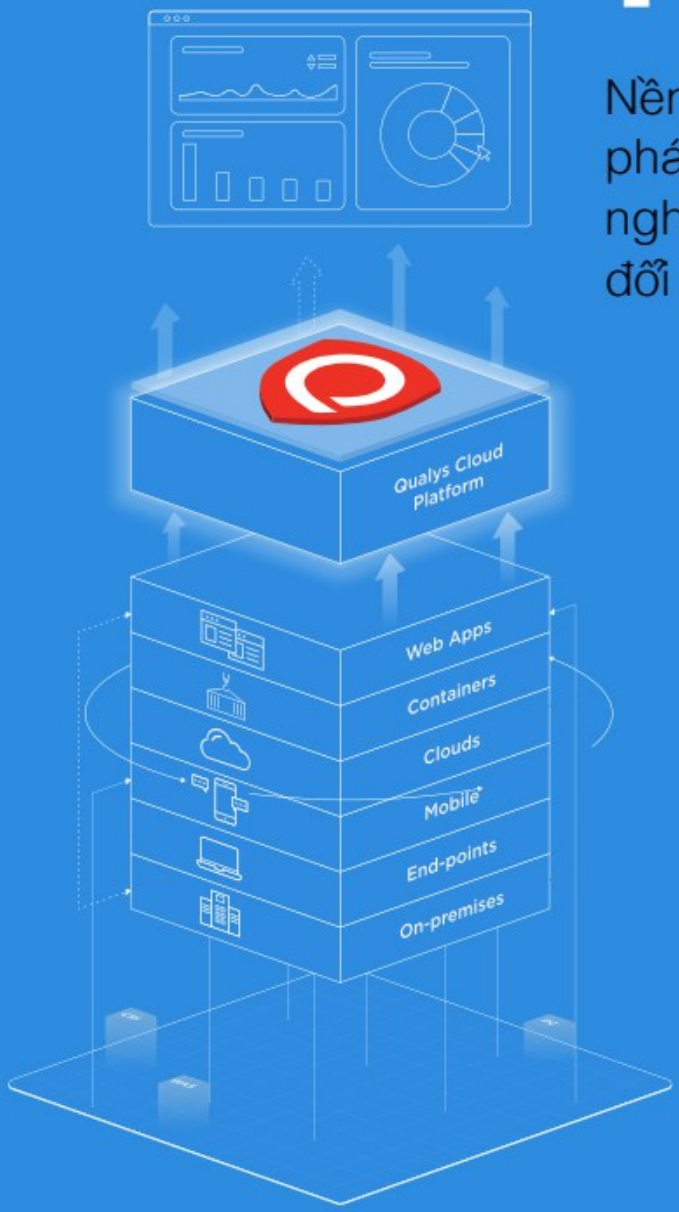
Qualys.

Qualys Cloud Platform

Nền tảng giúp tăng cường các giải pháp bảo mật và tuân thủ cho doanh nghiệp và bảo vệ quá trình chuyển đổi số



Mục lục

Giới thiệu 3

Môi trường IT hiện đại: Không giới hạn, phân tán, linh hoạt 4
IT lai ghép: một thách thức bảo mật 5
Những giới hạn mới của môi trường IT 6
Làm sao để giám sát và bảo vệ các môi trường IT từ xa? 7

Qualys Cloud Platform 8
Giới thiệu 9
Tổng quan về Qualys Cloud Platform 9
Cấu trúc ý tưởng về bảo mật chuyển đổi số 10

Phương thức hoạt động 12
Cảm biến linh hoạt 13
Qualys appliances Passive 14
Network Sensor Qualys 15
Cloud Agent Qualys Cloud 16
Apps 17

Phân loại dữ liệu Back-end, hình ảnh hoá và phân tích 22
Lợi thế của kiến trúc nền tảng cloud 24
Các dịch vụ và ứng dụng được cung cấp qua nền tảng public cloud, hoặc nền tảng private cloud 25

Đăng ký Qualys 27
Doanh nghiệp vừa, nhỏ, tư vấn và MSPs, chính phủ 27
Qualys Community Edition 30

Hỗ trợ và đào tạo toàn diện 31

Khách hàng 32
Khách hàng tiêu biểu 33
Geisinger Health Systems 34
Synovus Financial Corp 35

Phát triển 36
Dự đoán những gì sẽ tới 37

Giới thiệu chung

Trong bối cảnh các doanh nghiệp bắt đầu thực hiển chuyển đổi số để tăng cường năng lực và hiệu quả, môi trường IT bắt đầu trở nên phân tán, co giãn và lai ghép - một thách thức đối với đội ngũ IT. CISO đã không còn đủ tốt bởi các sản phẩm bảo mật thông thường được thiết kế để bảo vệ các hệ thống truyền thống, đã được định nghĩa sẵn, nơi mà hầu hết các tài sản IT đều ở trong doanh nghiệp.

Với sự phát triển của cloud, các thiết bị di động, ảo hoá và nhiều phát minh khác, ranh giới hạ tầng IT đã được mở rộng, không rõ ràng và có thể bị xoá bỏ. Để lấy lại được cái nhìn và khả năng kiểm soát các môi trường IT vô định hình này, CISCO thường phân loại lại vào các công cụ phân tích không đồng nhất, một cách tiếp cận rất thiếu hiệu quả và phản tác dụng.

Vì rất khó để tích hợp, quản lý và mở rộng một số lượng lớn các sản phẩm bảo mật khác nhau, chiến lược này dẫn tới kết quả hoạt động chồng lấn, tăng chi phí và phân mảnh dữ liệu. Tệ hơn nữa, nó khiến doanh nghiệp tạo ra các cơ hội khiến các hacker có thể tấn công một cách nhanh chóng, liên tục vào hệ thống IT.

Thay vào đó, bảo mật cần được thực hiện một cách rõ ràng xuyên suốt trong dự án chuyển đổi số. Điều đó yêu cầu một nền tảng bảo mật và tuân thủ đồng nhất cho việc ngăn chặn, phát hiện và phản ứng.

Qualys đã nhận thấy vấn đề này nhiều năm trước. Với tầm nhìn tiên phong, Qualys đã xây dựng nó tích hợp với nền tảng cloud nhằm giải quyết được những thách thức của kỷ nguyên số luôn bị tấn công liên tục.

Với Qualys, doanh nghiệp có thể xây dựng bảo mật nội tại và nhiều lớp trong hạ tầng IT lai ghép, thay vì chắp vá chúng, như cách thực hiện truyền thống trước đây.

Điều này cũng bao gồm cả việc kết hợp và tự động hoá bảo mật trong các liên kết DevOps, nơi cung cấp các dự án chuyển đổi số bằng cách liên tục và nhanh chóng phát triển và chuyển code. Nếu bảo mật vẫn bị tách biệt và mặc kẹt tại điểm cuối trước khi phần mềm được triển khai, nó sẽ làm chậm lại khả năng phát triển và truyền tải liên tục của DevOps', và xoá bỏ lợi ích của chuyển đổi số.

ORACLE®

"Qualys giúp chúng tôi chắc chắn rằng hệ thống được bảo mật, đảm bảo an ninh cho cả phía chúng tôi lẫn khách hàng."

Senior Manager,
GIT Security Engineering Team

Nói ngắn gọn, nền tảng Qualys Cloud Platform liên tục đánh giá bảo mật và tình trạng tuân thủ của doanh nghiệp, cung cấp cái nhìn tức thì với toàn bộ tài sản IT - tại nội bộ doanh nghiệp, trên cloud, và tại các thiết bị cuối điều khiển từ xa - cho phép giám sát và phản ứng liên tục.

Theo Robert Ayoub, Giám đốc nghiên cứu bảo mật của IDC phát biểu: "Qualys Cloud Platform đơn giản hoá những liên kết phức tạp với khả năng quản lý nhiều giải pháp bảo mật khác nhau, cùng với tăng khả năng tự động hoá, hiệu quả và tiên phong trong lĩnh vực bảo mật."

Hãy đọc tiếp để hiểu nền tảng của chúng tôi làm sao để củng có và tự động hoá bảo mật và tuân thủ, bảo vệ môi trường IT lai ghép thông qua các cảm biến linh động, công nghệ phân tích back-end và bộ tích hợp các ứng dụng.

Phần I

Môi trường IT hiện đại: Không giới hạn, phân tán và mềm dẻo

IT lai ghép: Một thách thức bảo mật

Một thách thức bảo mật mới là điện toán đám mây, di động và các phát minh IT khác được tạo ra cho bộ phận IT là một ví dụ rất tốt và rất thông dụng, là hệ thống thanh toán của các đại lý bán lẻ

Rủi ro của ứng dụng này nằm ở chỗ mỗi thành phần nằm tại một nơi khác nhau. Sản phẩm bảo mật chỉ có thể bảo vệ thiết bị cuối, các thiết bị ảo trên cloud hoặc các thiết bị tại doanh nghiệp. Việc cố gắng thống nhất nhiều giải pháp không đồng nhất dẫn tới việc tích hợp phức tạp, tốn chi phí và, rất có thể, hiệu suất tệ hại.

Giới hạn mới của môi trường IT

Các ranh giới trước đây thường xuất hiện trong hệ thống nội bộ doanh nghiệp, nhưng nay đã mở rộng ra cả cloud, thiết bị di động, web app, cảm biến IoT và cả những sản phẩm khác.

Các thiết bị di động, thiết bị khác và hệ thống IoT

Ranh giới hệ thống của bạn sẽ ngày càng mở rộng tới tất cả các thiết bị của nhân viên kết nối tới các mạng wifi công cộng và tại nhà: Laptops, smartphones, máy tính bảng và đồng hồ thông minh. Những thiết bị thường được mang theo khi du lịch chứa các dữ liệu và ứng dụng mật, rất dễ dàng bị mất, đánh cắp hay xâm phạm

Một điểm yếu khác: Doanh nghiệp có nhiều chi nhánh về mặt địa lý, như các văn phòng làm việc từ xa và các cửa hàng bán lẻ. Nó rất dễ dàng, nơi mà các máy tính cá nhân, hệ thống POS và các thiết bị cuối khác dễ bị khai thác và tấn công bảo mật hơn là các toà nhà tập đoàn lớn.

trong khi đó, các thết bị khác cũng kết nối đến mạng của bạn như máy copy, máy in, máy ổn định nhiệt, và kể cả thiết bị pha cafe qua Wifi

Các doanh nghiệp bắt đầu nhanh chóng hướng tới IoT và các cảm biến nhúng trong vô số thứ mà trước đây hoạt động offline như: Xe cộ, hệ thống HVAC, các thiết bị y tế, thiết bị công nghiệp và các cửa hàng. Chúng rất đa dạng và các thiết bị cuối này giờ đây thu thập rất nhiều dữ liệu nhạy cảm và truyền chúng trở về hệ thống IT của doanh nghiệp.

Do đó, doanh nghiệp sẽ cần một công cụ giúp họ giám sát và cường hoá bảo mật và tuân thủ của thiết bị di động và các thiết bị cuối không truyền thống, đặc biệt bởi khuynh hướng cho thấy chúng nhiều lỗ hổng hơn các thiết bị thông thường.

Dịch vụ điện toán đám mây

Theo xu hướng dịch vụ hạ tầng và nền tảng tính toán đám mây - PaaS và IaaS - liên tục phát triển trong các doanh nghiệp trên toàn cầu. Đội ngũ bảo mật thông tin phải bảo vệ những công việc trong quá trình chuyển giữa hạ tầng tại doanh nghiệp lên cloud. Các nhà cung cấp nền tảng cloud hoạt động trên một mô hình chia sẻ trách nhiệm: họ bảo vệ nền tảng của họ trong khi khách hàng có trách nhiệm bảo vệ dữ liệu và phần mềm của họ. Do đó, khách hàng cần thực hiện việc kiểm tra bảo mật và tuân thủ trong quá trình triển khai lên cloud, tương tự như khi họ triển khai tại doanh nghiệp, bao gồm quản trị lỗ hổng, rà soát web app, và tuân thủ chính sách. Để làm được điều này, họ cần một công cụ bảo mật giúp họ có cái nhìn toàn cảnh về các thiết bị cloud.

Web app và các liên kết Dev(Sec)Ops

Với các hoạt động chuyển đổi số của các doanh nghiệp, những phát kiến này được cung cấp qua web app: kết nối internet, nội bộ và các web-app trên nền cloud, cũng như các web service trên nền REST API. Với những web app này, doanh nghiệp đơn giản hoá và tự động hoá các chức năng và quy trình quan trọng cho nhân viên, khách hàng và đối tác. Tuy nhiên, nhiều ứng dụng web không được an toàn do các lỗ hổng và cấu hình yếu. Và không ngạc nhiên, chúng trở thành một trong những đối tượng yêu thích trong đánh cắp dữ liệu.

Một yếu tố quan trong trong cường hoá web app là tích hợp với việc kiểm tra bảo mật trong suốt liên kết DevOps nơi mà các dòng lệnh được nhanh chóng và liên tục xây dựng và triển khai. Khi bảo mật được kết hợp, quá trình này trở thành liên kết DevSecOps, các cấu hình thiếu an toàn và lỗ hổng sẽ được tự động phát hiện và xử lý. Bằng cách đó, bảo mật sẽ không bị phá vỡ, làm chậm quá trình CI/CD (liên tục tích hợp/chuyển giao) code giúp tăng hiệu quả chuyển đổi số.

Làm sao để giám sát và bảo vệ môi trường từ xa?

Để bảo vệ môi trường IT hiện đại, bạn cần một nền tảng đám mây quản trị tập trung, tích hợp cho bạn cái nhìn đơn giản về toàn bộ tài sản IT của mình và các lỗ hổng cũng như các cấu hình kém bảo mật. Bạn sẽ phải có khả năng sàng lọc dữ liệu, hình ảnh hoá với biểu đồ và báo cáo, và phân tích chia sẻ nó với nhiều người quản trị khác.

Bạn có thể thử xây một hệ thống cho bạn cái nhìn tổng thể và toàn diện về tất cả cả hiểm hoạ bằng cách kết hợp nhiều sản phẩm với nhau. Tuy nhiên nó sẽ phức tạp, tốn kém và không hiệu quả. Và thật may mắn, một giải pháp như vậy đã có sẵn cho bạn: Qualys Cloud Platform.

"Chúng tôi sử dụng Qualys như một cách để vẽ ra bức tranh về bảo mật và gửi nó cho người điều hành. Các bản báo cáo cung cấp cho những người điều hành cái nhìn nhanh chóng, thời gian thực về các hiểm hoạ của eBay's và đo được những thay đổi khi chúng tôi triển khia các phép đo bảo mật"

Senior Manager,
Information Security

ebay

Phần II

Qualys Cloud Platform

Làm sao chúng tôi làm được những điều người khác không thể? Tất cả những điều đó có trong nền tảng đám mây của chúng tôi. Nó liên tục thu thập, đánh giá và liên hệ bảo mật, IT và dữ liệu tuân thủ của tất cả các tài sản tại bất kỳ đâu - trên cloud, tại doanh nghiệp, tại thiết bị di động/ thiết bị từ xa. Qualys Cloud Platform là giải pháp bảo mật hoàn chỉnh cho phép khách hàng có cái hình toàn cảnh, thời gian thực về các hiểm hoạ giúp cho việc phòng chống, khắc phục và xử lý một cách toàn diện.

Giới thiệu chung về Qualys Cloud Platform

Qualys Cloud Platform được thiết kế dựa trên mục tiêu đơn giản hoá bảo mật bằng cách loại bỏ những điểm xung đột và khiến nó trở nên trực quan và tự động nhất có thể.

Qualys gọi nó là "Transparent Orchestration (™)", một nguyên tắc tiêu biểu cho bảo mật trong tương lai, và cung cấp nó như một định hướng và mục tiêu then chốt của Qualys.

Transparent Orchestration được phản ánh trong thiết kế của Qualys Cloud Platform, đặc biệt là trong ba khía cạnh: cảm biến linh hoạt, khả năng mở rộng backend mạnh mẽ và các bộ ứng dụng cloud tích hợp sẵn.

Với các cảm biến luôn hoạt động, Qualys Cloud Platform cung cấp cho doanh nghiệp cái nhìn thời gian thực, liên tục với toàn bộ tài sản IT - tại doanh nghiệp, thiết bị cuối hay trên cloud - cho phép ngăn chặn, phát hiện và phản ứng một cách toàn diện. Quản trị tập trung và tự động cập nhật, các cảm biến của Qualys bao gồm thiết bị cứng hoặc ảo hoá, hoặc các Agent.

Trong khi đó, các ứng dụng Qualys Cloud cung cấp công cụ và năng lực cho toàn bộ đội ngũ bảo mật, bao gồm những thành phần sau:

- Hạ tầng On-premises
- Tải công việc Cloud
- Các thiết bị cuối
- Các môi trường DevSecOps
- Các ứng dụng web
- Kiểm tra và tuân thủ IT

Bằng việc gia cố các lớp bảo mật trên các ứng dụng Qualys Cloud quản trị tập trung và tự động cập nhật, bạn có thể giúp đội ngũ IT luôn được đồng bộ. Bạn cũng có thể loại bỏ những mô hình phức tạp, những sản phẩm chắp vá hoạt động không hiệu quả, khó tích hợp và rất tốn kém để quản trị.

Qualys Cloud Platform có khả năng báo cáo, lưu trữ, phân tích dữ liệu, tìm kiếm kết quả, gắn thẻ tài sản một cách mạnh mẽ, trong tất cả các chức năng khác. Một giao diện đơn giản, quản trị tập trung trên nền web giúp bạn hoàn thiện và liên tục cập nhật về tình trạng, tình hình tuân thủ và bảo mật của môi trường IT của bạn.

Qualys cũng cung cấp nền tảng private cloud hỗ trợ toàn bộ các lợi ích của Qualys Cloud Platform ngay trong trung tâm dữ liệu của bạn. Qualys Private Cloud Platform cho phép doanh nghiệp lưu trữ dữ liệu rà soát được ngay trong nội bộ dưới sự kiểm soát tuân thủ với những chính sách nội bộ hoặc các điều luật khác.

Với kiến trúc cloud này, Qualys Cloud Platform được thiết kế độc nhất bảo vệ cho các môi trường IT lai ghép hiện nay, bao gồm các liên kết DevOps nơi mà chuyển đổi số đang được xây dựng và triển khai.

Hơn 1000 tỉ
sự kiện bảo mật

Hơn 3 tỉ
IP được rà soát/ kiểm tra mỗi năm

Hơn 28 tỉ
dữ liệu được thu thập và xử lý

99.999%
Độ chính xác six sigma

Cấu trúc ý tưởng về bảo mật chuyển đổi số

Qualys, người tiên phong trong tuân thủ và bảo mật trên nền cloud được thành lập năm 1999, là đơn vị duy nhất giúp các doanh nghiệp bảo vệ việc triển khai chuyển đổi số nhanh chóng.

Để xây dựng bảo mật trong việc cố gắng chuyển đổi số, các doanh nghiệp phải đưa quy trình và các công cụ bảo mật thông tin vào trong trục phân phối và triển khai phần mềm DevOps. Lý do: Các thiết bị di động và ứng dụng web, dịch vụ web được tạo ra từ đội ngũ DevOps là phương tiện cho việc chuyển đổi số.

Qualys có thể giúp doanh nghiệp đơn giản hoá sự sẵn sàng và sử dụng các công cụ bảo mật tự động cho người phát triển và điều hành, các đoạn mã đó có thể được rà soát lỗ hổng cấu hình lỗi và các vấn đề bảo mật thường gặp trong vòng đời phần mềm.

Đưa bảo mật vào DevOps – biến nó thành DevSecOps – sẽ khiến code trở nên rõ ràng hơn, và hệ thống trở nên bảo mật hơn. Điều này giúp bảo mật thông tin giữa đội ngũ IT và đội ngũ phát triển, giúp doanh nghiệp đẩy nhanh quá trình chuyển đổi số một cách an toàn.

Trong một bản báo cáo gần đây, 451 nhà phân tích tìm kiếm Scott Crawford nói rằng "Tầm nhìn chiến lược của Qualys đã giúp họ đặt chân vào các doanh nghiệp có môi trường lai ghép. Công ty đã từ lâu cung cấp những thứ mà ngày nay có thể gọi là "di sản" IT - nhưng nguồn gốc cloud cho biết chiến lược của họ để giải quyết CNTT vào ngày mai."

Các doanh nghiệp đang tìm kiếm sự nhanh nhạy, sáng tạo và hiệu quả thông qua chuyển đổi số, các cách tiếp cận bảo mật cũ có thể trở thành sự cản trở những công nghệ mới này trong việc tự động hoá, tích hợp và tăng tốc.

"Do đó, khả năng của các phương pháp mới này phải trở thành một dấu ấn của một thế hệ công nghệ bảo mật mới. Nền tảng Qualys' SaaS không chỉ là một tài sản mang lại cơ hội, những trải nghiệm nó mang lại trong việc phát triển cloud cho thấy nó chính là công cụ bảo mật mà doanh nghiệp đang tìm kiếm."

Do chuyển đổi số đang đến rất gần với các doanh nghiệp sử dụng dịch vụ public cloud, việc Qualys có thể giúp doanh nghiệp bảo vệ việc triển khai PaaS và IaaS là một điều rất đang chú ý.

Các doanh nghiệp đang tăng cường sử dụng nền tảng public cloud, họ gặp phải các hiểm hoạ tuân thủ và bảo mật, và các thách thức cụ thể, ví dụ:

- Thiếu khả năng giám sát các tài sản cloud, các tài nguyên và việc sử dụng chúng.
- Thiếu kiến thức về mô hình chia sẻ trách nhiệm bảo mật của các nhà cung cấp.

Điều này có nghĩa là các doanh nghiệp phải duy trì việc cập nhật thông tin một cách liên tục, và thực hiện việc kiểm tra tuân thủ và bảo mật thiết yếu trên các tài sản này.

Qualys cung cấp việc tích hợp và bảo mật, tuân thủ toàn diện sẵn có cho nền tảng public cloud, bao gồm cả AWS, Azure và Google Cloud, giúp bạn:

- Định danh, phân loại và giám sát toàn bộ các công việc và tài nguyên
- Tuân thủ với các chính sách nội bộ và quốc tế.
- Phân cấp ưu tiên khắc phục lỗ hổng

• Tự động tìm và loại bỏ mã độc trên website

• Tích hợp và tự động hoá bảo mật và tuân thủ thông qua liên kết DevOps

Qualys Cloud Platform cung cấp cho doanh nghiệp 5 điểm then chốt trong việc bảo mật chuyển đổi số:

• Khả năng quan sát

Nó cung cấp khả năng giám sát tài sản IT một cách hoàn thiện, liên tục và phát hiện những thay đổi trong cả hệ thống tại doanh nghiệp, cloud và các thiết bị liên kết từ xa.

• Chính xác

Nó thu thập, lưu trữ và phân tích tập trung toàn bộ dữ liệu bảo mật và tuân thủ, loại bỏ những thông tin rời rạc có từ những giải pháp không liền mạch, phân mảnh khác

• Khả năng mở rộng

Nó có khả năng mở rộng mạnh mẽ nhờ kiến trúc cloud, giúp bảo vệ những môi trường IT lai ghép lớn nhất.

• Ngay lập tức

Nền tảng mạnh mẽ cho phép nó có khả năng ngăn chặn và phản ứng ngay lập tức với các sự cố.

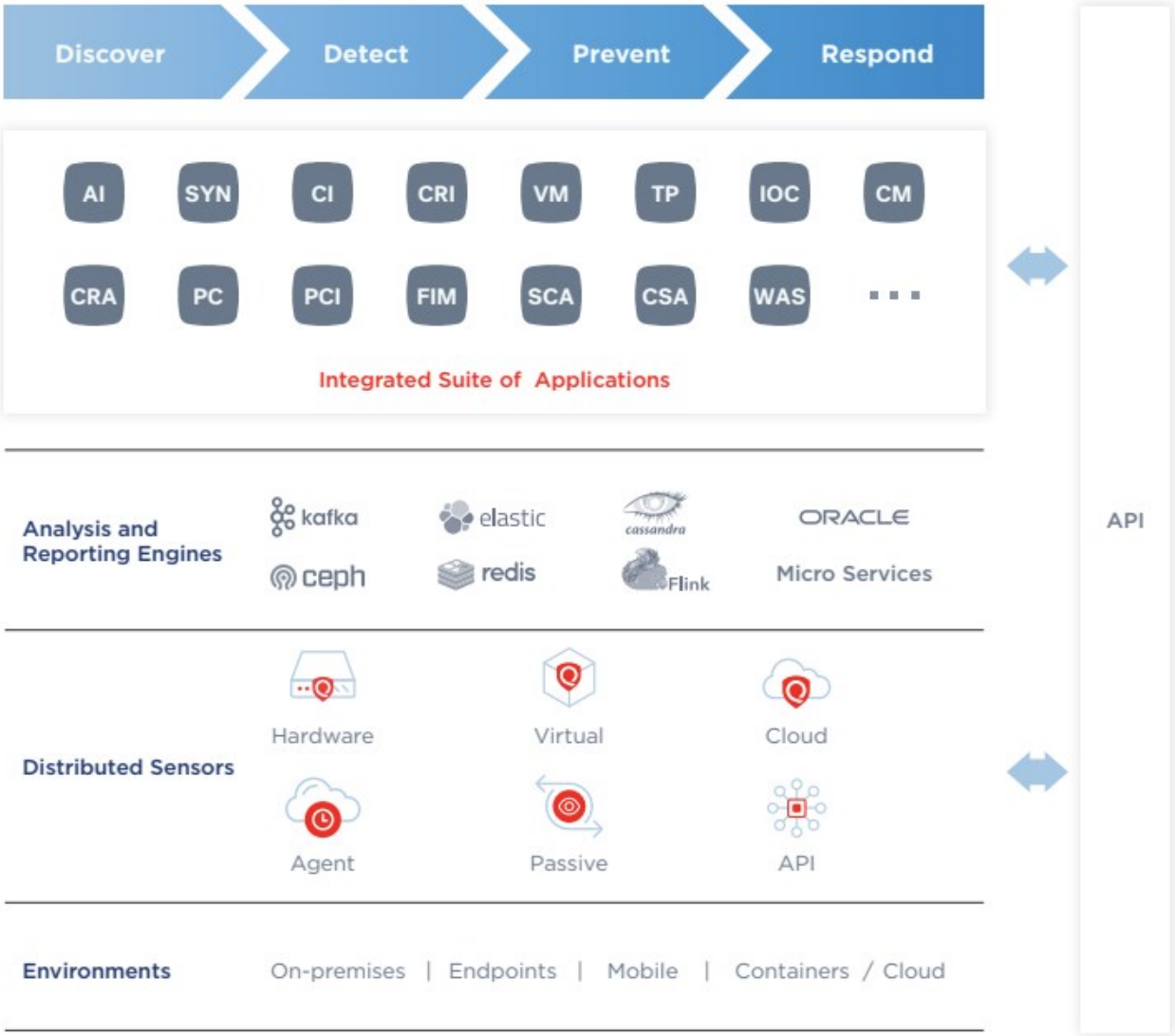
• Transparent Orchestration (™)

Nó cung cấp khả năng bảo mật tự động, đa dạng, đơn giản xuyên suốt môi trường IT, khiến nó trở nên trực quan đối với người phát triển và nhân viên IT.

Phương thức hoạt động

Qualys Cloud Platform được xây dựng trên hạ tầng linh hoạt, dễ mở rộng, mạnh mẽ và theo các khối dễ lắp ghép, tận dụng được cộng nghệ cloud và ảo hoá, giúp chúng ta dễ dàng phân bổ năng lực theo yêu cầu.

Chi tiết về hoạt động của Qualys Cloud Platform.



Các bộ cảm biến linh hoạt

Các cảm biến của Qualys Cloud Platform – dưới dạng thiết bị vật lý, ảo hoá hay Agent - luôn hoạt động, có khả năng triển khai từ xa, quản trị tập trung và tự động cập nhật. Chúng cho phép rà soát và giám sát toàn bộ các tài sản IT phân tán có trong môi trường IT lai ghép hiện nay, bao gồm:

- Từ Internet
- Trong vùng DMZ
- Trong mạng nội bộ
- Trên các nền tảng public cloud

Các cảm biến của Qualys thu thập dữ liệu từ môi trường IT và tự động gửi nó lên Qualys Cloud Platform, nơi liên tục phân tích và liên kết thông tin và giúp bạn nhanh chóng phát hiện và loại bỏ hiểm hoạ một cách chính xác.

Cloud Agents

Works everywhere. The secret to our continuous visibility

Virtual Scanners

Software-only internal scanning, on premises or in the cloud

Scanner Appliances

On-premises hardware scanners for internal networks

Internet Scanners

Fast and efficient external scanning, on premises or in the cloud

Passive Scanners

Real-time network analysis of your data

Out-of-Band Sensors

Secure highly locked-down devices or on air-gapped networks

Cloud Connectors

Collect data from 3rd party cloud platforms and software

APIs

Collect data from 3rd parties such as threat intelligence feeds

Thiết bị rà soát của Qualys

Qualys cung cấp nhiều loại thiết bị rà soát:

- Thiết bị cứng giúp rà soát các tài sản IT nội bộ

- Thiết bị ảo có thể rà soát từ xa môi trường private cloud và môi trường ảo hoá

- Thiết bị sẵn có trên Internet hỗ trợ rà soát nhanh và hiệu quả

- Thiết bị trên môi trường Cloud hỗ trợ rà soát các tài sản trên hạ tầng public Cloud IaaS và PaaS

Thiết bị rà soát được cấu hình thông qua giao diện trực quan dễ sử dụng, và được kích hoạt thông qua giao diện web của Qualys.

Cảm biến mạng lưới thụ động

Cảm biến mạng lưới thụ động (PNS) cung cấp khả năng phát hiện liên tục trong toàn bộ hệ thống kết nối mạng và các hoạt động của chúng theo thời gian thực

Với PNS, khách hàng có thể:

Loại bỏ các điểm mù: Qualys Cloud Platform kết hợp các dữ liệu của tài sản từ PNS, Qualys scanners và Qualys Cloud Agents nhằm kê khai thông tin chi tiết, đa chiều và toàn diện về tất cả các tài sản IT trong hạ tầng lai ghép. Nó bao gồm cả những thiết bị không nằm trong diện quản trị như các thiết bị di động cá nhân của nhân viên, hay các thiết bị lạ. PNS cũng phát hiện và lưu trữ thông tin tài sản mà không thể chủ động rà soát hay giám sát với Cloud Agent, như các thiết bị công nghiệp, hệ thống IoT và thiết bị y tế.

Xác định các kết nối đáng ngờ: PNS cung cấp khả năng rà soát chuyên sâu các gói tin nhằm liên tục phân tích và phát hiện các kết nối đang ngờ. Qualys Cloud Platform sau đó liên kết các thông tin bất thường này với các chỉ dấu xâm phạm để xác định tính an toàn

Bảo mật và kiểm soát truy cập: PNS giúp bạn tự động phản ứng với các hiểm hoạ bằng cách kiểm soát các truy cập đến các tài nguyên quan trọng. Kiểm soát truy cập, được PNS cung cấp bởi khả năng phát hiện, bảo vệ độc lập theo thời gian thực bằng cách cách ly các thiết bị không tuân thủ dựa trên chính sách đã được thiết lập và mô hình bảo mật.

(Qualys PNS dự kiến sẽ được phát hành trong năm 2019.)

Qualys PNS cung cấp khả năng quan sát tất cả các kết nối của thiết bị trong mạng của bạn.

Qualys Cloud Agent

Qualys Cloud Agent mở rộng khả năng bảo mật ra toàn cầu extends security throughout your global enterprise. Những agent rất nhẹ (2MB) có thể triển khai từ xa, quản lý tập trung, tự động cập nhật và tiêu tốn rất ít tài nguyên CPU.

Cloud Agents hoạt động ở những nơi mà không thể thực hiện các phiên rà soát. Đây là phương pháp được ưa thích đối với các tài sản như thiết bị có IP động, các tài sản cloud, người dùng từ xa, và hệ thống nhạy cảm với việc rà soát từ ngoài mạng.

Sau khi được triển khai, Cloud Agent sẽ đánh giá toàn bộ cấu hình của thiết và gửi dữ liệu thu được lên Qualys Cloud Platform để phân tích. Sau đó, ngay khi có sự thay đổi, Cloud Agent sẽ đẩy các thông tin cập nhật lên nền Qualys Cloud Platform, đảm bảo rằng bạn sẽ có dữ liệu mới nhất về tài sản IT của bạn ngay lập tức.

Có rất nhiều lợi ích đối với môi trường IT lai ghép, bao gồm:

- Không cần thực hiện rà soát. Agent luôn thu thập dữ liệu trên thiết bị được cài đặt, kể cả khi thiết bị đó offline.
- Nó liên tục giám sát thiết bị phát hiện lỗ hổng nhanh hơn và xác nhận bản vá.
- Không cần quản trị firewall và các tài khoản mật khẩu phức tạp. Nó chỉ kết nối ra ngoài tới Qualys platform.
- Nó hoạt động với nhiều ứng dụng của Qualys, giúp đội ngũ bảo mật xoá bỏ các trở ngại về quản trị và cường hoá công cụ bảo mật.

Sử dụng nhiều ứng dụng Qualys khác nhau tận dụng Cloud Agent, doanh nghiệp có thể có cái nhìn đa chiều về các tài sản bị xâm phạm.

Cảm biến hoàn thiện, linh hoạt nhất

Có toàn bộ các lựa chọn cảm biến khiến doanh nghiệp sử dụng kết hợp các phương pháp, công cụ và công nghệ sẽ trở nên rất có ý nghĩa đối hạ tầng đặc thù và nhu cầu của họ.

Các ứng dụng Qualys Cloud

Qualys đã xây dựng một bộ ứng dụng tuân thủ và bảo mật toàn diện bao gồm 18 ứng dụng và đang được tiếp tục phát triển thêm.

Các Cloud Apps tự đọng cập nhật, quản trị tập trung và tích hợp chặt chẽ và bao phủ mỗi dải rộng các chức năng như quản trị tài sản IT, bảo mật IT, bảo mật ứng dụng web và giám sát tuân thủ.

Tất cả các ứng dụng được xây dựng trên cùng một nền tảng, chia sẻ chung một giao diện, thu thập dữ liệu từ cùng một thiết bị rà soát hay agent, truy cập cùng một kho dữ liệu, và tận dụng chung một quyền người dùng. Điều này giúp giảm thiểu độ phức tạp trong khi duy trì được khả năng kiểm soát truy cập trong doanh nghiệp.

Bảng điều khiển tập trung, nền web, giao diện đơn giản cung cấp cái nhìn toàn cảnh và liên tục cập nhật về môi trường IT của bạn. Bảng điều khiển động, tương tác này cho phép bạn kết hợp và liên kết toàn bộ dữ liệu IT, bảo mật, tuân thủ tại cùng một nơi, dễ dàng xem chi tiết và xuất bản báo cáo tuỳ chỉnh dành cho các đối tượng xem khác nhau.

Thông thường, đội nghũ bảo mật thông tin sử dụng các công cụ rời rạc, không hoạt động ăn khớp với nhau với chi phí cao và rất khó duy trì và tích hợp, khiến nó trở nên rất khó để CISO có một cái nhìn đơn giản, thống nhất về tình hình bảo mật và tuân thủ của doanh nghiệp.

Bằng cách củng cố các lớp bảo mật với Qualys Cloud Apps, doanh nghiệp có thể thoát ra khỏi cơn ác mộng những công cụ rời rạc, và giữ cho đội ngủ bảo mật luôn đồng bộ, bao gồm các khả năng bảo vệ:

- Hạ tầng tại doanh nghiệp

Qualys giúp bảo vệ mạng doanh nghiệp và các trung tâm dữ liệu với công cụ quản trị lỗ hổng, giám sát liên tục, đánh giá cấu hình, phân ưu tiên hiểm hoạ, giám sát file và chỉ dấu xâm phạm.

- Hạ tầng cloud

Qualys giúp đảm bảo bảo mật và tuân thủ đối với các tài sản cloud, máy ảo, các thiết bị lưu trữ trên nền tảng public cloud. Qualys có thoả thuận và tích hợp với các nhà cung cấp cloud lớn, do đó bạn có thể quản lý tài sản, quản lý lỗ hổng, rà soát ứng dụng web, phân ưu tiên hiểm hoạ và tuân thủ chính sách

- Tuân thủ và đánh giá IT

Qualys tự động các công việc quản trị rủi ro và tuân thủ nên doanh nghiệp của bạn sẽ luôn đạt tuân thủ theo chính sách nội bộ và các chính sách ngoài thông qua quản lý tài sản, quản lý lỗ hổng, đánh giá cấu hình, tuân thủ PCI và quản trị rủi ro nhà cung cấp.

- Thiết bị cuối

Qualys liên tục phat hiện và giám sát sự phát triển và gia tăng phức tạp của mạng lưới các thiết bị cuối một cách toàn diện thông qua quản lý tài sản, quản lý lỗ hổng, đánh giá cấu hình, phân ưu tiên hiểm hoạ và chỉ dấu xâm phạm.

- DevSecOps và ứng dụng web

Bạn có thể sử dụng Qualys để tự động kiểm tra các lỗ hổng và cấu hình lỗi trong code của bạn cho tới việc triển khai ứng dụng web thông qua quản trị lỗ hổng, đánh giá cấu hình, phân ưu tiên hiểm hoạ, rà soát ứng dụng web, giám sát file và chỉ dấu xâm phạm.

Ứng dụng Cloud tích hợp

Doanh nghiệp của bạn có thể sử dụng các Cloud App theo nhu cầu. Khi bạn cần, chỉ cần đăng ký và mở rộng sử dụng.

Nhiều khách hàng đang sử dụng nhiều Cloud Apps để hiểu sâu hơn về tình hình bảo mật và tuân thủ của môi trường IT của mình. Qualys Cloud Platform hiện tại cung cấp những Cloud App sau:

Quản trị tài sản

AI

Qualys Asset Inventory (AI)

Qualys AI giúp bạn quản trị tài sản IT một cách liên tục và hoàn thiện tại bất kỳ đâu: tại doanh nghiệp, trên cloud hoặc tại các thiết bị di động cuối. Nó liệt kê các phần phần đã cài đặt trên thiết bị, các lỗ hổng đang có và chi tiết thông tin thiết bị. công cụ tìm kiếm mạnh mẽ giúp bạn tìm kiếm và lọc thông tin sử dụng các tiêu chí khác nhau.

SYN

CMDB Sync (SYN)

Ứng dụng được chứng nhận này đồng bộ dữ liệu Qualys AI với hệ thống quản trị cấu hình ServiceNow. Các thay đổi của thiết bị ngay lập tức được gửi tới Qualys Cloud Platform và được đồng bộ với ServiceNow, loại bỏ các tài sản không được phân loại hay xác định, và trễ khi cập nhật dữ liệu.

CI

Cloud Inventory (CI)

Qualys CI giúp bạn quản trị các tài sản trên hạ tầng public cloud. Nó liên tục phát hiện các tài nguyên triển khai trên môi trường cloud và cho bạn cái nhìn đơn giản nhất về toàn bộ chúng trong một bảng điều kiển tập trung.

CRI

Certificate Inventory (CRI)

Qualys CRI tập hợp và liên tục cập nhật thông tin về tài sản chứng thư số TLS/SSL của bạn bằng cách liên tục phát hiện và phân loại chứng thư từ các Certificate Authority. Nó cũng ngăn chặn việc hết hạn chứng thư gây gián đoạn các hệ thống quan trọng, và cung cấp cái nhìn toàn cảnh về các chứng thư đã hết hạn, sắp hết hạn ngay trong một cửa sổ đơn giản.

Bảo mật IT

VM

Vulnerability Management (VM)

Qualys VM là một giải pháp hàng đầu trong ngành giúp tự động kiểm tra và quản trị lỗ hổng trong mạng doanh nghiệp, bao gồm phát hiện và lập bản đồ mạng lưới, quản lý tài sản, báo cáo và theo dõi khắc phục lỗ hổng. Dựa trên KnowledgeBase toàn diện về các lỗ hổng, Qualys VM cho phép bảo vệ trước các lỗ hổng với chi phí hiệu quả mà không tiêu tốn tài nguyên triển khai.

TP

Qualys Threat Protection (TP)

Với Qualys TP, bạn có thể ưu tiên những hiểm hoạ nghiêm trọng nhất và xác định những gì bạn cần khắc phục trước. Qualys TP liên tục liên kết các thông tin hiểm hoạ hiện có với các lỗ hổng và tài sản IT của bạn, nhờ đó bạn luôn biết được hiểm hoạ nào đang nguy hiểm nhất đối với doanh nghiệp của bạn tại thời điểm đó.

CM

Qualys Continuous Monitoring (CM)

Xây dựng dựa trên Qualys VM, Qualys CM giám sát mạng lưới của bạn với những hiểm hoạ và những thay đổi không mong muốn, trước khi chúng chuyển thành xâm phạm. Ngay khi nó phát hiện một hành vi đáng ngờ, nó lập tức gửi cảnh báo tới đúng người với mỗi tình huống và mỗi thiết bị. Với Qualys CM, bạn có theo thoi dõi những gì đang xảy ra trong phạm vi mạng công cộng, mạng nội bộ và môi trường cloud.

IOC

Indication of Compromise (IOC)

Qualys IOC cũng cấp khả năng tìm kiếm hiểm hoạ, phát hiện hành vi đáng ngờ, và xác nhận sự hiện diện của mã độc trên thiết bị trong và ngoài mạng. Từ một giao diện đơn giản, bạn có thể giám sát lịch sử và hoạt động hiện tại của hệ thống đối với tất cả các server, thiết bị cuối, và các tài sản cloud.

CS

Container Security (CS)
Qualys CS liên tục phát hiện, theo dõi và bảo vệ các nơi lưu trữ trong liên kết DevOps và triển khai xuyên suốt môi trường nội bộ và cloud. Nó cho bạn cái nhìn đầy đủ về các host lưu trữ bằng cách thu thập các thông tin về các dự án này - ảnh, ảnh đăng ký và kết nối lưu trữ từ ảnh. Qualys CS giúp bạn rà soát, bảo vệ và bảo mật các lưu trữ hiện có.

CRA

Certificate Assessment (CRA)
Qualys CRA cho phép bạn đánh giá cấu hình SSL/ TLS bằng cách cung cấp liên tục giám sát, bảng điều khiển động và báo cáo tuỳ chỉnh về các vấn đề và lỗ hổng của chứng thư. Qualys CRA tạo ra các phân cấp chứng thư sử dụng phương pháp đơn giản giúp quản trị viên dễ dàng đánh giá cấu hình của SSL/ TLS server mà không cần kiến thức quá nhiều về SSL. Nó cũng chỉ ra các chứng thư số không tuân thủ như độ dài khoá yếu.

CSA

Cloud Security Assessment (CSA)
Qualys CSA tự động giám giát hạ tầng public cloud, phát hiện các cấu hình lỗi, các hành vi độc hại và triển khai không chuẩn, và cung cấp các bước khắc phục. Qualys CSA hỗ trợ REST API giúp đơn giản hoá việc tích hợp với công cụ CI/CD, cung cấp cho đội ngũ DevSecOps một công cụ đánh giá lộ lọt và rủi ro tiềm ẩn cập nhật nhất.

Giám sát tuân thủ

PC

Policy Compliance (PC)
Qualys PC thực hiện đánh giá cấu hình bảo mật tự động trên hệ thống IT và mạng, giúp giảm thiểu các rủi ro và liên tục tuân thủ với các chính sách nội bộ và điều luật bên ngoài. Với PC, bạn có thể tận dụng thư viện chính sách để nhanh chóng theo dõi đánh giá tuân thủ sử dụng những đề xuất thực tiễn tốt nhất của ngành.

PCI

PCI Compliance (PCI)
Qualys PCI đơn giản hoá và tự động hoá tuân thủ với các yêu cầu PCI DSS để bảo vệ việc thu thập, lưu trữ, xử lý và truyền dữ liệu thẻ. Qualys PCI rà soát tất cả các hệ thống và mạng kết nối internet với độ chính xác Six Sigma (99.9996%), tạo báo cáo và cung cấp các hướng dẫn vá chi tiết. Tính năng tự động gửi báo cáo giúp hoàn thiện quá trình tuân thủ.

FIM

File Integrity Monitoring (FIM)
Qualys FIM ghi dấu và theo dõi các sự kiện thay đổi file trong hệ điều hành của doanh nghiệp. Qualys FIM thu thập các thông tin quan trọng để nhanh chóng xác định sự thay đổi và chỉ ra các hành động vi phạm chính sách hoặc có khả năng là hành vi độc hại. Qualys FIM giúp bạn tuân thủ với các chính sách kiểm soát sự thay đổi và yêu cầu giám sát thay đổi.

SCA

Security Configuration Assessment (SCA)
Một tuỳ chọn mở rộng của Qualys VM, Qualys SCA mở rộng VM với khả năng tự động đánh giá cấu hình của tài sản IT sử dụng Center for Internet Security (CIS) Benchmarks mới nhất dành cho hệ điều hành, database, ứng dụng và các thiết bị mạng. Người dùng SCA có thể tự động tạo các bản báo cáo thể tải về và xem bảng điều khiển.

SAQ

Security Assessment Questionnaire (SAQ) Qualys SAQ tự động hoá và đơn giản hoá quy trình đánh giá rủi ro nội bộ và bên thứ ba, do đó bạn không cần phải thực hiện thủ công nữa. Với SAQ, bạn dễ dàng thiết kế một khảo sát để đánh giá người trả lời kiểm soát thủ tục của chính sách bảo mật IT. SAQ tự

động việc khởi chạy và giám sát của các chiến dịch đánh giá, và cung cấp các công cụ giúp hiển thị và phân tích dữ liệu.

Bảo mật ứng dụng Web

WAS

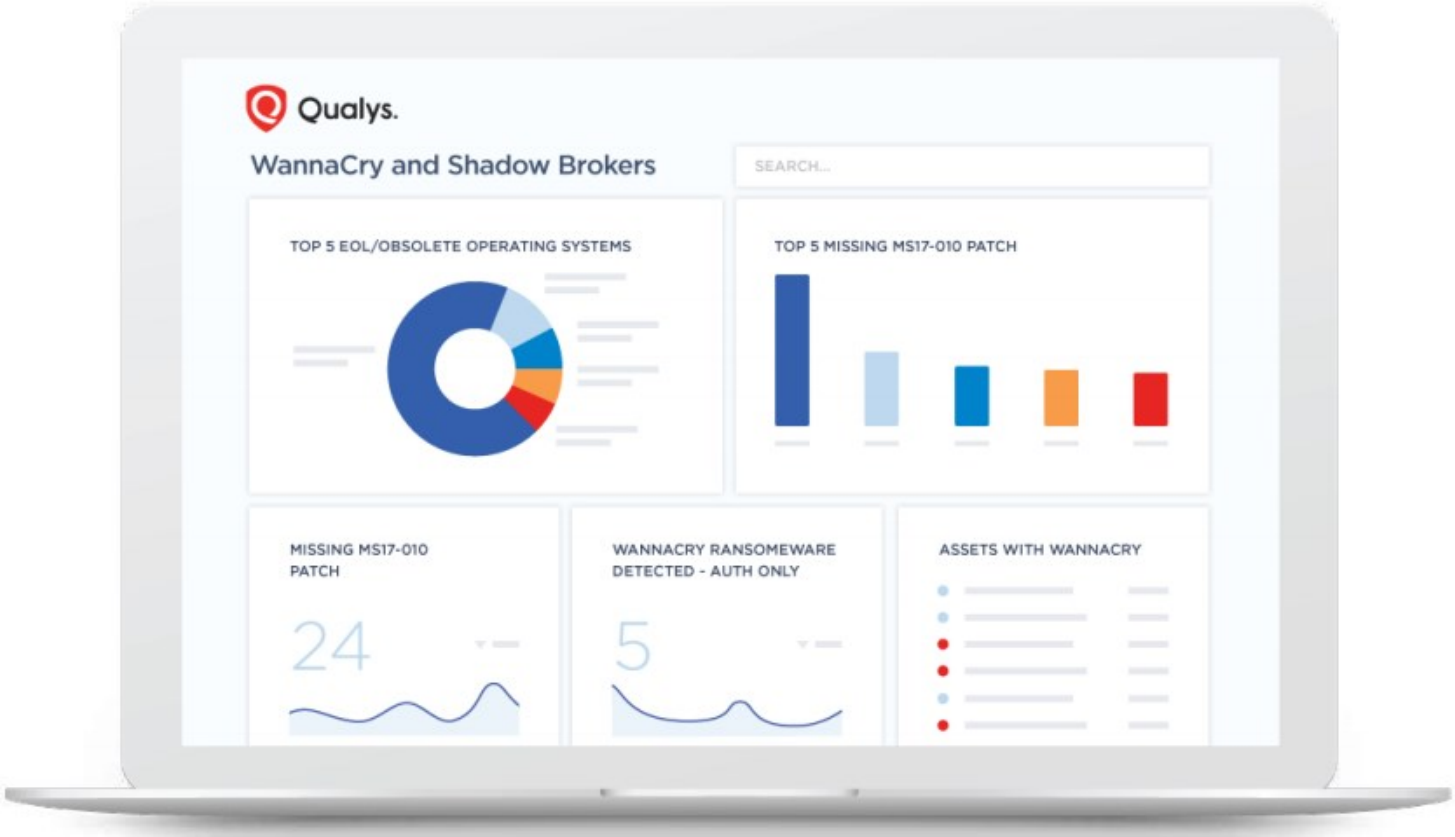
Web Application Scanning (WAS)

Qualys WAS liên tục phát hiện và phân loại ứng dụng web trong mạng và phát hiện lỗ hổng cũng như cấu hình lỗi. Tích hợp cùng Qualys WAF cung cấp khả năng vá lỗ hổng chỉ với một click. Với WAS, bạn cũng có thể đưa bảo mật vào môi trường DevOps. Qualys WAS cũng xác định và loại bỏ mã độc khỏi website sử dụng phân tích trạng thái và hành vi.

WAF

Web Application Firewall (WAF)

Đơn giản, có khả năng mở rộng và thích nghi, Qualys WAF chặn các cuộc tấn công, giúp bạn kiểm soát khi ứng dụng của bạn được truy cập. Qualys WAF và Qualys WAS hoạt động cùng nhau rất đơn giản. bạn rà soát website với Qualys WAS, triển khai bản vá ảo cho những lỗ hổng phát hiện được với một click trên WAF, và quản trị toàn bộ thông qua cổng quản trị tập trung trên nền cloud. Nó có thể được triển khai chỉ trong vài phút.

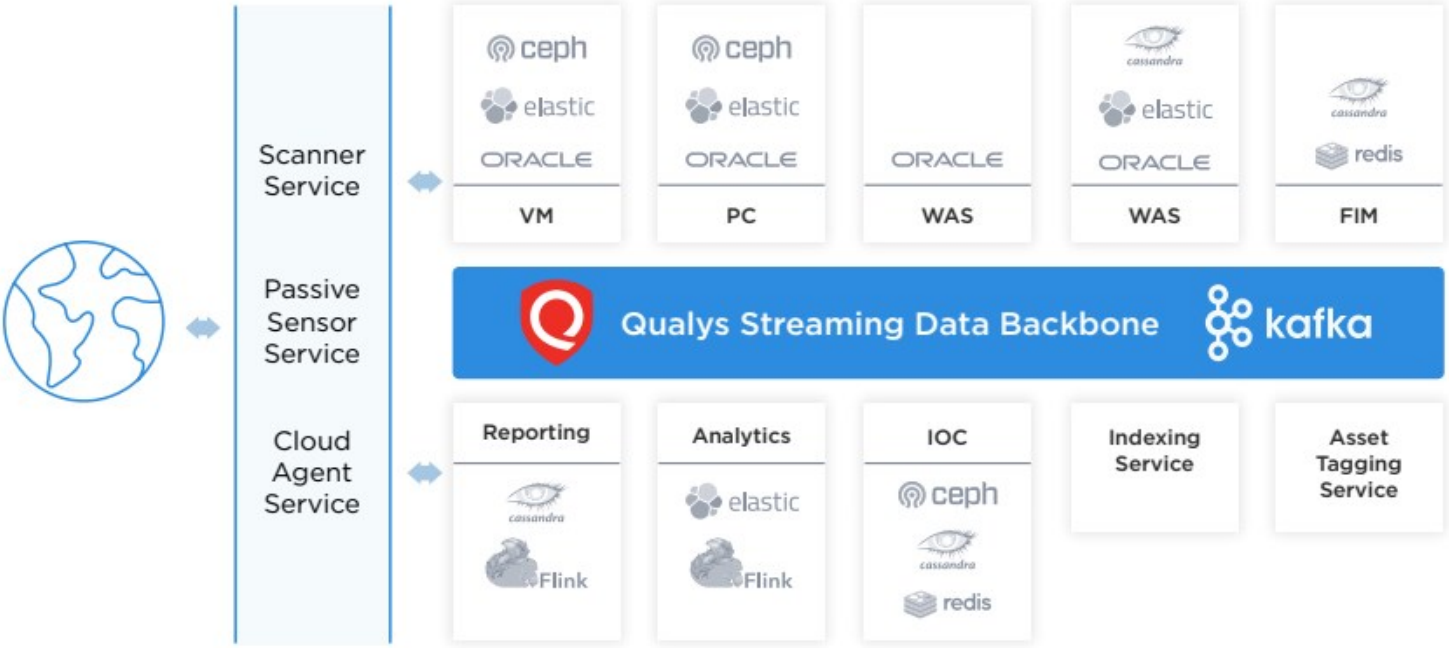


Có khả năng tuỳ biến, bảng điều khiển tuỳ chỉnh cùng với quy trình theo dõi thời gian thực của các cảnh báo khắc phục WannaCry

PHÂN LOẠI DỮ LIỆU BACK-END

HÌNH ẢNH HOÁ VÀ PHÂN TÍCH

Khả năng quản trị và gắn thẻ tài sản của nền tảng giúp khách hàng xác định, phân loại và quản trị số lượng lớn tài sản IT và tự động hoá quy trình kiểm kê và sắp xếp theo phân cấp. Trong khi đó, công nghệ báo cáo cao cấp giúp cường hoá báo cáo, biểu đồ và bảng điều khiển khiến khách hàng có thể tạo ra các hình ảnh trực quan về dữ liệu. Công nghệ phân tích lập chỉ mục hàng tỉ dữ liệu tuân thủ và bảo mật thu thập được từ môi trường IT của khách hàng, khiến những dữ liệu này có thể tìm kiếm được và liên kết được với các dữ liệu hiểm hoạ bên ngoài có trong Qualys KnowledgeBase.



Phân tích dữ liệu được thực hiện trên nhiều góc độ và quan điểm khác nhau. Ví dụ, nếu Qualys Cloud Platform phát hiện rằng một registry key bị thay đổi hoặc được thêm vào trên một máy tính xách tay Windows, dữ liệu sẽ được bắn về back-end, nơi nó được phân tích đa chiều. Trong trường hợp này, Qualys Cloud Platform sẽ tìm kiếm các nguyên nhân có thể cho sự thay đổi, điều tra xem có vi phạm tuân thủ chính sách đằng sau hay có sự hiện diện của mã độc hay không. Nói ngắn gọn, Qualys Cloud Platform nhận một dữ liệu và phân tích nó nhiều lần, một việc mà doanh nghiệp chỉ có thể thực hiện bằng cách mua vài giải pháp của các nhà cung cấp khác.

Quy trình Dịch vụ tích hợp sẵn giúp khách hàng nhanh chóng thực hiện đánh giá rủi ro và nắm bắt thông tin khắc phục, phân tính sự cố và điều tra pháp lý. Khách hàng có thể tạo các phiếu yêu cầu hỗ trợ, quản trị ngoại lệ tuân thủ và chính sách, theo dõi và tăng cấp bản vá và nỗ lực giảm thiểu rủi ro. Qualys Cloud Platform cũng có thể đẩy các thông báo tới những người phụ trách về các hành động và sự cố, như phát hiện lỗ hổng mới hay ảnh hưởng của mã độc, hoàn thành phiên rà soát, phiếu hỗ trợ được tạo hay nâng cấp hệ thống.

Lợi thế của kiến trúc trên nền cloud

• Cái nhìn đơn giản, toàn diện

Phân tích dữ liệu tập trung từ nhiều loại cảm biến khác nhau chỉ có thể thực hiện được với cloud. Thiết bị rà soát dễ triển khai và agent rất nhẹ của chúng tôi tự động gửi dữ liệu tuân thủ và bảo mật thu thập được từ môi trường IT của khách hàng tới Qualys Cloud Platform.

• Ứng dụng tốt nhất

Kiến trúc cloud của chúng tôi cho phép cung cấp một bộ ứng dụng tích hợp hoàn chỉnh, liên kết các dữ liệu rời rạc từ hệ thống nội bộ của doanh nghiệp, các thiết bị cuối và tài sản cloud, và dễ dàng thêm mới dịch vụ.

• Dễ dàng và trực quan

Không có gì để cài đặt và quản lý, tất cả các dịch vụ đều có thể truy cập trên cloud thông qua giao diện web. Qualys hoạt động và duy trì mọi thứ. Nền tảng luôn hoạt động và tự động cập nhật.

• Chi phí hoạt động thấp

Với mọi thứ trên cloud, sẽ không có chi phí đầu tư ban đầu, không cần thêm nhân sự, không có hạ tầng hay phần mềm cần mua và duy trì. Qualys cũng cho bạn khả năng kiểm soát nhiều hơn nhờ việc tính phí theo license thông qua mô hình đăng ký linh hoạt.

• Dễ dàng rà soát toàn cầu

Dễ dàng thực hiện rà soát từ bất kỳ vị trí địa lý nào và từ các phân đoạn mạng trong cả mạng nội bộ, phía sau firewall hay môi trường cloud động và thiết bị cuối.

• Liền mạch, mở rộng linh hoạt

Qualys Cloud Platform là một giải pháp có khả năng mở rộng cho tất các các dạng bảo mật IT . Sau khi triển khai, bạn có thể thêm người dùng, dịch vụ nếu cần. Các gói đăng ký được thiết kế cho mọi loại doanh nghiệp. Khách hàng cũng có thể đăng ký theo gói tuỳ ý.

• Tài nguyên cập nhật

Qualys có danh sách lỗ hổng lớn nhất trong ngành, và thực hiện rà soát 3 tỉ IP mỗi năm. Tất cả các cập nhật bảo mật đều được thực hiện theo thời gian thực.

• Dữ liệu lưu trữ được bảo mật

Dữ liệu lỗ hổng được lưu trữ và xử lý bảo mật trên kiến trúc máy chủ nhiều tầng cân bằng tải. Cơ sở dữ liệu bảo mật được bảo vệ cả về mặt logic và vật lý.

Các ứng dụng và dịch vụ được cung cấp qua nền tảng public cloud hoặc private cloud

Lựa chọn nền tảng Public Cloud

Nền tảng public cloud đa lớp, đa dụng, và có khả năng mở rộng cao, được cung cấp từ trung tâm dữ liệu đặt tại Santa Clara, California; Ashburn, Virginia; Geneva, Thuỵ Điển; Pune, Ấn Độ; và Amsterdam, Hà Lan.

Nền tảng Qualys public cloud có thể được truy cập tại bất kỳ đâu thông qua trình duyệt web, được duy trì tình khả dụng 99%. Nó cập nhật một cách rõ ràng minh bạch, không làm gián đoạn người dùng, và được chỉ định offline mỗi quý một lần để bảo trì.

Dữ liệu được lưu trữ dưới dạng mã hoá. Qualys mã hoá dữ liệu của mỗi người dùng riêng biệt, do đó chỉ có người dùng tạo ra dữ liệu đó mới có thể truy cập được. Qualys không thể xem được dữ liệu của khác hàng. Qualys cũng không thể truy cập được vào khoá mã hoá, do đó không thể giải mã được dữ liệu được lưu trữ.

Qualys Cloud Platform nằm phía sau mạng lưới, thiết bị dự phòng, firewall khả dụng cao và các giải pháp giám sát xâm phạm. Them vào đó, mỗi host chạy trên một firewall cục bộ được tuỳ chỉnh, phiên bản Linux đã gia cố, đặng biệt với Qualys.

Nền tảng được host trên trung tâm dữ liệu tuân theo SSAE 16 tối thiểu hàng năm hoặc các tiêu chuẩn ngành được kiểm tra bởi các công ty kiểm tra quốc tế. Tất cả các thiết bị được đặt tại một vị trí an toàn về mặt vật lý, riêng biệt, các cabin được khoá và bảo vệ bởi nhiều yếu tố bao gồm cả sinh trắc học.

Các dịch vụ chủ chốt bao gồm:

- Quản trị và gắn thẻ tài sản
- Bảng điều khiển và báo cáo
- Bộ câu hỏi và tương tác
- Quy trình và khắc phục
- Công nghệ phân tích và liên kết Big Data
- Thông báo và cảnh báo

Lựa chọn nền tảng Private Cloud

Đối với các doanh nghiệp cần giữ bảo mật và tuân thủ dữ liệu dưới sự kiểm soát của chính họ, chúng tôi có lựa chọn Qualys Private Cloud Platform, bao gồm toàn bộ các tính năng và lợi ích của nền tảng public cloud. Qualys Private Cloud Platform là ý tưởng dành cho những doanh nghiệp ở những quốc gia có quy định cụ thể về dữ liệu, các đơn vị chính phủ với các yêu cầu về quản lý dữ liệu, và MSSP muốn cung cấp các lựa chọn độc quyền.

Giải pháp được dựng sẵn như một máy chủ đầy đủ hoặc các rack ảo cho cách doanh nghiệp lớn, hoặc như một thiết bị độc lập dành cho doanh nghiệp nhỏ, thiết bị all-in-one được tải sẵn phần mềm của Qualys và cấu hình sẵn cho việc nhanh chóng và dễ dàng triển khai. Tất các cả rack vật lý và cáp kết nối được làm sẵn trước khi thiết bị được chuyển đến khách hàng. Các thiết bị này được cập nhật và duy trì từ xa bởi Qualys, kể cả việc mở rộng các thành phần cứng cần thiết.

Đăng ký Qualys

Doanh nghiệp vừa và nhỏ, đơn vị tư vấn và MSP, chính phủ

Qualys cung cấp cho tất cả các loại doanh nghiệp với tất cả các kích cỡ với nhiều lựa chọn đăng ký khác nhau. Các phương án có thể được tuỳ chỉnh và mở rộng để phù hợp với nhu cầu của khách hàng, với chi phí dựa trên các tính năng, ứng dụng, thiết bị rà soát, agent và phạm vi giám sát tài sản IT của Qualys Cloud Platform.

Chúng tôi cung cấp lựa chọn cho doanh nghiệp lớn, doanh nghiệp vừa và nhỏ, và các đơn vị chính phủ. Chúng tôi cung có các lựa chọn cho đơn vị tư vấn và MSP sử dụng Qualys để cung cấp bảo mật và tuân thủ cho dịch vụ khách hàng.

Tất cả các lựa chọn đều bao gồm hỗ trợ vào đào tạo miễn phí. Khách hàng có thể rà soát thiết bị và website không giới hạn, và sử dụng không giới hạn số lượng Cloud Agents.

Hãy xem chi tiết từng lựa chọn riêng biệt.

Qualys cho doanh nghiệp vừa

Đối với doanh nghiệp vừa, Qualys có thể giúp họ đơn giản hoá bảo mật IT và giảm thiểu chi phí tuân thủ. Gói Qualys Express bao gồm tính năng quản lý tài sản IT, quản lý lỗ hổng, giám sát liên tục, rà soát lỗ hổng web và firewall, phân ưu tiên hiểm hoạ, tuân thủ chính sách bao gồm tuân thủ PCI và quản trị rủi ro nhà cung cấp.

- Rà soát lên tới 5,120 IP
- Rà soát lên tới 200 web apps
- 5 scanners
- Không giới hạn số users
- Phiếu yêu cầu và theo dõi khắc phục
- Tích hợp với public clouds

Qualys cho doanh nghiệp nhỏ

Bảo mật IT thường là một liên kết rất yếu trong doanh nghiệp nhỏ, bởi họ thiếu tài nguyên và kiến thức về mảng này. Với bộ giải pháp tuẩn thủ và bảo mật Qualys Express Lite, doanh nghiệp nhỏ có thể giám sát bảo mật và tuân thủ ngay trên trình duyệt. Nó cũng có khả năng giám sát liên tục, quản trị lỗ hổng, phân ưu tiên hiểm hoạ, tuân thủ PCI, quản trị rủi ro nhà cung cấp và rà soát ứng dụng web

- Rà soát lên tới 256 IP
- Rà soát lên tới 25 web apps
- 2 scanners
- 3 users

Qualys cho doanh nghiệp lớn

Qualys cung cấp cho doanh nghiệp lớn giải pháp tuân thủ và bảo mật toàn diện, do đó họ có thể giảm chi phí bằng cách loại bỏ những sản phẩm đơn lẻ, truyền thống đang có những giới hạn về chứng năng và hoạt động chồng chéo.

- Không giới hạn số IP rà soát
- Không giới hạn số website rà soát
- Không giới hạn số scanner
- Không giới hạn số users
- Phiếu yêu cầu và theo dõi khắc phục
- Tích hợp với public clouds

Qualys cho đơn vị tư vấn và MSP

Các thách thức, yêu cầu và áp lực của các đơn vị tư vấn bảo mật là sự cường hoá, do hạ tầng của khách hàng của họ ngày càng phức tạp và các hacker ngày càng táo bạo và hiệu quả.

Để thành công, các đơn vị tư vấn không thể chỉ dựa vào kinh nghiệm và hiểu biết: họ cần có trong tay một công cụ hỗ trợ được công việc của họ.

Với lựa chọn trên nền cloud, quản lý tập trung Consulting Edition, Qualys một phần tham gia vào thị trường toàn những công cụ thủ công và có chức năng giới hạn này.

Consulting Edition giúp các đơn vị tư vấn và MSP cung cấp cho khách hàng một dải rộng các dịch vụ đánh giá tuân thủ và bảo mật ở cấp độ cơ bản.

• Dịch vụ chia sẻ: Dễ dàng quản lý và sắp xếp dữ liệu từ nhiều khách hàng khác nhau trên một bảng điều khiển tập trung. Khi bạn rà soát, kết quả trực tiếp gắn với những khách hàng liên quan. Bạn có thể chia thành các nhóm khách hàng khác nhau.

• Linh hoạt và toàn diện: Cung cấp một dải rộng dịch vụ, bao gồm quản lý lỗ hổng, tuân thủ chính sách, và rà soát ứng dụng web - tại hạ tầng doanh nghiệp, trên cloud và thiết bị cuối. Đó là nhờ cảm biến linh hoạt của Qualys, bao gồm cả nội bộ, thiết bị rà soát vật lý và ảo hoá, Cloud Agent. Tất cả các tiến trình này đều được tự động hoá thông qua Qualys API.

• Báo cáo hữu ích: Tạo các báo cáo thể hiện xu hướng lỗ hổng thuận tiện cho khách hàng và có thể lưu dưới nhiều định dạng khác nhau (HTML, DocX, MHT, XML, PDF, CSV). Bạn có thể thêm logo và cá nhân hoá báo cáo với thương hiệu doanh nghiệp của bạn.

Qualys dành cho chính phủ

Các đơn vị chính phủ đang thực hiện chuyển đổi số, việc sử dụng cloud là lựa chọn hàng đầu. Các nỗ lực bảo mật số bằng cách xác định, phát hiện và phản ứng với các hiểm hoạ mạng trong khi vẫn đạt được các yêu cầu tuân thủ và điều chỉnh là rất quan trọng trong chuyển đổi số. Để làm được điều này, các đơn vị liên bang, tỉnh thành, địa phương và DoD yêu cầu một nền tảng tuân thủ và bảo mật tích hợp, đảm bảo khả năng kiểm soát đầy đủ và liên tục môi trường IT ngày càng phát triển của họ

Nền tảng được uỷ quyền bởi FedRAMP Qualys Gov Platform cung cấp một giải pháp thống nhất cho các đơn vị có thể triển khai một cách dễ dàng với mọi quy mô, giúp dễ dàng nắm bắt được tình trạng tuân thủ và bảo mật của các tài sản IT của họ. Qualys Gov Platform khắc phục được những hạn chế của các sản phẩm bảo mật cũ vốn được thiết kế cho các môi trường đồng nhất, khép kín. Thay vào đó, Qualys Gov platform cung cấp khả năng mở rộng, nhanh nhạy và linh hoạt thông qua giải pháp phòng thủ tấn công mạng giúp bảo vệ các môi trường IT lai ghép, không biên giới và thay đổi liên tục.

Những điểm nổi bật của Qualys Gov Platform:

• **Được uỷ quyền bởi FedRAMP và chấp thuận bởi CDM**: Qualys Gov Platform nhận được uỷ quyền hoạt động của FedRAMP từ 2016, và nằm trong danh sách được chấp thuận của chương trình General Services Administration's CDM.

• **Triển khai linh hoạt**: Đối với các đơn vị có yêu cầu về quản lý dữ liệu, lựa chọn Qualys' Private Cloud Platform (PCP) cung cấp toàn bộ lợi ích của Qualys Gov Platform ngay trong trung tâm dữ liệu của bạn, giúp bạn lưu trữ dữ liệu dưới quyền kiểm soát của mình

• **Mẫu tuỳ chọn dành cho các đơn vị chính phủ**: Qualys Cloud Apps cung cấp nhiều mẫu khác nhau, có khả năng xây dựng và tạo sẵn các nội dung phục vụ cho các chính sách và yêu cầu tuân thủ.

• **Nền tảng bảo mật End-to-End**: Hoàn toàn khớp với NIST Cybersecurity Framework, Qualys Gov Platform giúp doanh nghiệp của bạn từ xác định và phát hiện, đến bảo vệ và phản ứng.

Qualys Community Edition

Nhằm giúp các doanh nghiệp nhỏ giải quyết các thách thức bảo mật và tuân thủ, Qualys cung cấp Qualys Community Edition, một phiên bản miễn phí trên nền tảng của Qualys. Với phiên bản này, doanh nghiệp nhỏ có thể tận dụng được độ chính xác và độ tin cậy của Qualys Cloud Platform để phát hiện các tài sản IT, lỗ hổng, xác định khoảng cách tuân thủ và có được các báo cáo chi tiết.

Sử dụng agent và các thiết bị rà soát, phiên bản này cung cấp phát hiện tài sản, đánh giá lỗ hổng, đánh giá cấu hình, rà soát ứng dụng web và quản trị tài sản cloud.

Thông qua bảng điều khiển tương tác, tuỳ biến và động, Qualys Community Edition cung cấp cho doanh nghiệp nhỏ một cái nhìn đơn giản và thống nhất về các tài sản và web app đang được giám sát.

Không có gì cần cài đặt, duy trì và quản lý: tất cả các dịch vụ đều trên cloud, truy cập thông qua giao diện web. Qualys Community Edition rà soát hạ tầng IT và website của họ và sử dụng cùng với Qualys Knowledgebase để xác định lỗ hổng.

Qualys Community Edition bao gồm cả Qualys CloudView và Qualys CertView.

CloudView cho phép doanh nghiệp có cái nhìn về toàn bộ các tài sản và tài nguyên cloud của họ trên một giao diện đơn giản, tập trung. Nó liên tục phát hiện và theo dõi các tài sản và tài nguyên như máy ảo, gói lưu trữ, database, nhóm bảo mật, ACL, ELB, người dùng tại tất cả các vùng miền, đa tài khoản và đa nền tảng.

CertView giúp doanh nghiệp có được sự kiểm soát các chứng thư số Internet-facing bằng cách kiểm kê và đánh giá chúng. Nó cho bạn cái nhìn vào toàn bộ chứng thư số Internet-facing và cấu hình SSL/TLS, giúp bạn kiểm soát tập trung và ưu tiên hoá khắc phục các cấu hình chứng thư. Bảng điều khiển có thể tuỳ chỉnh với các widget giúp bạn dễ dàng nắm được tình trạng chứng thư, phân loại thông tin và dữ liệu lỗ hổng.

CloudView và CertView cũng hoạt động như những ứng dụng độc lập ngoài phiên bản Community Edition.

HỖ TRỢ VÀ ĐÀO TẠO TOÀN DIỆN

Qualys nhận thấy tầm quan trọng của việc hợp tác và hỗ trợ khách hàng của họ trên suốt chặng đường.

Qualys cung cấp dịch vụ đào tạo và hỗ trợ qua điện thoại 24/7 miễn phí. Cuộc gọi sẽ được trả lời trong một phút và được chuyển tới nhân viên kỹ thuật, hỗ trợ và điều hành tương ứng. Email hỗ trợ được trả lời trong khoảng trung bình 24 giờ. Chúng tôi có trung tâm hỗ trợ khách hàng đặt tại trụ sở Foster City, California; Raleigh, North Carolina; Reading, Anh; và Pune, Ấn Độ.

Thêm vào đó, website của Qualys còn có cộng đồng hỗ trợ với hơn 20,000 thành viên, video đào tạo và kiến thức cơ bản. Tại đó, nhân viên của Qualys và khách hàng có thể chia sẽ những trải nghiệm và trả lời những câu hỏi của người khác.

Phần III

Khách hàng

Khách hàng tiêu biểu

Bằng chứng tốt nhất về chất lượng dịch vụ của chúng tôi chính là những khách hàng đã sử dụng. Qualys có hơn 10,300 khách hàng trong mọi lĩnh vực ngành nghề trên hơn 130 quốc gia. Chúng tôi cũng có khách hàng phần lớn nằm trong top Forbes Global 100 và Fortune 100.

- 9 trong top 10 khách hàng **Phần mềm**
- 8 trong top 10 khách hàng **Ngành tiêu dùng tự do**
- 8 trong top 10 khách hàng **Nguyên liệu tiêu dùng**
- 8 trong top 10 **Ngân hàng lớn**
- 8 trong top 10 khách hàng **Công nghệ**
- 8 trong top 10 khách hàng **Viễn thông**
- 7 trong top 10 ngành **Y tế**
- 6 trong top 10 ngành **Vật liệu và công nghiệp**
- 5 trong top 10 ngành **Bảo hiểm**

Qualys cũng thiết lập quan hệ đối tác chiến lược với các nhà cung cấp dịch vụ và công ty tư vấn hàng đầu bao gồm Accenture, AT&T, HPE, BT, Deutsche Telekom, HCL Technologies, IBM, Infosys, NTT, Verizon và Wipro.

VinGroup - Tìm kiếm sự tiện dụng với ThreatProtect

VinGroup là một trong số các tập đoàn kinh tế hàng đầu của Việt Nam, hệ thống công nghệ thông tin của VinGroup được xây dựng và phát triển phục vụ cho tất cả các ngành nghề kinh doanh của mình như bất động sản, giáo dục, y tế, thương mại điện tử và được quản lý tập trung.

Với bối cảnh quy mô của hệ thống tài sản IT ngày một mở rộng với nhiều chủng loại, công nghệ khác nhau, các lỗ hổng mới được phát hiện ra hàng ngày, nguồn nhân lực lại hạn chế về số lượng, kết hợp với hệ điều hành, phần mềm chưa cập nhật, các thiết bị cấu hình chưa đạt chuẩn là nguyên nhân có thể khiến hệ thống CNTT bị xâm nhập và khai thác.

VinGroup cần một giải pháp giải quyết được các vấn đề trên. Đồng thời, giải pháp cần có khả năng mở rộng mạnh mẽ bởi số lượng tài sản IT của VinGroup là rất lớn.

Hàng ngàn thiết bị, server quan trọng cần được giám sát và quản lý lỗ hổng, VinGroup lựa chọn các ứng dụng quản lý lỗ hổng, tuân thủ chính sách và ThreatProtect. Các ứng dụng này giúp Vingroup rà soát các lỗ hổng trên các thiết bị tối quan trọng, kiểm soát sự tuân thủ chính sách và bảo mật. Đặc biệt, với ThreatProtect, Qualys giúp Vingroup phân ưu tiên các lỗ hổng quan trọng, cung cấp cho Vingroup cái nhìn nhanh chóng về tình trạng hiện tại của hệ thống.

"Chúng tôi đang tìm kiếm những giải pháp có thể giúp đưa ra cái nhìn toàn cảnh nhất về hệ thống hiện tại của VinGroup. Các vấn đề cần giải quyết sẽ được tự động cảnh báo và thể hiện qua một giao diện trực quan, đơn giản. Bạn không cần phải là chuyên gia IT vẫn có thể hiểu và sử dụng được công cụ này. Với ThreatProtect, một buổi sáng ngủ dậy, thấy màn hình cảnh báo hiển thị một màu xanh an toàn, là hôm đó tôi có thể thảnh thơi làm việc" - Ian Patrick Simpson, Director Systems and Information Security

LotteFinance - Cloud Agent mang lại sự tiện lợi

LOTTE
FINANCE

Lotte Finance là một trong những công ty hàng đầu Việt Nam trong lĩnh vực tài chính. Mục tiêu của công ty là mang đến các giải pháp tài chính linh hoạt và phù hợp với phong cách sống của người dân, từ đó gia tăng giá trị và lợi ích cho khách hàng, đồng thời là cơ sở để tối ưu hóa nền tảng hạ tầng, tiệm cận với nhu cầu ngày càng đa dạng từ người tiêu dùng.

Không giống những doanh nghiệp khác, LotteFinane tìm kiếm giải pháp Cloud để đảm bảo bảo mật cho môi trường IT nhằm tối ưu hoá chi phí, tận dụng được những công nghệ tiên tiến mà không mất quá nhiều công sức trong việc quản trị và duy trì hệ thống.

Qualys Cloud Agent làm thay đổi cách thức mà Lotte Finance đang thực hiện trong việc giám sát và quản lý tài sản IT, nơi mà các chính sách bảo mật rất chặt chẽ, hạn chế việc tiến hành rà soát trong nội bộ của doanh nghiệp.

Lotte Finance với đặc thù hệ thống được quản lý rất chặt chẽ về chính sách, đồng thời các máy chủ cần giám sát được đặt tại nhiều phân vùng mạng khác nhau, việc sử dụng thiết bị rà soát trong nội bộ là không phù hợp. Do đó, lựa chọn Cloud Agent giúp Lotte Finance đơn giản hoá việc triển khai mà vẫn đảm bảo tuân thủ chính sách nội bộ. Nhờ các công cụ triển khai phần mềm diện rộng, Cloud Agent được cài đặt trên các thiết bị cần thiết và hỗ trợ cấu hình proxy để kết nối đến Qualys Cloud Platform.

Đáp ứng nhu cầu giám sát thông tin thiết bị, các phầm mềm được cài đặt, giám sát sự thay đổi của file, đồng thời phát hiện lỗ hổng và các vi phạm tuân thủ, Cloud Agent kết hợp với các ứng dụng quản lý lỗ hổng, tuân thủ chính sách, giám sát file mang lại cho Lotte Finance một giải pháp toàn diện và thống nhất.

VietFund Management - Bảo mật ứng dụng web

VFM
VIETFUND MANAGEMENT

VFM là công ty quản lý quỹ nội địa đầu tiên có tổng tài sản được quản lý lớn nhất tại thị trường Việt Nam. VFM cần có một giải pháp rà soát ứng dụng web mạnh mẽ và thân thiện, đảm bảo an toàn thông tin cho website.

Một trong những yêu cầu tiên quyết của VFM, đó là giải pháp phải đảm bảo hạ tầng linh hoạt và có khả năng mở rộng dễ dàng, đồng thời có độ chính xác cao giúp xác định chính xác các vấn đề mà website của họ đang gặp phải. Và giải pháp Cloud là sự lựa chọn phù hợp đối với những yêu cầu này.

Với Qualys WebApp Scanning, VFM dễ dàng xác định được các lỗ hổng trên website, cùng với khả năng báo cáo mạnh mẽ, tình trạng an ninh của VFM đều được hình ảnh hoá qua các loại báo cáo phù hợp cho từng đối tượng: Giám đốc điều hành, giám đốc kỹ thuật, kiểm toán, nhân viên khắc phục.

Thêm vào đó, công cụ giúp VFM luôn giám sát và loại bỏ mã độc phát hiện được trên website, và liên tục cảnh báo cho người quản trị ngay khi có sự cố hoặc hành vi bất thường xảy ra.

Phần IV

Phát triển

Dự đoán những gì sắp tới

Qualys Cloud Platform sẽ tiếp tục lớn mạnh nhờ việc liên tục đương đầu với các thách thức. Những sản phẩm mới đang được thực hiện bao gồm cả những ứng dụng cloud để quản lý bản vá và chứng thư số.

Ngoài ra: Bảo mật dành cho các thiết bị di động bao gồm Cloud Agents cho iOS, Android & Windows Mobile, EMM (enterprise mobility management), cũng như kiểm kê tài sản, quản lý lỗ hổng, phát hiện hiểm hoạ và áp đặt tuân thủ chính sách.

Chúng tôi liên tục sáng tạo và cung cấp các sản phẩm dẫn đầu trong ngành, khách hàng sẽ luôn có được những lợi ích đặc biệt từ nền tảng Qualys Cloud Platform, với định hướng cloud, phân khối, kiến trúc toàn diện và tích hợp, bao gồm:

- Các bộ giải pháp thống nhất tốt nhất
- Cung cấp trên toàn cầu
- Triển khai nhanh, đơn giản và tối ưu chi phí
- Chất lượng cao
- Liên tục cải tiến

Qualys: Xây dựng bảo mật liền mạch trong môi trường IT lai ghép nhằm thúc đẩy chuyển đổi số.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 10,300 customers in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes and substantial cost savings. The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading managed service providers and consulting organizations

Qualys, Inc. - Headquarters
Qualys is a global company with offices around the world. To find an office near you, visit
http://www.qualys.com

919 E Hillsdale Blvd, 4th Floor Foster City, CA 94404 USA
T: 1 (800) 745 4355,
info@qualys.com