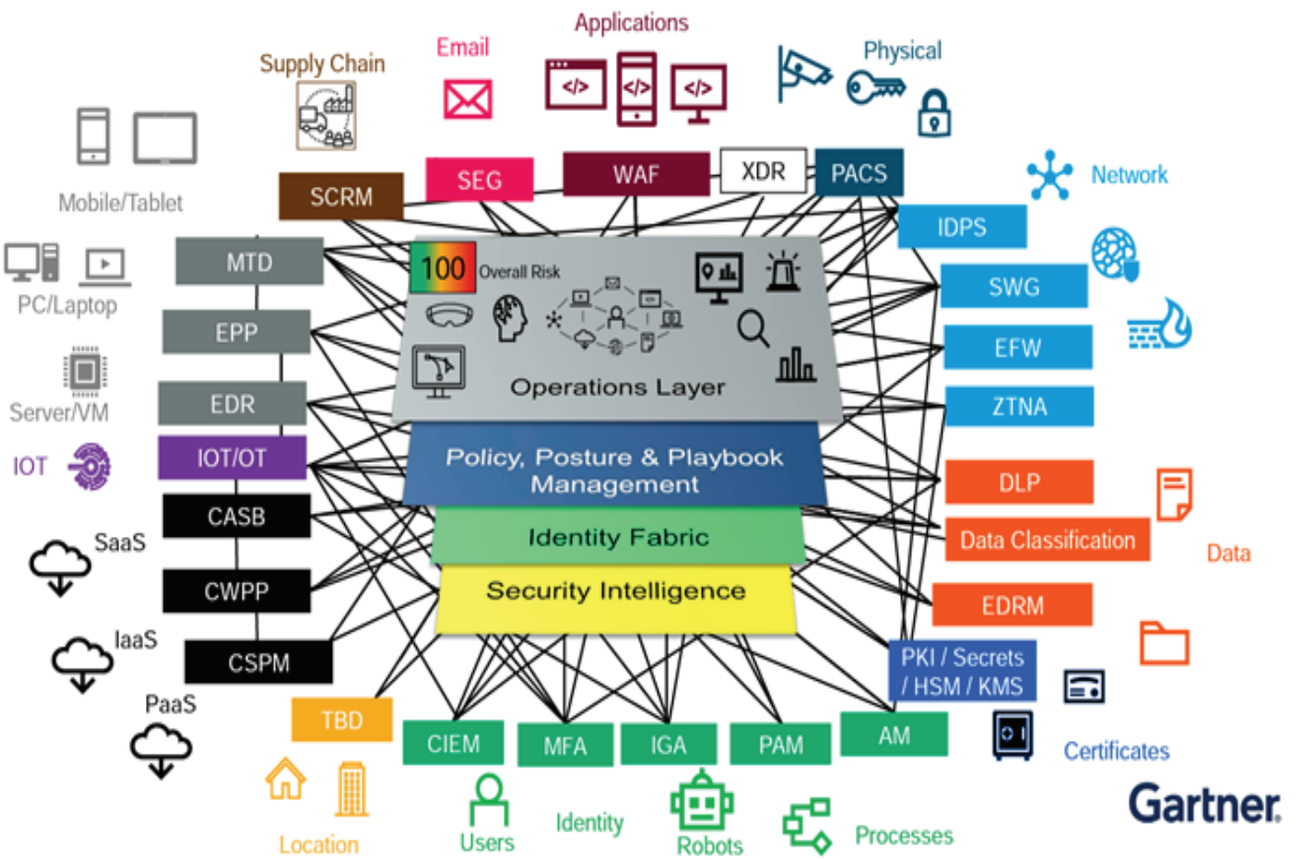


Kiến trúc mạng lưới an ninh mạng được Gartner phát triển. Ảnh: ST.

KIẾN TRÚC MẠNG LƯỚI AN NINH MẠNG: HƯỚNG TIẾP CẬN MỚI TRONG BẢO MẬT DOANH NGHIỆP PHÂN TÁN

ThS. Tạ Thị Tâm, ThS. Trương Đình Dũng

Trường Cao đẳng Kỹ thuật Thông tin, Binh chủng Thông tin liên lạc, Bộ Quốc phòng

Trong bối cảnh chuyển đổi số và mô hình làm việc từ xa ngày càng phổ biến, các tổ chức đang phải đối mặt với thách thức lớn trong việc bảo vệ tài sản số phân tán và đa dạng. Để giải quyết vấn đề này, Gartner - công ty chuyên nghiên cứu và tư vấn về công nghệ đã giới thiệu kiến trúc mạng lưới an ninh mạng (Cybersecurity Mesh Architecture - CSMA), một cách tiếp cận linh hoạt, có thể mở rộng và hợp tác trong việc xây dựng hệ sinh thái an ninh mạng.

Tổng quan kiến trúc mạng lưới an ninh mạng

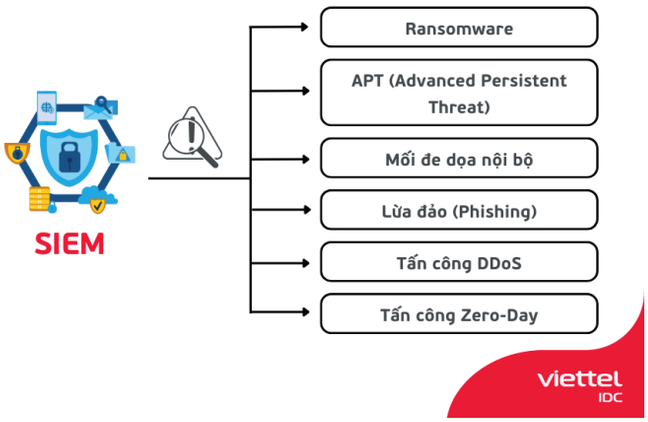
CSMA là một khung kiến trúc tổng thể cho phép các tổ chức tích hợp, phối hợp và tối ưu hóa các công cụ bảo mật hiện có. Thay vì triển khai bảo mật tại một điểm trung tâm cố định, CSMA khuyến khích việc phân phối các biện pháp bảo mật đến gần các tài sản cần được bảo vệ - cho dù đó là thiết bị đầu cuối, ứng dụng đám mây, cơ sở dữ liệu hay người dùng từ xa. Sự phân tán này giúp giảm độ trễ, nâng cao hiệu suất và đặc biệt là tăng khả năng thích ứng với các kịch bản tấn công hiện đại.

Một trong những đặc điểm nổi bật nhất của CSMA là khả năng tích hợp các thành phần bảo mật không đồng nhất vào một "mạng lưới" có thể phối hợp chặt chẽ với nhau. Điều này được thực hiện thông qua các lớp nền tảng hỗ trợ như: trí tuệ an ninh (security intelligence), hạ tầng danh tính phân tán (distributed identity fabric), quản lý chính sách và tư thế hợp nhất (consolidated policy and posture management) và bảng điều khiển hợp nhất (consolidated dashboards). Các lớp này đóng vai trò môi trường kết nối, đảm bảo rằng các công cụ bảo mật, dù đến từ nhiều nhà cung cấp khác nhau vẫn có thể chia sẻ dữ liệu, phối hợp hành động và thực thi chính sách một cách nhất quán.

Ngoài ra, CSMA cũng giúp hiện thực hóa mô hình bảo mật Zero Trust bằng cách kiểm soát truy cập không dựa vào vị trí mạng, mà dựa trên danh tính, ngữ cảnh và mức độ rủi ro. Việc triển khai hạ tầng danh tính phân tán cho phép xác thực liên tục, theo dõi hành vi người dùng và kiểm soát truy cập động, tất cả đều là những yếu tố then chốt trong chiến lược bảo mật hiện đại. CSMA mang lại một sự chuyển dịch mạnh mẽ trong tư duy bảo mật: từ "phòng thủ theo chu vi" sang "bảo mật linh hoạt theo từng điểm nút". Nhờ đó, tổ chức có thể ứng phó hiệu quả hơn với các mối đe dọa mạng ngày càng tinh vi và có thể đảm bảo an toàn cho tài sản số trong môi trường phân tán, linh hoạt và không ngừng thay đổi ngày nay.

Các lớp nền tảng của kiến trúc mạng lưới an ninh mạng

Phân tích và trí tuệ an ninh: Lớp này tập trung vào việc thu thập, tổng hợp và phân tích dữ liệu an ninh từ nhiều nguồn khác nhau như nhật ký hệ thống, sự kiện bảo mật và cảnh báo. Các công cụ như SIEM (Security Information and Event Management) và SOAR (Security Orchestration, Automation, and Response) được sử dụng để phát hiện mối đe dọa, điều tra và phản ứng kịp thời với các sự cố bảo mật.



Mô hình SIEM phát hiện mối đe dọa an ninh mạng dành cho doanh nghiệp.

Hạ tầng danh tính phân tán: Trong môi trường làm việc hiện đại, danh tính người dùng trở thành yếu tố then chốt trong việc kiểm soát truy cập và bảo vệ tài sản số. Lớp hạ tầng danh tính phân tán cung cấp các dịch vụ quản lý danh tính và truy cập (IAM - Identity and Access Management), hỗ trợ mô hình bảo mật Zero Trust - giải pháp bảo mật toàn diện, không tin tưởng tuyệt đối bất kỳ người dùng hay một thiết bị nào ngay cả khi đã được xác thực.

Quản lý chính sách và trạng thái bảo mật hợp nhất: Lớp này đảm bảo rằng các chính sách bảo mật được áp dụng một cách nhất quán trên toàn bộ môi trường công nghệ thông tin, bao gồm cả đám mây, hệ thống tại chỗ và thiết bị đầu cuối. Nó cho phép chuyển đổi các chính sách tổng thể thành các quy tắc và cấu hình cụ thể cho từng môi trường hoặc công cụ.

Bảng điều khiển hợp nhất: Trong một môi trường an ninh mạng phức tạp, việc có một cái nhìn tổng thể và thống nhất về tình trạng bảo mật là điều cần thiết. Lớp bảng điều khiển hợp nhất cung cấp giao diện trực quan, cho phép các nhóm an ninh theo dõi, phân tích và phản ứng với các sự kiện bảo mật một cách hiệu quả.

Lợi ích của kiến trúc mạng lưới an ninh mạng đối với mô hình doanh nghiệp phân tán

Tăng cường khả năng phục hồi: CSMA nâng cao khả năng phục hồi an ninh mạng bằng cách phân phối các cơ chế kiểm soát bảo mật đến gần tài sản cần bảo vệ, thay vì tập trung vào một trung tâm cố định. Khi một phần của hệ thống bị tấn công hoặc bị lỗi, các thành phần khác vẫn tiếp tục hoạt động độc lập, hạn chế tối đa rủi ro lan truyền. Mô hình này đặc biệt hiệu

quả trong các môi trường đa đám mây và phân tán, nơi mà ranh giới truyền thống không còn rõ ràng. Nhờ đó, tổ chức có thể duy trì hoạt động liên tục ngay cả trong tình huống khẩn cấp về bảo mật.

Cải thiện khả năng hiển thị và kiểm soát: Một trong những điểm mạnh lớn nhất của CSMA là khả năng cung cấp cái nhìn toàn cảnh về trạng thái an ninh của tổ chức. Thông qua các bảng điều khiển hợp nhất và hệ thống phân tích tập trung, CSMA giúp các nhà quản trị nắm bắt được hoạt động của người dùng, luồng dữ liệu, sự kiện bảo mật và các chỉ số rủi ro trên toàn hệ thống. Đồng thời, việc quản lý chính sách bảo mật cũng trở nên hiệu quả hơn nhờ khả năng áp dụng đồng nhất và linh hoạt trên nhiều môi trường khác nhau. Điều này không chỉ giảm thiểu lỗ hổng bảo mật mà còn tăng cường khả năng kiểm soát tuân thủ.

Tăng tính linh hoạt và khả năng thích ứng: CSMA mang lại sự linh hoạt cao trong việc tích hợp các công nghệ bảo mật mới mà không gây gián đoạn đến hạ tầng hiện tại. Nhờ cấu trúc mô-đun và khả năng liên kết giữa các giải pháp khác nhau, tổ chức có thể dễ dàng mở rộng, nâng cấp hoặc thay thế từng thành phần bảo mật mà không cần xây dựng lại toàn bộ hệ thống. Điều này đặc biệt hữu ích trong môi trường công nghệ thông tin thay đổi nhanh chóng, nơi mà nhu cầu bảo mật và các mối đe dọa liên tục biến động. CSMA giúp tổ chức thích nghi hiệu quả với sự đổi mới mà vẫn duy trì độ an toàn cao.

Cải thiện phản ứng sự cố và phát hiện mối đe dọa: Với sự tích hợp của các công cụ như SIEM, SOAR và nguồn dữ liệu đa dạng, CSMA nâng cao đáng kể khả năng phát hiện và phản ứng với các sự cố bảo mật. Các mối đe dọa có thể được phát hiện theo thời gian thực, quy trình phản ứng được tự động hóa nhằm giảm thiểu độ trễ và sai sót do con người. Khả năng này giúp tổ chức rút ngắn đáng kể thời gian tồn tại của mối đe dọa trong hệ thống (dwell time), giảm thiểu tác động và thiệt hại có thể xảy ra. Ngoài ra, CSMA còn hỗ trợ điều tra và phục hồi nhanh chóng sau sự cố.

*

* *

CSMA không chỉ là một khái niệm kỹ thuật mới, mà còn là một chiến lược toàn diện để ứng phó với những thách thức ngày càng phức tạp trong môi trường an ninh mạng hiện đại. Trong bối cảnh người dùng, thiết bị và dữ liệu phân tán ngày càng phổ biến từ văn phòng truyền thống đến môi trường làm việc từ xa, từ trung tâm dữ liệu nội bộ đến môi trường đa đám mây - mô hình bảo mật tập trung truyền thống đang dần bộc lộ những điểm yếu rõ rệt. CSMA ra đời như một bước tiến mang tính cách mạng, giúp tổ chức thích nghi tốt hơn với thực tế này bằng cách chuyển sang một mô hình bảo mật phân tán, hợp tác và linh hoạt hơn. Trong tương lai, khi các mối đe dọa ngày càng tinh vi hơn và ranh giới giữa các môi trường công nghệ thông tin tiếp tục mờ dần, CSMA sẽ đóng vai trò là nền tảng chiến lược để xây dựng một hệ thống an ninh mạng hiện đại, bền vững và thích ứng cao. Đây không chỉ là lựa chọn kỹ thuật, mà còn là hướng đi chiến lược mà các tổ chức cần cân nhắc nghiêm túc nếu muốn đảm bảo an toàn cho hoạt động số hóa và chuyển đổi số của mình ✍

TÀI LIỆU THAM KHẢO

1. L. Livera (2024), “Cybersecurity mesh architecture (CSMA): A new paradigm for securing the distributed enterprise”, *Linkedin*, https://www.linkedin.com/pulse/cybersecurity-mesh-architecture-csma-new-paradigm-securing-livera-egwic, truy cập ngày 04/03/2024.

2. Fortinet (2025), “What is cybersecurity mesh?”, https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity-mesh, truy cập ngày 04/04/2025.

3. S. Rose, O. Borchert, S. Mitchell, et al. (2020), *Zero Trust Architecture*, NIST Special Publication 800-207, DOI: 10.6028/NIST.SP.800-207.

4. Exabeam (2025), “SIEM architecture: Technology, process and data”, https://www.exabeam.com/explainers/siem/siem-architecture/, truy cập ngày 04/04/2025.

5. S. Shea (2025), “SOAR (security orchestration, automation and response)”, https://www.techtarget.com/searchsecurity/definition/SOAR, truy cập ngày 04/04/2025.