Cisco AI Endpoint Analytics: A New Path Forward

Contents

Introduction

Figure 1.
AI Endpoint Analytics, Cisco's next-generation endpoint visibility with AI-driven analytics and network-driven deep-packet inspection

As organizations embark on digital transformation journeys, they are adding more and more devices to their network. Studies indicate that endpoints, both user and IoT devices, are projected to grow at exponential rates into the foreseeable future.

To network administrators, IoT devices present management and security challenges. Not only are their numbers increasing, they are sometimes added in an ad-hoc manner. Another challenge is that these IoT devices are might be unpatched and vulnerable due to end of life, lack of vendor support, patch availability, etc. All of these issues can increase the attack surface of your IoT and IT environment. In 2019, the Cisco® Talos® Security Research Team published 87 advisories about IoT,[1] 23 percent more advisories than the next largest category, desktop computing.

There is growing evidence that bad actors are taking advantage of these weaknesses. Cyberattacks on IoT devices surged by over 300 percent in 2019[2] and over 75 percent of vulnerabilities discovered in 2019 were from IoT devices.[3] These IoT devices are ubiquitous inside and outside your IT environment, from office spaces, parking lots, warehouses, hospitals and even in your homes. It is clear, therefore, that organizations must build appropriate security as they deploy IoT devices at scale.

[1] https://blog.talosintelligence.com/2019/12/vulnerability-discovery-2019.html

[2] Melissa Michael, Attack Landscape H1 2019: IoT, SMB traffic abounds, Blog at F-Secure.com, December 2019

[3] Martin Zeisser, Talos Vulnerability Discovery Year in Review – 2019, December 2019

The first step in securing IoT devices is knowing what devices you have in your network. Endpoint context plays a key role in identifying IT and IoT devices in a connected enterprise network. In simpler terms, "You cannot protect what you cannot see." Once identified, ensuring proper access control and segmentation prevents these IoT devices from being misused and being attacked by bad actors trying to get to your most important and sensitive data about your customers, patients (healthcare), employees, and partners. This white paper presents a solution to better secure your enterprise by enhancing your visibility to IoT devices in your enterprise.

Cisco AI Endpoint Analytics, our next-generation endpoint visibility solution, gathers deeper context from your network and IT ecosystem to make all endpoints visible and searchable. It detects and reduces the number of unknown endpoints in your enterprise using the following techniques:

1. **Deep packet inspection (DPI)** gathers deeper endpoint context by scanning and understanding applications and communications protocols of IT, Building Automation and Healthcare endpoints.
2. **Machine learning (ML)** intuitively groups endpoints with common attributes and helps IT administrators label them. These unique labels are then anonymously shared with other organizations as suggestions, where similar groups of unknown endpoints may be observed. This helps reduce the unknown endpoints and group them based on newer labels.
3. **Integrations** with Cisco and third-party products provide additional network and non-network context that is used to profile endpoints.

In summary, Cisco AI Endpoint Analytics reduces or eliminates the first hurdle that many of our customers face when implementing security policies: overcoming a lack of visibility of endpoints, with high fidelity. It is available in Cisco DNA Center Release 2.1.2.x and higher as a new application. Customers with subscription level of Cisco DNA Advantage and higher will have access to Cisco AI Endpoint Analytics. This short technology primer will look at Cisco AI Endpoint Analytics and how Cisco customers stand to benefit from it.

Endpoint profiling

Endpoint profiling starts with aggregating and analyzing endpoint data from various data sources. Examples of these data sources include network devices or appliances supporting deep packet inspection, Cisco Identity Services Engine (ISE), external configuration databases, and more. Endpoints are categorized and labelled by comparing data from these sources and from endpoints themselves to an extensive library of endpoint fingerprints or system rules to find the best match.

Cisco AI Endpoint Analytics provides you with granular endpoint profiling details by defining the endpoint type, manufacturer, model, and operating system. To support this goal, system rules are updated frequently by constantly listening and analyzing endpoint data from a large set of application and discovery protocols and from more than 250 attributes. The system rule library is a composite of a variety of IT and IoT devices in an enterprise's carpeted space, healthcare and building management, universities and more. Beyond the system rule library, Cisco AI Endpoint Analytics has a machine-learning component that helps build endpoint fingerprints, when they are not otherwise available, to reduce the net unknown endpoints in your environment.

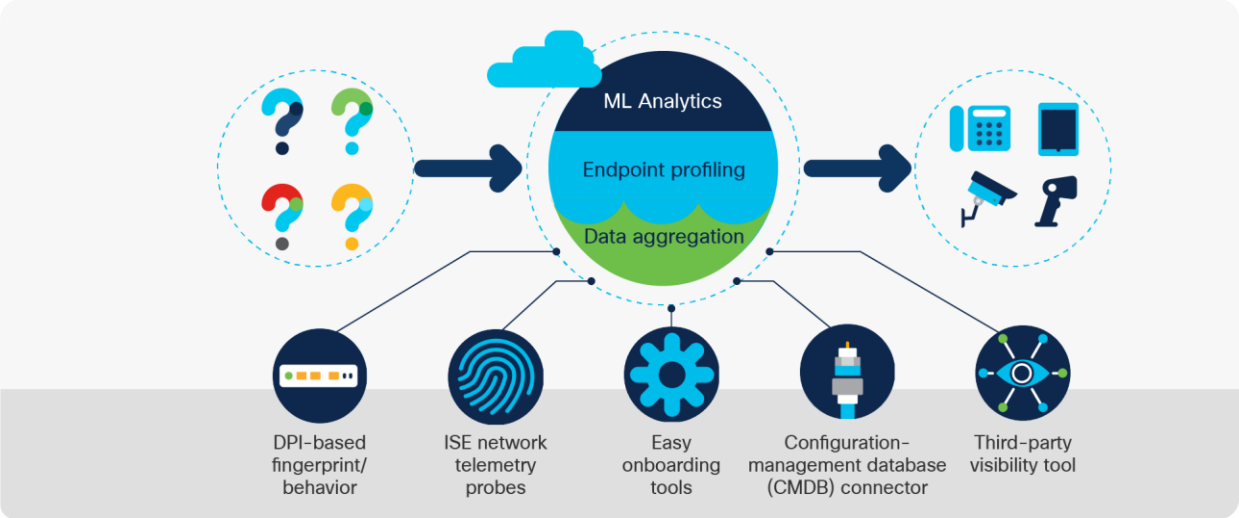

Figure 2.
Overview of AI Endpoint Analytics

Data sources

Deep packet inspection

Deep packet inspection (DPI) uses Network-Based Application Recognition (NBAR) technology to inspect the application layer of endpoint data packets that are being sent over the network. In doing this, Cisco AI Endpoint Analytics has much more context about what an endpoint may be. For example, if I told you that an endpoint was connecting to Facebook and CNN and also doing Google searches, that may lead you to believe the endpoint is a workstation or mobile device; however, if I told you that an endpoint was using a healthcare protocol called DICOM that is very specific to medical imaging endpoints, that would lead you to believe the endpoint may be a CT scanner, an ultrasound, or some other medical imaging device.

Beyond just knowing what protocols or applications an endpoint is utilizing, DPI intelligence built into Cisco AI Endpoint Analytics knows where to look within the packet payload that provides information relevant for profiling. This is based on the first set of inferences on the endpoint. For example, if it is an imaging device, DPI looks for specific information within DICOM to glean what type of endpoint it is, what model it is, who is the manufacturer, etc.

Integrations

Cisco Identity Services Engine (ISE)

Cisco Identity Services Engine (ISE) is a software application used to gain visibility of IT assets, authenticate them, and control their network access. It collects endpoint metadata from IT systems using traditional protocols such as RADIUS, DHCP, SNMP, etc., to detect IT assets in an enterprise. ISE also integrates with mobile device management providers, external data sources such as Microsoft Active Directory, and sources from endpoint agents such as Cisco AnyConnect®, to augment endpoint context. This rich context has been used on its own in ISE for profiling endpoints for many years. This data, and all the system profiling rules that are included in ISE today, is available in Cisco AI Endpoint Analytics.

ServiceNow

Many customers allow IoT device owners to use a configuration-management database (CMDB) such as ServiceNow (SNOW) to register IoT endpoints. In this registration process, the IoT device owner may directly tell the CMDB what an endpoint is by defining the asset tag, serial number, model, and more. As you can imagine, this is a rich context to aid in endpoint profiling. Cisco AI Endpoint Analytics allows you now to pull this information from your CMDB (ServiceNow will be supported at launch) and use this information to help profile endpoints.

Cisco Cyber Vision

For industrial IOT, Cisco Cyber Vision provides a comprehensive view for operations (OT) to manage endpoints and identify alarms, alerts, and vulnerabilities from the endpoints. This asset information can be shared with ISE and sent to Cisco AI Endpoint Analytics for profiling.

Third-party integrations through Cisco pxGrid

Cisco pxGrid is an open, scalable and IETF standards-driven data-sharing and threat control platform. It allows data sharing and control between more than 50 security products and ISE. Through its integration with ISE, Cisco AI Endpoint Analytics can leverage pxGrid to be a single pane of glass for all these security products.

Machine learning

Machine learning overview

Machine learning (ML) is one of the hottest technological advancements of modern times and is being used in many industries and applications such as speech recognition, autonomous driving, and much more. One of the main use cases of machine learning relevant to endpoint profiling is clustering entities. The goal of this is to group together objects that are similar to each other. Figure 3 shows an example of this. For humans, it is very easy to tell that the red data points are similar to each other, the black data points are similar to each other but that they are distinct groups from one another.

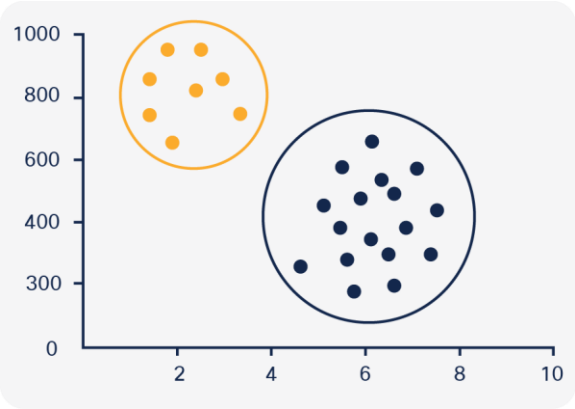

Figure 3.
Example of clustering (https://datavizproject.com/data-type/cluster-analysis/)

This is not a straightforward task for a machine, and this is where machine learning clustering algorithms come into play. Clustering algorithms take into account of the distance between cluster members, the density areas of the data space, and more, to cluster objects together similarly to the way a human would and, in many cases, cluster them more consistently and across many more dimensions than would be feasible for a human.

ML used for visibility

Now that we know what machine learning clustering is, let us see how we use clustering to help with endpoint visibility. Cisco AI Endpoint Analytics uses aggregated endpoint data and extensive profile fingerprints to profile a given endpoint dynamically. If a match is found, the endpoint is profiled, and no further action is needed. If an endpoint is still unknown, machine learning kicks in. Similar to the example above, machine learning clusters all of the unknown endpoints based on over 250 different attributes. It finds all the endpoints that are the same and proposes these endpoints to you as a cluster with an intuitive wizard that creates sets of underlying rules automatically. A key advantage here is that you are able to profile hundreds of connected endpoints at the same time. Doing this reduces the management time and effort required to tweak a profiling rule that is generic enough to capture all the endpoints you want while still being specific enough to not capture outliers.

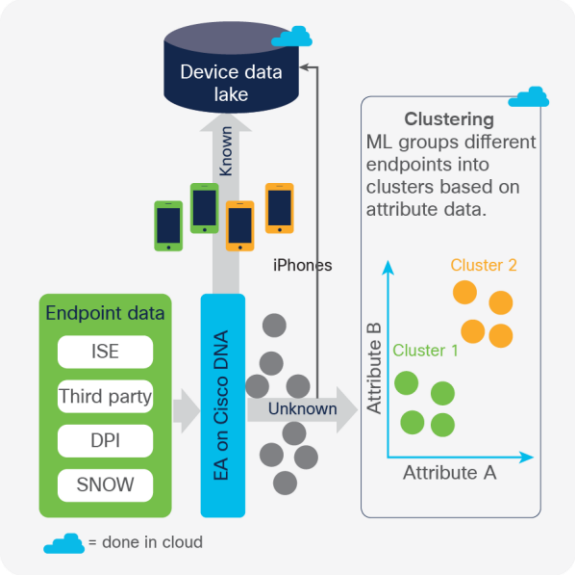

Figure 4.
Endpoint visibility using machine learning

Crowdsourcing labels

If customers use machine learning functionality in Cisco AI Endpoint Analytics to profile a group of unknown endpoints on their network, shouldn't there be a way to utilize these past experiences and data in your environment? With Cisco AI Endpoint Analytics, the answer is “Yes.” We crowdsource non-sensitive data (for example, manufacturer, model, etc.) across our vast customer base to suggest proper labels for endpoints. This completely automates the profiling workflow by associating endpoint labels with clusters, which helps administrators easily identify IoT devices they may not be aware of otherwise.

Flexible architecture

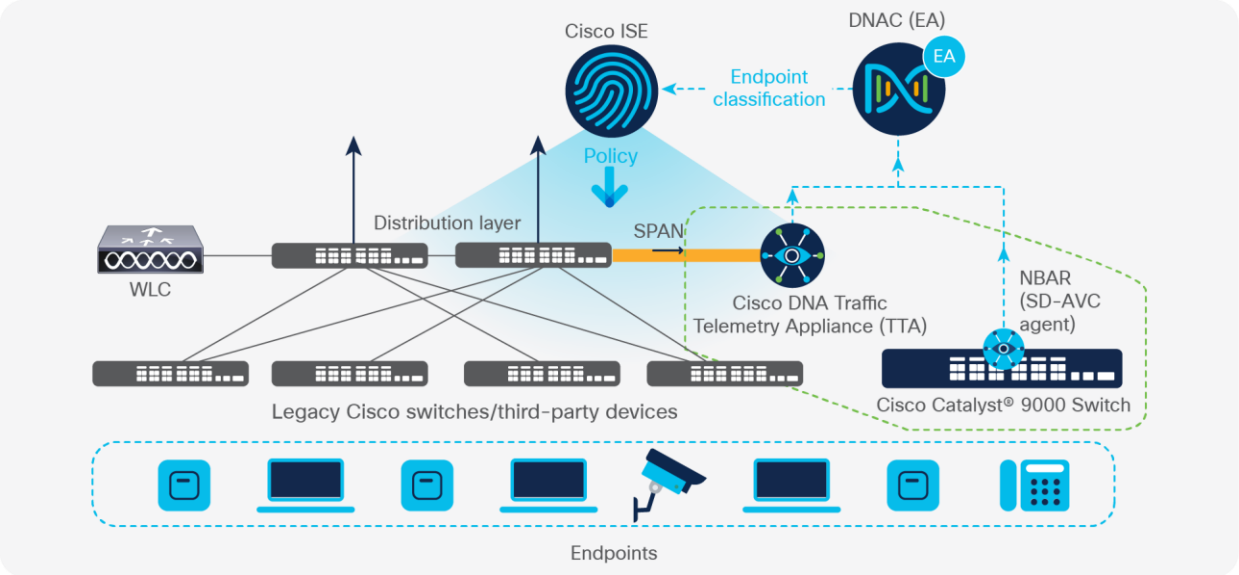

Figure 5.
Flexible deployment enabled by DPI-based profiling being supported both natively on existing network infrastructure and using a new telemetry appliance

Cisco AI Endpoint Analytics flexible architecture supports DPI-based profiling both natively on existing network infrastructure and using a new telemetry appliance. Starting in Cisco IOS® XE 17.3.1, users can enable all of the DPI-based profiling capabilities described above on their Cisco Catalyst 9000 access switches and Cisco Catalyst 9800 Series Wireless Controllers. Compared to all other solutions on the market today, this offers by far the most elegant and cost-effective approach when this infrastructure is already in place. For users who don't meet these infrastructure requirements because they have older hardware or are using third-party hardware, a Cisco Traffic Telemetry Appliance (Cisco TTA) will be available to purchase to enable DPI-based profiling capabilities. This solution works by mirroring traffic from the distribution layer to the TTA. Please reach out to your account team for more information on the Cisco TTA.

Customers who have legacy infrastructure and do not need the DPI-based profiling capabilities provided by the Cisco TTA can still take advantage of the machine learning-based profiling capabilities, built-in integrations, and all other capabilities that Cisco AI Endpoint Analytics has to offer without the use of DPI.

Regardless of the architecture, endpoint context and labels are shared with Cisco Identify Services Engine (ISE) to apply the right set of access permissions, leading to secure segmentation of the endpoints.

Product evolution

In the initial release of Cisco AI Endpoint Analytics, the primary goal is to provide granular endpoint visibility through the methods described above. Cisco AI Endpoint Analytics aims to provide further context about endpoints beyond visibility. Here is a sneak peek at what is coming soon to Cisco AI Endpoint Analytics.

Trust Score

The ability to understand and detect when an endpoint is vulnerable, exhibits anomalous behavior, or is out of an organization's compliance (posture) requirements is a challenge for today's enterprise. In order to address this need, organizations have various products and processes in place that evaluate an endpoint. Aggregating these various sources is challenging, and the results are complex due to an overload of information that is difficult to digest and commonly conflicts. Trust Score is an aggregation of various inputs and sources that evaluate endpoint trust into a single, comprehensive, and flexible score.

AI Spoofing Detection

AI Spoofing Detection introduces cloud-generated behavior models for certain types of endpoints. These models are trained using crowdsourced NetFlow data for a known endpoint type that is functioning under normal operating conditions. Abnormalities that impact the Trust Score are tracked.

This is just the first of many Trust Score sources that Cisco AI Endpoint Analytics will use to evaluate overall endpoint trust. This functionality will be expanded to understand additional context, including threats to and vulnerability of endpoints.

Conclusion

Figure 6.
The five pillars of Workplace Zero Trust Security

Using machine learning, DPI, and integrations, Cisco AI Endpoint Analytics provides fine-grained endpoint identification and labelling not previously possible. This information is extremely valuable to gather endpoint asset data and analytics of what is connecting to your network; however, remember that endpoint visibility is just the first step toward segmentation and zero trust security. These advanced security controls benefit the organization by reducing overall risk, shrinking the scope of compliance, limiting the lateral movement of malware, and containing threats like ransomware. Organizations have been hesitant to adopt them since the process can be complicated and error prone due to a lack of visibility. Cisco AI Endpoint Analytics and other zero-trust offerings in Cisco DNA Center, including Group-Based Policy Analytics and Group-based Access control Application, lower these barriers by overcoming the challenges that organizations face, gearing them to a more secure architecture model with zero trust.

References

- Get help: Cisco EN Validated Design and Deployment Guides
- Watch video: Segmentation in three easy steps
- Read blogs: Cisco AI Endpoint Analytics

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-744237-00 10/20