



Bảo mật cơ sở dữ liệu trong kiến trúc Zero Trust

## Bảo mật cơ sở dữ liệu trong kiến trúc Zero Trust

.

Huyết mạch của doanh nghiệp kỹ thuật số ngày nay - dữ liệu - liên tục bị tấn công từ tội phạm mạng lành nghề, có tổ chức, được tài trợ tốt. Với các mối đe dọa ngày càng phát triển như ransomware như một dịch vụ, lừa đảo, botnet tiên tiến và các mối đe dọa nội bộ, các tổ chức phải bỏ lại giả định sai lầm rằng mạng là an toàn. Các phương pháp bảo mật hiện tại không bảo vệ được dữ liệu vì chúng được xây dựng trên phương pháp tiếp cận dựa trên vành đai mạng cũ.

Hệ sinh thái kinh doanh kỹ thuật số ngày nay không có vành đai truyền thống và các chuyên gia an ninh mạng có ít quyền kiểm soát hơn đối với các mạng,

ứng dụng, thiết bị và con người. Khoảng trống này sẽ tiếp tục khi các tổ chức tiếp tục áp dụng cơ sở hạ tầng đa đám mây, duy trì lực lượng lao động từ xa và triển khai công nghệ để đáp ứng nhu cầu phân tán của doanh nghiệp. Các tổ chức phải chuyển sang cách tiếp cận Zero Trust tập trung vào dữ liệu, điều này sẽ cho phép họ chuyển đổi các chương trình bảo mật của mình để phù hợp với những thay đổi cần thiết để hoạt động hiện tại và trong tương lai.

# Zero Trust là gì?

Zero Trust hoạt động trên nguyên tắc "không bao giờ tin tưởng, luôn xác minh". Đó là một giả định về vi phạm và rủi ro đó là một yếu tố cố hữu cả bên trong và bên ngoài mạng.

Thông tin nhanh

John Kindervag, một nhà phân tích ngành công nghiệp tại Forrester đã phổ biến thuật ngữ "Zero Trust" nhưng nó được đặt ra bởi Stephen Paul Marsh cho luận án tiến sĩ về bảo mật tính toán vào tháng Tư năm 1994.

Như được định nghĩa trong NIST SP 800-207, "Zero Trust (ZT) cung cấp một tập hợp các khái niệm và ý tưởng được thiết kế để giảm thiểu sự không chắc chắn trong việc thực thi các quyết định truy cập chính xác, ít đặc quyền nhất cho mỗi yêu cầu trong thông tin

Các hệ thống và dịch vụ khi đối mặt với một mạng được coi là bị xâm phạm."

**2**

## Bảo mật cơ sở dữ liệu trong kiến trúc Zero Trust

.

## Nhưng điều đó có nghĩa là gì?

Zero Trust là một mô hình bảo mật tập trung vào tiền đề rằng niềm tin không bao giờ được cấp ngầm mà phải được đánh giá liên tục. Là một mô hình an ninh, nó tập trung vào các nguyên tắc hướng dẫn để có một chiến lược phòng thủ nhiều lớp phối hợp tập trung vào:

* Giảm rủi ro đối với các chức năng và dữ liệu quan trọng
* Giám sát bảo mật toàn diện để xác định hoạt động độc hại
* Kiểm soát truy cập dựa trên rủi ro chi tiết và năng động
* Nguyên tắc đặc quyền tối thiểu

Zero Trust mang lại sự bảo mật cho người dùng, dữ liệu, ứng dụng, API, thiết bị, mạng, đám mây, v.v. mọi lúc mọi nơi – thay vì buộc họ vào một mạng "an toàn". Nói cách khác, Zero Trust chuyển vai trò nhận thức của bảo mật hạn chế kinh doanh sang bảo mật cho phép kinh doanh.

# Tại sao các tổ chức chuyển sang Zero Trust?

Không có gì bí mật rằng nhiều tổ chức có thể làm tốt hơn với các chương trình bảo mật của họ. Zero Trust cho phép phát triển chiến lược của một tổ chức. Nó cũng buộc các tổ chức phải suy nghĩ lại cách tiếp cận của họ để bảo mật dữ liệu để đáp ứng các yêu cầu của các quy định về quyền riêng tư dữ liệu và kỳ vọng từ khách hàng và đối tác kinh doanh của họ.

Các tổ chức có đầu óc rủi ro nhìn thấy cơ hội để áp dụng tư duy Zero Trust và áp dụng nó tốt nhất có thể để phù hợp với cơ sở hạ tầng nhà nước hiện tại và tương lai của họ. Không có một quy mô nào phù hợp với tất cả các cách tiếp cận và các tổ chức cần phải nhận thức được điều này mà không cố gắng buộc một số thay đổi quy trình hoặc công nghệ nhất định có thể gây ra nhiều rủi ro hơn.

Zero Trust đang trở thành mô hình bảo mật được lựa chọn cho các doanh nghiệp và chính phủ. Tuy nhiên, các nhà lãnh đạo bảo mật thường không biết bắt đầu triển khai nó từ đâu hoặc họ cảm thấy nản lòng trước những thay đổi cơ bản trong chiến lược và kiến trúc mà Zero Trust yêu cầu.

Hướng dẫn thực hành để triển khai Zero Trust, Forrester Tháng Ba 2021

**3**

## Bảo mật cơ sở dữ liệu trong kiến trúc Zero Trust

.

# Dữ liệu là trung tâm của Zero Trust

Áp dụng đặc quyền tối thiểu. Không cung cấp nhiều quyền truy cập vào dữ liệu và ứng dụng hơn mức người dùng cần. Đây là một trong những nguyên tắc quan trọng nhất của thực hành ZTX IAM vững chắc. Bạn cần có quy trình xem xét chứng thực/quyền truy cập hàng năm, theo đó người quản lý và chủ sở hữu ứng dụng/dữ liệu xem xét các quyền của người dùng và cấp hoặc thu hồi các quyền đó trong quá trình quản lý và quản trị danh tính

(IMG) nền tảng. Tương tự, bạn phải đảm bảo rằng người dùng đặc quyền không có quyền truy cập vào các chức năng quản trị

Trên các hệ thống, họ không cần phải thực hiện công việc của mình. Khi người dùng chuyển từ công việc này sang công việc khác và dự án này sang dự án khác, hãy chắc chắn ngừng quyền truy cập của họ vào tài sản. Người dùng quá đặc quyền — nhân viên, nhân viên dự phòng, đối tác kinh doanh và khách hàng — và thông tin đăng nhập truy cập ngày dẫn đến vi phạm.

Hướng dẫn thực hành để triển khai Zero Trust, Forrester Tháng Ba 2021

Để hiện thực hóa cách tiếp cận Zero Trust, các tổ chức cần chuyển sang Kiến trúc Zero Trust (ZTA). Sự thay đổi bắt buộc này không có nghĩa là bạn cần phải loại bỏ tất cả các kiểm soát bảo mật hiện tại của mình và bắt đầu lại. Zero Trust là một mục tiêu dài hạn, nhưng các tổ chức có thể bắt đầu hưởng lợi với công nghệ mà họ có ngày nay bằng cách chuyển sang nguyên tắc quan trọng là hạn chế quyền truy cập vào dữ liệu.

Có nhiều cách tiếp cận khác nhau đối với Kiến trúc Zero Trust. Một số tổ chức có thể tìm cách thực hiện phương pháp tiếp cận phân khúc vi mô, trong khi những tổ chức khác chú ý nhiều hơn đến quản trị truy cập và nhận dạng nâng cao. Các tổ chức nên áp dụng một trong những phù hợp nhất với môi trường của họ nhưng nên bao gồm các thành phần cốt lõi để giải quyết các nguyên tắc hướng dẫn. Các thành phần này bao gồm:

* **Đánh giá lỗ hổng và cấu hình:** Điều này cho phép các tổ chức liên tục hiểu trạng thái hiện tại của tài sản của họ và khắc phục các vấn đề để giảm rủi ro cho các chức năng và dữ liệu quan trọng.
* **Quản lý truy cập danh tính:** Điều này cung cấp quản lý tài khoản người dùng và thúc đẩy các chính sách kiểm soát truy cập.
* **Chính sách truy cập và thực thi dữ liệu:** Điều này đặt ra các quy tắc kinh doanh cho ai và cái gì có quyền truy cập vào dữ liệu quan trọng. Để thực thi đúng các chính sách này, việc xác thực liên tục các đặc quyền là cần thiết.
* **Giám sát và hiển thị liên tục:** Điều này cung cấp khả năng phát hiện và thu thập thông tin có giá trị để phân tích sau này. Khả năng hiển thị là cần thiết trên người dùng, ứng dụng, thiết bị, mạng, đám mây và đặc biệt là dữ liệu.
* **Nguồn cấp dữ liệu thông tin về mối đe dọa:** Điều này cung cấp thông tin từ các nguồn bên trong và bên ngoài để giúp thúc đẩy các thay đổi cần thiết đối với chính sách và cấu hình.

Trọng tâm của tất cả là dữ liệu và nó phải là một trong những động lực chính khi xem xét lộ trình của tổ chức đến Zero Trust.

**4**

## Bảo mật cơ sở dữ liệu trong kiến trúc Zero Trust

.

# Bảo mật cơ sở dữ liệu phù hợp với đâu

trong Zero Trust?

Bảo mật cơ sở dữ liệu đóng một phần không thể thiếu trong Kiến trúc Zero Trust. Biết rằng dữ liệu là trọng tâm của Zero Trust, cơ sở dữ liệu cần được coi là tài sản quan trọng với các cân nhắc bảo mật thích hợp được áp dụng.

Các phương pháp tiếp cận Zero Trust tập trung vào phân khúc vi mô hoặc quản trị danh tính và truy cập nâng cao không phủ nhận nhu cầu kiểm soát bảo mật cơ sở dữ liệu mạnh mẽ - chúng chỉ thực thi nó.

Cũng giống như bảo mật tập trung vào các ứng dụng, thiết bị, người dùng, mạng và đám mây, bảo mật được xây dựng theo mục đích cụ thể nên được tập trung vào cơ sở dữ liệu. Bảo vệ dữ liệu như mã hóa và che giấu là những phần công nghệ quan trọng, nhưng chỉ giải quyết một số mối đe dọa nhất định. Giống như các thành phần cốt lõi được đề cập ở trên, nhu cầu tập trung cụ thể

xảy ra ở cấp cơ sở dữ liệu. Cơ sở dữ liệu rất phức tạp với các hệ thống con xác thực, cấu hình bảo mật và lỗ hổng bảo mật của riêng chúng. Họ yêu cầu giám sát cụ thể cho phép họ đáp ứng nhu cầu hiệu suất của doanh nghiệp.

# Trustwave DbProtect trợ giúp như thế nào?

Trustwave DbProtect chủ động đánh giá các mối đe dọa đối với cơ sở dữ liệu để các tổ chức có được khả năng hiển thị các điều kiện trong cơ sở dữ liệu tại chỗ hoặc đám mây của họ có thể dẫn đến vi phạm dữ liệu. Nó tự động hóa việc bảo mật dữ liệu quan trọng bằng cách phát hiện ra các lỗ hổng mà kẻ tấn công có thể khai thác, hạn chế quyền truy cập của người dùng vào dữ liệu nhạy cảm nhất và cảnh báo về các hoạt động đáng ngờ , xâm nhập và vi phạm chính sách.

Các nhóm bảo mật đã sử dụng DbProtect để tuân thủ các nguyên tắc hướng dẫn cho dù họ có đang trên hành trình đến Zero Trust hay không.

* **Giảm rủi ro cho các chức năng và dữ liệu quan trọng:** DbProtect chủ động đánh giá tình hình bảo mật cơ sở dữ liệu phát hiện ra các điểm yếu bảo mật, như lỗ hổng và cấu hình sai có thể bị kẻ tấn công khai thác và dẫn đến rò rỉ dữ liệu.
* **Giám sát bảo mật toàn diện để xác định hoạt động độc hại:** DbProtect liên tục giám sát hoạt động cơ sở dữ liệu dựa trên các chính sách được xác định cụ thể của tổ chức và sẽ cảnh báo về các sự kiện đáng ngờ tiềm ẩn dựa trên phân tích hành vi.
* **Kiểm soát truy cập dựa trên rủi ro chi tiết và động:** DbProtect cung cấp phân tích đặc quyền kiểm soát truy cập chi tiết cho tất cả các tài khoản cơ sở dữ liệu. Điều này cho phép

Xác thực liên tục rằng các tài khoản quản trị, ứng dụng và dịch vụ được giới hạn ở chức năng quan trọng và quyền truy cập dữ liệu cần thiết.

* **Nguyên tắc đặc quyền tối thiểu:** DbProtect cung cấp phân tích sâu về người dùng, vai trò, đối tượng và đặc quyền cần thiết để thực thi lý tưởng Zero trust. Thông tin này được các tổ chức sử dụng để giới hạn các tài khoản cơ sở dữ liệu ở mức truy cập cần thiết cần thiết và để điều chỉnh và thực thi các chính sách truy cập dữ liệu.

Trustwave DbProtect sẽ giúp bạn triển khai các biện pháp kiểm soát bảo mật cơ sở dữ liệu cần thiết để hỗ trợ hành trình của bạn đến Kiến trúc Zero Trust.

* Phương pháp quản lý rủi ro để bảo mật cơ sở dữ liệu
* Đánh giá lỗ hổng được xây dựng theo mục đích cho cơ sở dữ liệu
* Giám sát hoạt động cơ sở dữ liệu có thể tùy chỉnh dựa trên phân tích hành vi thông minh
* Một giải pháp để bảo vệ dữ liệu của bạn tại cơ sở hoặc trên đám mây
* Tập trung khám phá, phân tích và bảo vệ dữ liệu nhạy cảm của bạn
* Thông tin khắc phục được cung cấp bởi nhóm nghiên cứu bảo mật cơ sở dữ liệu chuyên dụng của Trustwave SpiderLabs

**5**

## Bảo mật cơ sở dữ liệu trong kiến trúc Zero Trust

.

# Kết thúc

Khi các tổ chức xem xét hành trình đến Zero Trust, họ phải áp dụng cách tiếp cận tập trung vào dữ liệu. Với việc tập trung vào dữ liệu và hiểu nó sống ở đâu và ai và cái gì đang truy cập nó, rõ ràng bảo mật cơ sở dữ liệu là một phần quan trọng đối với Kiến trúc Zero Trust. Điều cần thiết là phải có những hiểu biết cần thiết về rủi ro của dữ liệu trong

cơ sở dữ liệu, có khả năng hiển thị để biết khi nào hoạt động độc hại đang xảy ra và thông tin chi tiết để liên tục xác thực rằng quyền truy cập của người dùng bị hạn chế để đáp ứng nhu cầu của doanh nghiệp.

Trustwave là nhà cung cấp dịch vụ bảo mật được quản lý và an ninh mạng hàng đầu tập trung vào việc phát hiện và ứng phó với mối đe dọa. Cung cấp danh mục toàn diện các dịch vụ bảo mật được quản lý, dịch vụ tư vấn và chuyên nghiệp cũng như công nghệ bảo vệ dữ liệu, Trustwave giúp các doanh nghiệp nắm bắt chuyển đổi kỹ thuật số một cách an toàn. Trustwave là một công ty Singtel và là chi nhánh bảo mật toàn cầu của Singtel, Optus và NCS, với khách hàng tại 96 quốc gia.

Để biết thêm thông tin về Trustwave, hãy truy cập [*www.trustwave.com*](https://www.trustwave.com/)*.*



**6**