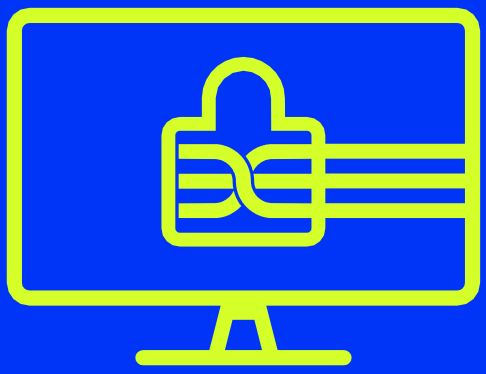
DATASHEET

Deep Instinct cho điểm cuối



Công nghệ	Ngăn chặn	Ngăn chặn mối đe dọa trong	Chỉ
DEEP LEARNING Đầu tiên trên thế giới	>99% Mối đe dọa xác định, không xác định	<20MS	1-2 cập nhật mỗi năm

Ngăn chặn các cuộc tấn công không xác định trong <20ms

Kẻ tấn công có nhiều thời gian — bạn thì không.

Kể từ khi phần mềm độc hại thực thi trên điểm cuối, việc ngăn chặn nó là cuộc chạy đua với thời gian. Các giải pháp bảo mật truyền thống cố gắng để phát hiện và ngăn chặn nhanh chóng các mối đe dọa không xác định mất vài phút, vài giờ hoặc thậm chí vài ngày — trong lúc đó phần mềm độc hại đã thực thi thành công và môi trường của bạn đã bị xâm phạm. Các công cụ thông thường có thể ngăn chặn các cuộc tấn công đã biết nhưng phần lớn không hiệu quả trước các mối đe dọa không xác định và zero-day. Deep Instinct ngăn chặn ransomware và các mối đe dọa zero-day đã biết, chưa xác định, trong thời gian <20ms trước khi một cuộc tấn công có thể thực hiện trên điểm cuối.

Deep Instinct phát hiện và ngăn chặn > 99% phần mềm độc hại đã biết và không xác định, giảm đáng kể phần trăm dương tính giả, cải thiện tính hiệu quả của các giải pháp bảo mật hiện có và giảm rủi ro tổng thể dành cho tổ chức/doanh nghiệp. Các nhóm bảo mật của bạn sẽ dành ít thời gian hơn để phản hồi các cảnh báo không nguy hiểm và nhiều thời gian hơn để tập trung vào các cảnh báo có ảnh hưởng xấu như săn lùng mối đe dọa, vá lỗi và tăng cường khả năng phòng thủ cho tổ chức/doanh nghiệp.

Sự khác biệt của Deep Instinct: Deep Learning và Machine Learning

Các giải pháp Phát hiện và Phản hồi Điểm cuối (EDR) dựa trên Machine Learning. Cách tiếp cận này yêu cầu cuộc tấn công bắt đầu thực hiện trước khi nó có thể được phát hiện. Ví dụ, ransomware bắt đầu mã hóa sau 15 giây, nhưng giải pháp EDR trung bình có thể mất vài phút hoặc vài giờ để phát hiện — khá lâu để ngăn chặn vi phạm. Vào thời điểm các công cụ EDR phát hiện một cuộc tấn công, các thiết bị nhỏ giọt đã được cài đặt trên các điểm cuối mạng của bạn.

Với công cụ Deep Learning, phương pháp phòng ngừa nhiều lớp của Deep Instinct mang lại hiệu quả cao nhất và khả năng phát hiện nhanh nhất và nó giúp phòng ngừa. Điều này áp dụng cho cả phần mềm độc hại đã biết và chưa từng thấy trước đây, cũng như các cuộc tấn công không có tệp, trong bộ nhớ và dựa trên tập lệnh. Deep Instinct cũng có thể phát hiện hành vi đáng ngờ để cải thiện khả năng săn tìm mối đe dọa, điều tra và phân tích nguyên nhân gốc rễ của bạn.

Lợi ích sản phẩm

- Ngăn chặn ransomware và các mối đe dọa zero-day đã biết, chưa xác định, trong thời gian <20ms
- Tiết kiệm thời gian bằng cách giảm đáng kể số dương tính giả xuống <0,1%
- Đảm bảo phần mềm độc hại không thực thi trên điểm cuối của bạn
- Ngăn chặn các cuộc tấn công ransomware phức tạp
- Ngăn chặn nhiều lớp chống lại các cuộc tấn công phức tạp nhất
- Bảo vệ những tấn công AI của kẻ thù
- Không yêu cầu tra cứu Cloud

Deep Instinct cho điểm cuối

Thời điểm kẻ tấn công cố gắng đưa một phần mềm độc hại lên điểm cuối mục tiêu của chúng, Deep Instinct cho điểm cuối sẽ ngăn chặn trước khi nó thực thi.

Deep Instinct tiên phong sử dụng Deep Learning trong an ninh mạng để ngăn chặn phần mềm độc hại xác định và chưa xác định, zero-day, ransomware và các cuộc tấn công dựa trên tập lệnh phổ biến cho nhiều loại tệp nhất, nhanh hơn và ít dương tính giả hơn so với các công cụ bảo mật dựa vào về chữ ký, heuristics hoặc machine learning.

Dự đoán và Ngăn chặn: Phân tích tĩnh trước khi thực thi

Ngăn chặn> 99% phần mềm độc hại đã biết và chưa biết bao gồm ransomware, zero-day, các cuộc tấn công dựa trên tệp và dựa trên tập lệnh bằng công cụ phân tích tĩnh của Deep Instinct.

- Phần mềm độc hại xác định
- Phần mềm độc hại chưa xác định và biến thể
- Các cuộc tấn công dựa trên tệp
- Zero-day
- Ransomware
- Tập lệnh chung

Các loại tệp phân tích tĩnh

- PE
- PDF
- Office
- Macro
- RTF
- SWF
- JAR
- TIFF
- Fonts
- Mach-O
- ELF
- APK
- JTD
- HWP
- LNK

Phạm vi kiểm soát tập lệnh

- PowerShell
- JavaScript
- VBScript
- Macros
- HTML applications (HTA files)
- rundll32

Thực thi: Phân tích động và hành vi

Sử dụng cách tiếp cận nhiều lớp để ngăn chặn, Deep Instinct sử dụng thêm các lớp phân tích động và hành vi để phát hiện và tự động hóa các phản ứng đối với các mối đe dọa nâng cao nhất, bao gồm:

- Các cuộc tấn công không lọc
- Chèn mã từ xa (Reflective.NET, Reflective DLL)
- Shellcode xác định hoặc chưa xác định
- Trộm cắp thông tin xác thực
- Bỏ qua Anti-AMSI
- Bán phá giá thông tin xác thực
- Phần mềm gián điệp, bao gồm trojans ngân hàng, keylogger và dropper
- Các tập lệnh nâng cao như shellcode không xác định
- Các cuộc tấn công nhiều giai đoạn
- Các cuộc tấn công AI

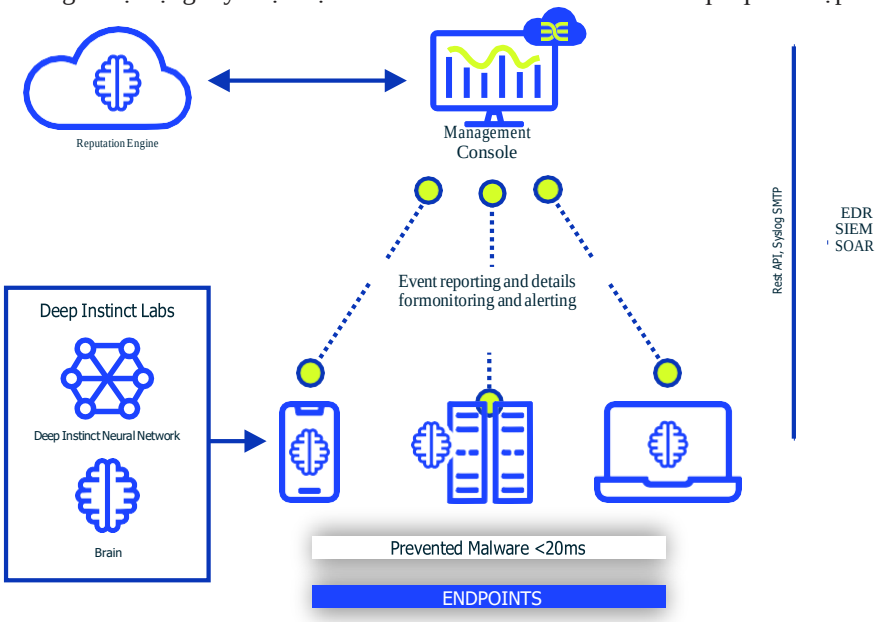
Ngoài ra, Deep Instinct cung cấp bối cảnh để hiểu mức độ nghiêm trọng và chiến thuật của một mối đe dọa:

- Cảnh báo về các sự kiện đáng ngờ để săn lùng mối đe dọa
- Thực hiện phân tích danh tiếng

Hậu thực thi: Phân tích tự động

Deep Instinct phân tích dựa trên danh tiếng và tự động tùy chọn dựa trên chính sách và danh sách cho phép đã nhập.

Kiến trúc sản phẩm



Tự động hóa phản hồi và tích hợp với SIEM, EDR, SOAR

Tất cả các sự kiện bị ngăn chặn sẽ được gửi đến bảng điều khiển của Deep Instinct và phần mềm độc hại được phân loại ngay lập tức để cung cấp bối cảnh cho cuộc tấn công đã cố gắng xâm nhập. Các tổ chức có thể đưa ra phản hồi thủ công hoặc tự động để đạt được những điều sau:

- Cách ly máy
- Cách ly / Xóa / Khôi phục
- Chính sách cập nhật: cho phép và khôi phục (Chứng chỉ, Thư mục, Tập lệnh, Quy trình)
- Chấm dứt quá trình
- Làm sạch để loại bỏ sự tồn tại
- Gửi các sự kiện bị ngăn chặn đến hộp thư để phân tích thêm

Deep Instinct tích hợp với SIEM, SOAR, EDR hoặc các công cụ bảo mật hiện có khác của bạn thông qua REST API, Syslog và SMTP để cải thiện khả năng điều tra, khắc phục và săn lùng mối đe dọa.

Tính năng bổ sung

Deep Instinct kết hợp khả năng phòng chống không gian mạng hàng đầu của chúng tôi với các bộ tính năng trực quan giúp khách hàng tiết kiệm thời gian và làm việc thông minh hơn.

Giao diện và trang tổng quan chuyên nghiệp
Bảng điều khiển quản lý dễ điều hướng của chúng tôi có thể tùy chỉnh để trình bày những gì quan trọng nhất đối với người dùng cuối được ủy quyền.

Báo cáo tích hợp
Báo cáo xu hướng và mối đe dọa tự động.

Có thể quản lý nhiều máy
Giải pháp cho nhiều đối tượng thuê riêng dành cho Đối tác, MSP và MSSP giữ cho tất cả dữ liệu được an toàn và cách ly khỏi sự lây nhiễm chéo và quản lý nhiều môi trường từ một bảng điều khiển tập trung.

Bảo mật nâng cao
Ghi nhật ký / kiểm tra đầy đủ tất cả các hành động của quản trị viên, kiểm soát truy cập dựa trên vai trò, 2FA và tích hợp SAML.

Chính sách dựa trên nhóm
Cấu hình các chính sách bảo mật dựa trên nhiều tiêu chí thủ công hoặc tự động, bao gồm quy ước đặt tên, IP, AD, OU, v.v.

Môi trường ảo được hỗ trợ

- Amazon Workspaces
- Citrix Hypervisor and XenDesktop
- VMware ESX and Horizon
- Microsoft Hyper-V

Hệ thống được hỗ trợ

- Windows
- macOs
- Android
- Chrome OS
- Linux

www.deepinstinct.com | info@deepinstinct.com

Deep Instinct áp dụng phương pháp phòng ngừa ưu tiên hàng đầu để ngăn chặn ransomware và các phần mềm độc hại khác bằng cách sử dụng khung bảo mật mạng học sâu được xây dựng đầu tiên và duy nhất trên thế giới. Chúng tôi dự đoán và ngăn chặn các mối đe dọa đã biết, chưa biết và zero-day trong <20 mili giây, nhanh hơn 750 lần so với ransomware nhanh nhất có thể mã hóa. Deep Instinct có độ chính xác >99% và hứa hẹn tỷ lệ dương tính giả <0,1%. Nền tảng phòng ngừa của Deep Instinct là một bổ sung cần thiết cho mọi ngăn xếp bảo mật— cung cấp khả năng bảo vệ nhiều lớp, chống lại các mối đe dọa trên các môi trường kết hợp.