Palo Alto Network – Nextgen Firewalls

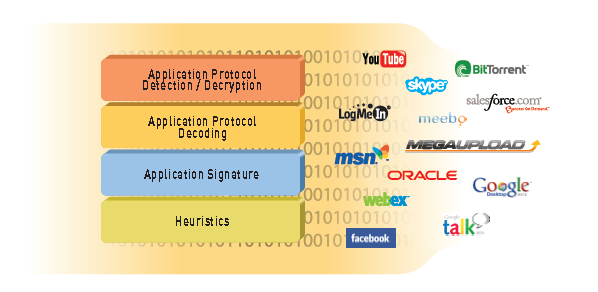
The Palo Alto Networks next-generation firewalls provide granular control over the traffic allowed to access your network. The primary features and benefits include:

* **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 provides 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 Toàn cảnh™, 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>

McAfee – Nextgen IPS

**Các tính năng:**

* **Unparalleled threat prevention**
* Next-generation architecture
* Advanced botnet detection
* Behavior-based analysis
* **Comprehensive malware protection**
  + Signature-less, advanced malware analysis
  + Malware investigation dashboard
  + Predictive malware detection via McAfee GTI
* **Security Connected**
* Real-time host context via McAfee ePO software
* McAfee GTI
* Integrated forensic analysis
* **Performance and availability**
* Up to 20 Gbps throughput
* Industry-leading reliability
* Active-active high availability
* **Intelligent security management**
  + Scalable web-based management
  + Intelligent alert prioritization
  + Progressive disclosure workflows
* **Visibility and control**
* Application identification
* User identification
* Device identification
* **Advanced intrusion prevention**
* IP defragmentation and TCP stream reassembly
* Anomaly detection
* McAfee, user-defined, and open-source signatures
* Host quarantine
* Advanced evasion protection
* Inspection of virtual environments
* **Botnet protection**
* Heuristic bot detection
* Multi-attack correlation
* Command and control database
* **DoS and DDoS prevention**
* Threshold and heuristic-based detection
* Host-based connection limiting
* Self-learning profile-based detection
* **McAfee GTI**
* File reputation
* IP reputation
* Geo-location
* **High availability**
* Active-active with stateful failover
* External fail-open (active)
* Built-in fail-open (for copper ports only)
* **Protocol tunneling support**
* IPv6
* V4-in-V4, V4-in-V6, V6-in-V4, and V6-in-V6 tunnels
* MPLS
* GRE
* Q-in-Q Double VLAN
* **McAfee Network Security Manager**
* Tiered management, up to 1,000 sensors
* User authentication (Radius, LDAP, and TACACS)
* Automated failover and fail-back
* Disaster recovery of critical configuration data
* Centralized, hierarchical policy management

**Ref:**

[**https://websecurityworks.com/Network-Security-Platform-M-1250.asp**](https://websecurityworks.com/Network-Security-Platform-M-1250.asp)

[**https://www.websecurityworks.com/datasheets/ds-network-security-platform-m-series\_new.pdf**](https://www.websecurityworks.com/datasheets/ds-network-security-platform-m-series_new.pdf)

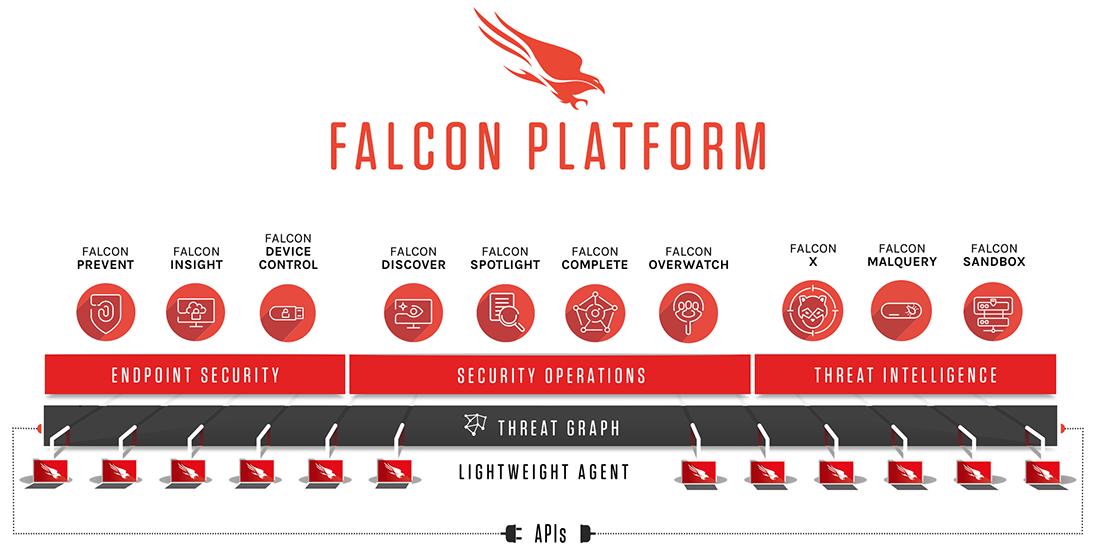
CyberArk PAM

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.

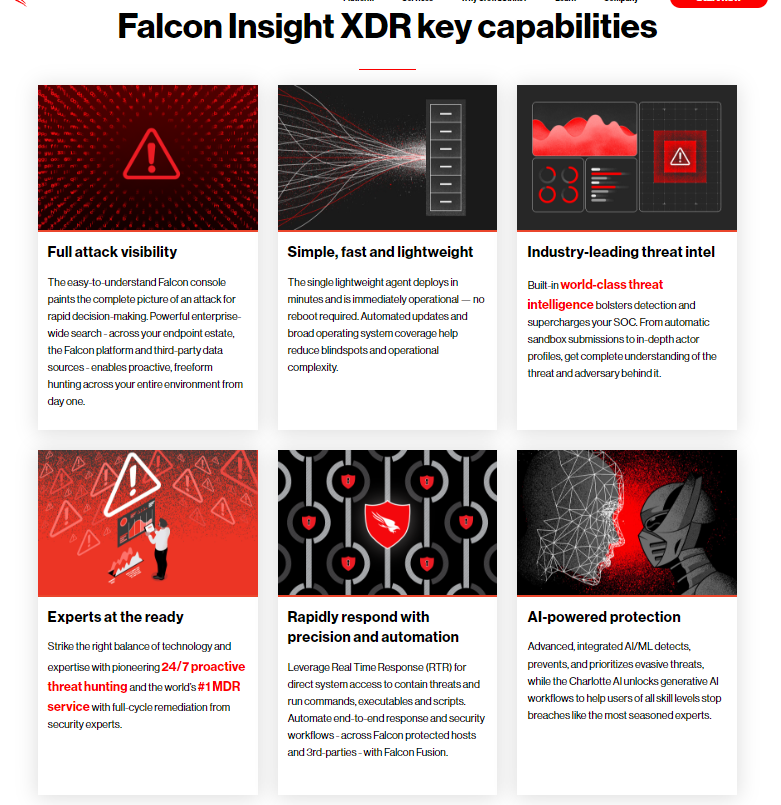
1. **Credential Management:** CyberArk giúp tổ chức lưu trữ, quản lý và xoay các thông tin đăng nhập của tài khoản đặc quyền, chẳng hạn như mật khẩu và khóa SSH một cách an toàn.
2. **Privileged Session Management:** Nó cho phép tổ chức theo dõi, ghi âm và kiểm tra các phiên làm việc liên quan đến các 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..

Ref: <https://docs.cyberark.com/PAS/11.4/en/Content/PASIMP/OPM-PAM-LP.htm>

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)

TENABLE:

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

Mô tả được tạo tự động

**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)

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/>

IBM

**QRadar SIEM**

* **Phân tích mối đe dọa mạng:** QRadar SIEM kết hợp liền mạch dữ liệu hành vi mạng vào phân tích mối đe dọa để tương quan và phát hiện các mối đe dọa.
* **Phân tích hành vi người dùng (UBA):** Có được khả năng hiển thị rõ ràng hơn về các mối đe dọa nội bộ, phát hiện hành vi bất thường, nhanh chóng xác định những người dùng có nguy cơ cao và tạo ra những hiểu biết có ý nghĩa.
* **Thông tin về mối đe dọa**: Hiểu bối cảnh mối đe dọa mới nhất bằng cách tận dụng các địa chỉ IP độc hại, URL và tệp băm tệp phần mềm độc hại mới nhất từ ​​X-Force Threat Intelligence và các nguồn thông tin về mối đe dọa khác.
* **Tối đa hóa thời gian và tài năng của nhà phân tích**

Trải nghiệm sức mạnh của AI cấp doanh nghiệp của IBM được thiết kế để nâng cao hiệu quả và chuyên môn của mọi nhóm bảo mật. Với QRadar SIEM, các nhà phân tích có thể giảm bớt các công việc thủ công lặp đi lặp lại như tạo trường hợp và ưu tiên rủi ro để tập trung vào các nỗ lực điều tra và khắc phục quan trọng.

* **Tăng tốc phát hiện và ứng phó mối đe dọa**

Phá vỡ các cuộc tấn công mạng nâng cao và phản hồi nhanh hơn với nội dung tiên tiến bao gồm tích hợp gốc với cộng đồng SIGMA nguồn mở. Không cần bối cảnh bổ sung với dữ liệu sự kiện nhật ký tương quan, bao gồm IBM X-Force Threat Intelligence, phân tích hành vi người dùng và phân tích mạng.

* **Giảm độ phức tạp trong vận hành**

Dễ dàng làm việc trên tất cả các loại nguồn dữ liệu và công cụ bảo mật với khả năng tương tác mạnh mẽ. Được trang bị hơn 700 tiện ích tích hợp dựng sẵn và tiện ích mở rộng đối tác\*, QRadar SIEM tích hợp liền mạch với các công cụ phát hiện mối đe dọa hiện có của bạn để đảm bảo bạn có được khả năng hiển thị đầy đủ trên hệ sinh thái bảo mật của mình.

**QRadar SOAR (IBM Security Resilent)**

* **Trải nghiệm phân tích liền mạch:** Ứng phó với các mối đe dọa và khắc phục sự cố nhanh hơn nhờ nền tảng mở mang đến cảnh báo từ các nguồn dữ liệu khác nhau đến một trang tổng quan duy nhất để điều tra và ứng phó.
* **Phản hồi của nhà phân tích hiệu quả:** Đảm bảo quá trình phản hồi của bạn được đáp ứng nhanh hơn bằng cách áp dụng cách tiếp cận toàn diện hơn để quản lý trường hợp với bố cục tùy chỉnh, sổ tay có thể điều chỉnh và phản hồi phù hợp.
* **Tự động hóa:** Sử dụng tự động hóa để thu hẹp khoảng cách kỹ năng. Tương quan giả tạo, điều tra và ưu tiên trường hợp được tự động hóa trước khi ai đó chạm vào trường hợp. Cẩm nang của bạn sẽ phát triển khi quá trình điều tra diễn ra, với việc làm phong phú thêm mối đe dọa diễn ra ở mỗi giai đoạn của quy trình.
* **Phản hồi vi phạm**: Chuẩn bị và ứng phó với các hành vi vi phạm quyền riêng tư bằng cách tích hợp các tác vụ báo cáo quyền riêng tư vào cẩm nang ứng phó sự cố tổng thể của bạn. Làm việc cùng với các nhóm về quyền riêng tư, nhân sự và pháp lý để giải quyết các yêu cầu đối với hơn 180 quy định.
* **Tăng tốc ứng phó sự cố:** Các giải pháp QRadar SOAR sử dụng các tiêu chuẩn mở theo cách tiếp cận quản lý trường hợp tùy chỉnh. Nó có một hệ sinh thái kết nối rộng lớn, sử dụng các cẩm nang động và hoạt động với các quy trình phản hồi hiện có.
* **Điều tra sự cố nhanh hơn:** Các giải pháp QRadar SOAR sử dụng tự động hóa để tương quan, làm phong phú, điều tra và ưu tiên trường hợp, điều này có thể giúp giảm thời gian phản hồi sự cố tới 85%.⁵
* **Sắp xếp và tự động hóa phản hồi:** Các giải pháp QRadar SOAR có rào cản gia nhập thấp để các nhà phân tích xây dựng tự động hóa, cung cấp phản hồi tự động cho các cảnh báo có độ chính xác cao, nhanh chóng xác định các sự cố thực tế và loại bỏ các kết quả dương tính giả.
* **Bắt đầu dễ dàng hơn:** QRadar SOAR, người chiến thắng Giải thưởng Thiết kế Red Dot, cung cấp thông tin về mối đe dọa và khả năng tìm kiếm liên kết mà không phải trả thêm phí. Có được tốc độ và độ chính xác bạn cần trên mô hình định giá có thể dự đoán được.

Ref: <https://www.ibm.com/products/qradar-siem>

<https://www.ibm.com/products/qradar-soar>

**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**

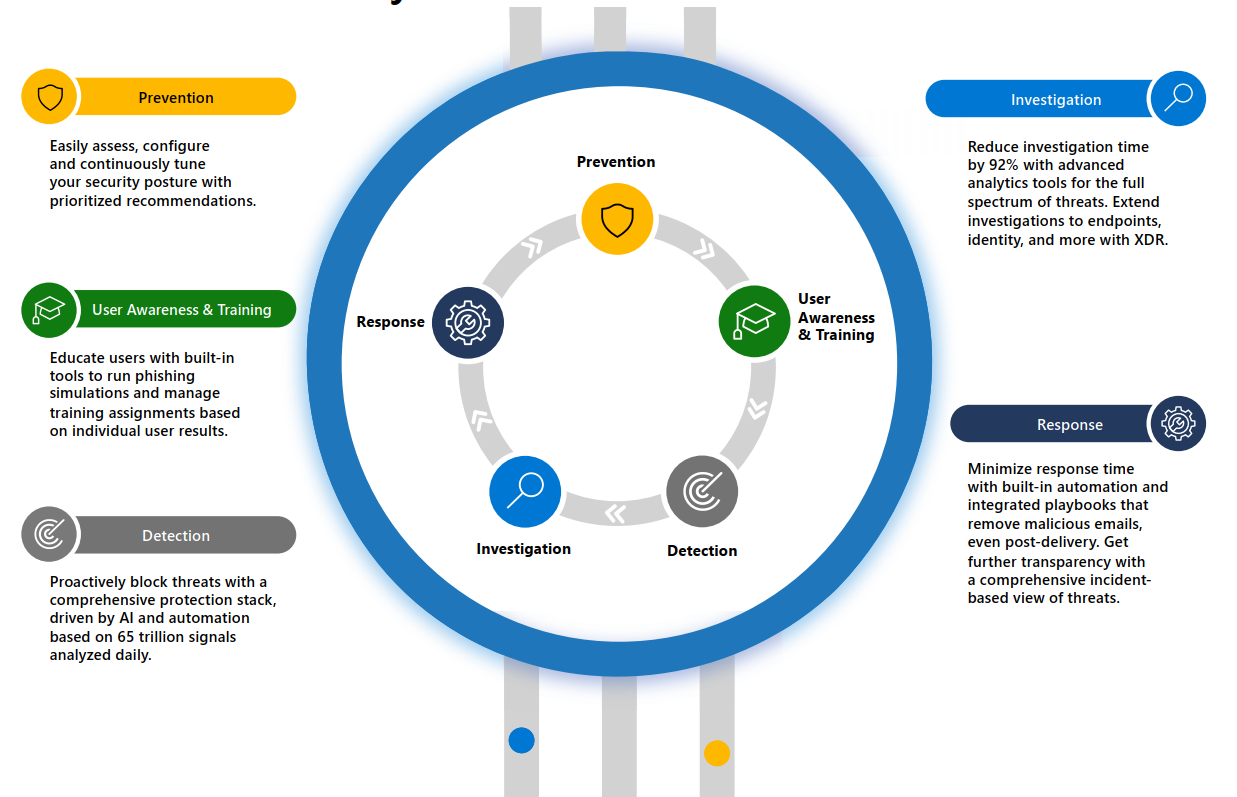
Bộ nhớ trong SAN được quản lý và cấu hình tập trung, điều đó có nghĩa là việc tăng giảm quy mô lưu trữ có thể được thực hiện linh hoạt và dễ dàng để thích ứng với nhu cầu của doanh nghiệp trong từng giai đoạn.

**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…).

Office 365 Security:

* List tính năng:
* **Anti-malware protection**
* **Anti-spam protection**
* **Connection filtering**
* **Outbound spam protection**
* **Anti-phishing protection**
* **Safe Attachments in Defender for Office 365**
* **Safe Links in Defender for Office 365**
* **Zero-hour Auto Purge (ZAP)**
* **Allow and block**
* **Attack simulation training in Denferder for Office 365**
* **Advanced delivery policies**
* **User tags and priority account Email entity page, Teams message entity panel**
* **Threat Tracker**
* **Alert policies**
* **Auditting**
* **Investigate and Respond**
* **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.
* **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.
* **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.
* **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.
* **Information Protection**: Cho phép mã hóa dữ liệu và quản lý quyền truy cập dữ liệu theo chính sách.
* **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.
* **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.
* **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.
* **Audit Logging and Reporting**: Cung cấp khả năng ghi lại các hoạt động và tạo báo cáo về quản lý và tuân thủ.
* **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.
* **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.
* **Insider Risk Management**: Giúp phát hiện và đối phó với các mối đe dọa nội bộ trong tổ chức.
* **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.
* **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://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/?view=o365-worldwide)

[**https://www.microsoft.com/vi-vn/security/business/siem-and-xdr/microsoft-defender-office-365**](https://www.microsoft.com/vi-vn/security/business/siem-and-xdr/microsoft-defender-office-365)

ORACLE DATABASE FIREWALL

Tường lửa mạng ngày nay đóng một vai trò quan trọng trong việc bảo vệ các trung tâm dữ liệu khỏi sự truy cập trái phép từ bên ngoài. Tuy nhiên, các cuộc tấn công vào trung tâm dữ liệu ngày càng trở nên phức tạp, vượt qua phạm vi bảo mật, lợi dụng các tầng trung gian đáng tin cậy và thậm chí giả mạo thành những người trong cuộc có đặc quyền. Do đó, việc thực thi các biện pháp kiểm soát bảo mật xung quanh cơ sở dữ liệu đã trở nên quan trọng. ORACLE DATABASE FIREWALL tạo ra một vành đai phòng thủ bên trong để giám sát và thực thi hành vi ứng dụng thông thường, giúp ngăn chặn việc tiêm SQL, bỏ qua ứng dụng và các hoạt động độc hại khác tiếp cận cơ sở dữ liệu

**Các tính năng:**

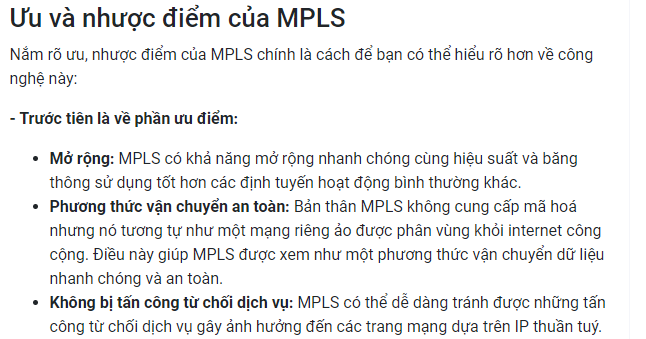
* Các mô hình triển khai linh hoạt bao gồm giám sát và chặn
* Chính sách dựa trên back list, white list và exception list
* Kiến trúc có khả năng mở rộng cao cho các ứng dụng doanh nghiệp
* AD Authentication - Permission
* **Auditing Sensitive Data**
* **Data Theft Protection**
* **Database Vulnerability**
* **Audit Access to Cardholder Information**
* **Dynamic Data Masking**
* Hàng chục báo cáo tuân thủ có thể tùy chỉnh được tích hợp sẵn
* Cảnh báo bảo mật theo thời gian thực
* Hỗ trợ Oracle, MySQL, Microsoft SQL Server, Sybase và IBM DB2
* **Hỗ trợ TDE bảo mật nâng cao của Oracle (Transparent Data Encryption)**

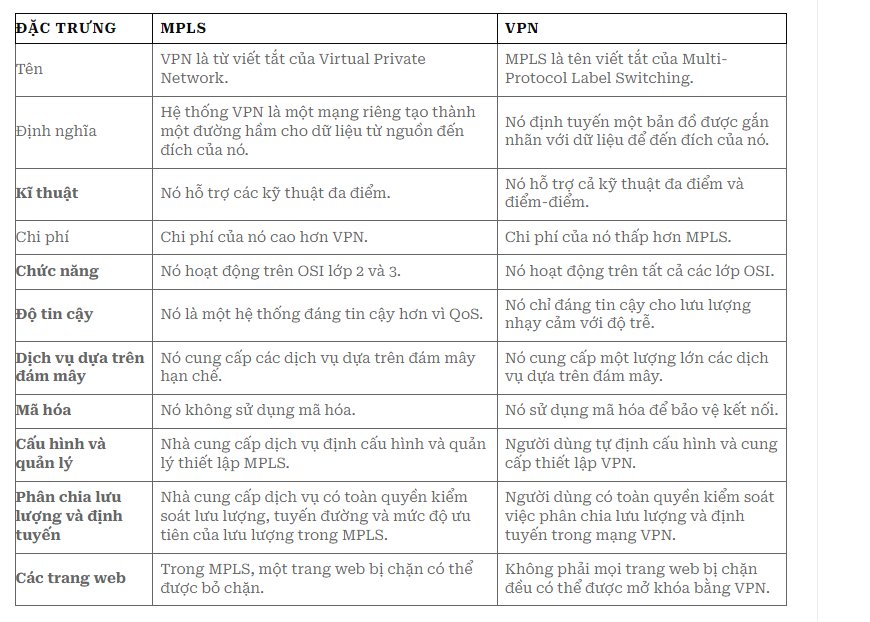
MPLS

[**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>

* Dịch vụ kênh thuê riêng Leasedline là dịch vụ cung cấp đường kết nối vật lý dành riêng cho khách hàng (bằng cáp quang, đồng hay Viba) để truyền thông tin giữa các điểm cố định trong nước hoặc trong nước đi quốc tế theo phương thức kết nối điểm – điểm hoặc điểm – đa điểm. Khách hàng sẽ không bị chia sẻ băng thông tại mọi thời điểm.
* Internet Leased Line là dịch vụ đường truyền Internet có cổng kết nối quốc tế riêng biệt dành cho các văn phòng, công ty có yêu cầu cao về chất lượng dịch vụ.
* Office Wan là dịch vụ cung cấp mạng riêng (nội bộ) với mục đích truyền dữ liệu dành cho doanh nghiệp có nhiều chi nhánh, trụ sở trên toàn quốc dựa trên hạ tầng MPLS/VPN (Multi-Protocol Label Switching/Virtual Private Network) của Viettel.
* MPLS là tận dụng ưu điểm của định tuyến IP cho phép nâng cao khả năng chuyển gói qua mạng, tăng cường hiệu quả hoạt động của mạng. Đồng thời hỗ trợ các tính năng QoS (Quality of Service), CoS (Class of Service) cho các dịch vụ yêu cầu chất lượng khác nhau như: voice, data, Video…

VMware vSphere

Vmware vSphere sở hữu những chức năng tương tự như với hai loại VMware Work Station và VMware Server, nhưng VMware vSphere có khả năng sử dụng được trên phạm vi rộng hơn để phù hợp với các doanh nghiệp, các tổ chức lớn. Mục đích chính của VMware được sử dụng là để tạo ra cơ sở hạ tầng điện toán đám mây và server/máy chủ là nơi cài đặt chính. Nó bao gồm một bộ các ứng dụng [ảo hóa](https://bkhost.vn/blog/virtualization-technology-ao-hoa/) dành cho doanh nghiệp, trong đó nền tảng là ESX/ESXi.

**VMware vCenter Server**

[VMware vCenter Server](https://bkhost.vn/blog/vmware-vcenter-server/) cung cấp một điểm kiểm soát duy nhất cho cả trung tâm [dữ liệu](https://bkhost.vn/blog/data-du-lieu/). vCenter thực hiện chức năng của một dịch vụ trung tâm dữ liệu cần thiết ví dụ như: kiểm soát truy cập, cấu hình, giám sát hiệu suất

Phần mềm VMware vSphere bao gồm các sản phẩm có nhiều các chức năng, đầy đủ công cụ, tính năng để ảo hóa như:

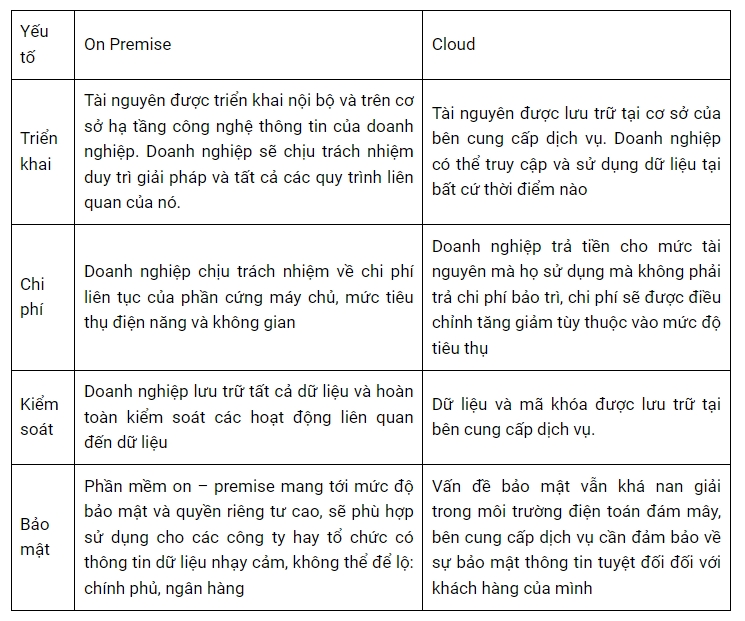
* Di chuyển nhanh chóng các máy ảo sang một hệ thống khác mà không có downtime.
* Di chuyển động các máy ảo sang các phân vùng storage khác mà không có downtime.
* Hỗ trợ mở rộng tài nguyên CPU, RAM của host, không cần có downtime.
* Bảo mật dữ liệu, thực hiện backup và restore các máy ảo.
* Đảm bảo 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.

Route53

Amazon Route 53 là một dịch vụ web đám mây (DNS) có khả năng duy trì mở rộng cao. Nó được thiết kế để cung cấp cho các nhà phát triển và doanh nghiệp cách để định tuyến end user đến các ứng dụng Internet một cách đáng tin cậy và hiệu quả bằng việc dịch tên như [www.example.com](http://www.example.com/) vào địa chỉ IP như 192.0.2.1 để các máy tính có thể kết nối đến nhau. Router 53 cũng hoàn toàn tuân thủ IPv6.

Amazon Route 53 kết nối hiệu quả các request của người dùng với hệ thống infra đang chạy trong AWS - chẳng hạn như các instance Amazon EC2, Elastic Load Balancer hoặc Amazon S3 bucket - và cũng có thể được sử dụng để định tuyến người dùng đến các hệ thống infra ngoài AWS. Lưu lượng truy cập Amazon Route 53 giúp bạn dễ dàng quản lý lưu lượng trên toàn cầu thông qua nhiều loại định tuyến khác nhau, bao gồm Định tuyến dựa trên độ trễ (Latency Based Routing), DNS địa lý (Geo DNS), Geoproximity và Round Robin có trọng số (Weighted Round Robin) - tất cả những thứ có thể kết hợp với DNS chịu lỗi để cho phép nhiều loại định tuyến và kiến thức chịu lỗi.

On premise

**On premise** hay được biết đến là những phần cứng hay phần mềm tại chỗ. Đây là một giải pháp công nghệ hỗ trợ lưu trữ dữ liệu tại chỗ. Phần mềm On premise yêu cầu doanh nghiệp mua giấy phép hoặc bản sao của phần mềm để sử dụng được phần mềm đó. 

AWS Direct Connect

AWS Direct Connect là dịch vụ mạng cung cấp lựa chọn thay thế cho việc kết nối với AWS qua Internet. Khi bạn sử dụng AWS Direct Connect, những dữ liệu trước đây được truyền qua Internet giờ sẽ được cung cấp qua một kết nối mạng riêng giữa cơ sở của bạn và AWS