cung cấp các tính năng quản lý như vMotion, High Availability (HA), Distributed Resource Scheduler (DRS) và Update Manager.
* vMotion: Cho phép di chuyển máy chủ ảo từ một máy chủ vật lý sang một máy chủ vật lý khác mà không ảnh hưởng đến hoạt động của ứng dụng.
* High Availability (HA): Đảm bảo tính sẵn sàng cao cho các ứng dụng bằng cách tự động khởi động lại các máy chủ ảo trên các máy chủ vật lý khác trong trường hợp máy chủ ảo gặp sự cố.
* Distributed Resource Scheduler (DRS): Tự động phân bổ tài nguyên giữa các máy chủ ảo để đảm bảo hiệu suất tối ưu cho các ứng dụng.
* Fault Tolerance (FT): Giúp tăng tính sẵn sàng cao cho các ứng dụng bằng cách tạo một bản sao đang chạy của máy chủ ảo trên một máy chủ khác, đảm bảo rằng ứng dụng sẽ không bị gián đoạn nếu máy chủ gặp sự cố.
* vSphere Replication: Cho phép sao lưu và phục hồi dữ liệu của các máy chủ ảo giữa các máy chủ vật lý khác nhau.
* vSphere Storage APIs: Cung cấp giao diện lập trình ứng dụng (API) cho phép quản lý lưu trữ và tích hợp với các giải pháp lưu trữ khác.
* vSphere Web Client: Cung cấp giao diện web để quản lý hạ tầng ảo hóa trên các thiết bị di động và máy tính.
* vRealize Operations: Cung cấp giám sát, phân tích và tối ưu hoá hạ tầng ảo hóa và ứng dụng.
* **Tăng hiệu quả sử dụng tài nguyên máy chủ**: VMware vSphere cho phép các doanh nghiệp sử dụng tài nguyên máy chủ hiệu quả hơn bằng cách tạo ra nhiều máy chủ ảo trên một máy chủ vật lý, giúp tiết kiệm chi phí đầu tư phần cứng.
* **Tăng tính sẵn sàng cao cho hạ tầng IT**: VMware vSphere cung cấp các tính năng như vMotion, High Availability (HA), Fault Tolerance (FT) và vSphere Replication giúp đảm bảo rằng các ứng dụng luôn có sẵn để sử dụng.
* **Quản lý hạ tầng ảo hóa dễ dàng**: vCenter Server giúp quản lý các máy chủ ảo, tài nguyên ảo và mạng ảo trên một giao diện đồng nhất. Nó cung cấp các tính năng quản lý như vMotion, High Availability (HA), Distributed Resource Scheduler (DRS) và Update Manager.
* **Giảm thiểu thời gian gián đoạn dịch vụ**: VMware vSphere cho phép các doanh nghiệp thực hiện bảo trì và cập nhật hạ tầng IT mà không ảnh hưởng đến hoạt động của các ứng dụng.
* **Tăng tính linh hoạt cho hạ tầng IT**: VMware vSphere cho phép các doanh nghiệp tăng hoặc giảm kích thước hạ tầng IT dễ dàng bằng cách thêm hoặc xóa các máy chủ ảo mà không cần phải thay đổi phần cứng vật lý.
* **Cung cấp dịch vụ máy chủ ảo**: VMware vSphere cung cấp các tính năng giúp các nhà cung cấp dịch vụ đám mây cung cấp dịch vụ máy chủ ảo cho khách hàng của họ.
* **Giảm thiểu tiêu thụ điện năng và khí thải**: VMware vSphere cho phép các doanh nghiệp giảm tiêu thụ điện năng và khí thải bằng cách giảm số lượng máy chủ vật lý và tăng hiệu quả sử dụng tài nguyên.
* **vCenter**
* vCenter là một phần mềm về cơ sở dữ liệu thuộc bộ giải pháp vSphere. Nó cho phép người dùng quản lý tài nguyên, giám sát tập trung và bảo mật cho cơ sở hạ tầng ảo VMWare vSphere một cách dễ dàng. vCenter Server sử dụng các cơ sở dữ liệu back-end để lưu trữ toàn bộ dữ liệu về các máy ảo và máy chủ.
* Thông qua một bảng điều khiển duy nhất, vCenter cho phép quản trị viên của hệ thống vSphere quản lý nhiều máy chủ ESX, ESXi và máy ảo VM. vSphere có nhiều tính năng chính như VMWare Distributed Resource Scheduler (DRS). Hay vSphere Fault Tolerance, VMWare vMotion, vSphere High Av available và yêu cầu hoạt động vCenter Server. Nó sẽ hợp lý hoá việc triển khai VM.
* Các tính năng ảo hóa của VMware vSphere
* Phần mềm VMware vSphere bao gồm các sản phẩm có nhiều các chức năng, đầy đủ công cụ, tính năng để ảo hóa như:
* Di chuyển nhanh chóng các máy ảo sang một hệ thống khác mà không có downtime.
* Di chuyển động các máy ảo sang các phân vùng storage khác mà không có downtime.
* Hỗ trợ mở rộng tài nguyên CPU, RAM của host, không cần có downtime.
* Bảo mật dữ liệu, thực hiện backup và restore các máy ảo.
* Đảm bảo tính liên tục của ứng dụng ngay cả trong tình huống server bị lỗi mà dữ liệu không bị mất.
* Cho phép các bên thứ 3 sử dụng các APIs này cho các ứng dụng backup.
* Quản lý tập trung tài nguyên các server thành 1 khối và tự động cân bằng tải.
* Đảm bảo tính liên tục của công việc khi một hệ thống có lỗi.
* Cho phép tạo, cấu hình và duy trì các vùng bảo mật riêng biệt.
* Quản lý tập trung và theo dõi các kết nối mạng sử dụng cluster-level.
* Quản lý, theo dõi và tự động cân bằng tải trên các thiết bị storage và network.
* Tạo các máy ảo thông qua các template.
* Tự động triển khai các host với ESXi.
* Lựa chọn storage theo các policy đã định nghĩa sẵn.
* Tự động cân bằng tải trên storage.
* Kết hợp các traffic từ nhiều cổng song song vào 1 giao diện quản lý.