ESET DYNAMIC THREAT DEFENSE

Allgemeines:

ESET Dynamic Threat Defense ist eine unabhängige Testumgebung (Cloud Sandbox) zur Ausführung verdächtiger Programme. Das Verhalten des Samples wird beobachtet, dokumentiert und analysiert und die Ergebnisse sofort im Kundennetzwerk geteilt.

Cloud Sandbox:

Hierbei handelt es sich um eine physikalische oder virtuelle Testumgebung (je nach Eignung des Samples) aus verschiedenen Betriebssystemen, in denen die verdächtige Datei ausgeführt und analysiert wird, ohne die eigentliche Umgebung des Anwenders zu gefährden. Die Server der ESET Cloud Sandboxes stehen im ESET HQ im europäischen Bratislava.

Größte Sicherheitsbedenken (Marktbefragung):

Unternehmen und Organisationen sehen Ransomware und Zero-Day-Angriffe (bisher unbekannte Gefahren) als größte Bedrohung für ihre Sicherheit.

Zentrale Verkaufsaktivitäten:

Produktpräsentation (direkt) gegenüber Kunden und Partnern (Demo und PoC).

Zentrale Verkaufsargumente:

Zusätzliche Schutzschicht. Zusätzliche Marge für Partner.

Zielgruppe (Markt/Einzelkunde):

Jeder ESET Kunde mit der ESET Endpoint Security v7 oder ESET Mail Security v7 und jeder neue Kunde mit Interesse, seinen Schutz zu erweitern (Bundle-Lösung).

Marktsegment: Kunden mit 250+ Seats

Jeder Kunde, der schützenswerte Vermögenswerte, Know-how, Technologie, Patente, sensible Daten speichert und verarbeitet (Banken, Schulen, Krankenhäuser, Produzenten, Versorgungsunternehmen, Anwälte usw.), denn letztlich profitiert jeder – egal, ob bereits ESET Kunde oder nicht – von einer zusätzlichen Schutzschicht. (Interessenten mit weniger als 250 Seats werden als Ausnahmen behandelt und müssen vom ESET HQ gesondert genehmigt werden.)

Voraussetzungen für die Nutzung:

Aktiver ESET Business Account (EBA) mit Verbindung zum ESMC
ESET Security Management Center
Version 7 mindestens eines dieser Produkte

Gültige ESET Dynamic Threat Defense-Lizenz

Abgrenzung zum Standard Endpoint-Produkt:

EDTD erhöht die Sicherheit immer dann, wenn die Endpoint-Lösung nicht erkennen kann, ob eine verdächtige Datei bösartig ist oder nicht (Zero-Days/ bisher unbekannte Angriffsmethoden). Jede Datei, die durch unser LiveGrid nicht zu 100% als gutartig eingestuft wird, wird automatisch an die EDTD-Sandbox gesendet. EDTD hindert Dateien nicht selbst daran, ausgeführt zu werden. EDTD funktioniert auf den Endpoints reaktiv: Ausführbare Inhalte werden nicht blockiert, sondern im Hintergrund zur Analyse eingereicht. Handelt es sich um Schadsoftware, dann wird die weitere Ausbreitung der Malware im Kundennetzwerk unterbunden.

Abgrenzung zum Standard Mail Security-Produkt:

In Sachen Mail Security bietet EDTD bereits proaktiven Schutz: E-Mails mit verdächtigen Anhängen (unbekannte Dateien) werden durch die EDTD-Sandbox überprüft und nur dann an den Empfänger weitergeleitet, wenn sie als sauber eingestuft werden.

Abgrenzung zu LiveGrid:

LiveGrid blockiert nur solche Dateien, die als bösartig bekannt sind, keine Zero-Days/unbekannten Dateien. LiveGrid analysiert nur ausführbare Dateien, EDTD prüft Skripte, Archive, ausführbare Dateien und Dokumente. Erkennt LiveGrid eine bisher unbekannte Bedrohung, kann es einige Stunden dauern, bis Updates verfügbar sind, EDTD benötigt hierfür nur wenige Minuten. LiveGrid fügt eine Datei nur dann der Liste zu blockierender Dateien hinzu, wenn zu 100% sicher ist, dass sie bösartig ist; EDTD blockt auch verdächtige Dateien. LiveGrid schützt alle Kunden im gleichen Maß. Jeder Teilnehmer trägt durch das Einsenden seiner Daten zu einem allgemein höheren Schutzniveau bei. EDTD ist auf den Schutz des Einzelnen mit Informationen des Einzelnen ausgelegt.

Schlüsselfeatures von EDTD (allgemein):

Die EDTD-Sandbox ergänzt den ESET-Schutz um den Schutz gegenüber Zero-Day-Gefahren und Ransomware. Im Rahmen einer mehrstufigen Analyse werden aktuellste Erkennungsmechanismen, Verhaltensanalyse und Machine Learning kombiniert. Ergebnisse sind so bereits 2-5 Minuten nach Einreichung der Daten verfügbar. Die Erkennungsregeln auf allen Endpoints werden sofort aktualisiert und das komplette Unternehmen in Echtzeit geschützt. Die Ergebnisse können in Kurzübersichten oder umfassenden Verhaltensberichten abgefragt werden. Dateien lassen sich sowohl manuell als auch automatisch einreichen (private Cloud-Sandbox für Kunden).

Roadmap:

Das geplante Release v7.2 ergänzt die Lösung um „aktive“ Abwehr: Unbekannte Dateien werden vor der Analyse durch EDTD prophylaktisch auf dem Endpoint blockiert.

Zusätzliche Materialien:

https://www.eset.com/int/business/dynamic-threat-defense/
Product Bulletin:
„Lange“ Produktübersicht:
ESET Hilfe: *https://help.eset.com/edtd/en-US/*

Vergleich von ESET Dynamic Threat Defense, ESET Threat Intelligence und ESET LiveGrid®

Sowohl ESET Dynamic Threat Defense, ESET Threat Intelligence als auch ESET LiveGrid analysieren verdächtige Samples. Dennoch bestehen signifikante Unterschiede zwischen den drei Produkten in Erkennungstechnologie und -prozess.

Komponente	ESET Dynamic Threat Defense	ESET Threat Intelligence	ESET LiveGrid®	In ESET Produkte integrierte Sandbox	Windows 10 Sandbox
Datei-übermittlung	Dateien können eingereicht werden aus: • Sicherheitsprodukt mit manuell oder automatisch aktivierter ESET Dynamic Threat Defense • ESMC Web-Konsole, wenn Datei als Gefahr identifiziert wird (Bedrohungen → auf konkrete Bedrohung klicken → Details anzeigen → An EDTD senden)	Nur manuelle Einreichung von Dateien per ESET Threat Intelligence-Portal.	Automatisch und manuell. Die Mehrheit unserer Kunden hat das Feature zum Hochladen von Dateien jedoch deaktiviert und erhält lediglich LiveGrid-Feedback (Informationen zu Daten, die andere hochgeladen haben).	-	-
Analyse-ergebnisse	Analyseergebnisse können im Rahmen eines vollständigen Verhaltensberichts über die ESMC-Konsole abgefragt werden.	Das Ergebnis der Analyse kann aus der ETI-Konsole als .pdf oder .xml-Dokument heruntergeladen werden.	Keine sichtbaren Ergebnisse.	-	-
Mögliche Ergebnisse	Sauber, Verdächtig, Sehr verdächtig. Bösartig.	Erkannt, nicht erkannt.	Keine	-	-
Informationen für den Administrator	Analyseergebnisse und genaue Beschreibung des Dateiverhaltens.	Sehr detaillierte technische Informationen zum Verhalten der fraglichen Datei.	Keine	-	-

Komponente	ESET Dynamic Threat Defense	ESET Threat Intelligence	ESET LiveGrid®	In ESET Produkte integrierte Sandbox	Windows 10 Sandbox
Für Analyse verwendete Technologie	ESET Dynamic Threat Defense verwendet ein mehrstufiges Verfahren aus aktuellsten Erkennungsmechanismen, Verhaltensanalyse und Machine Learning.	ETI nutzt das Reputationssystem des ESET LiveGrid® und 100 Millionen Sensoren weltweit, um Angriffe vorherzusagen und zu verhindern.	ESET LiveGrid nutzt Fuzzy Hashing von Verhaltensmustern, die über die DNA-Erkennungen und verschiedene Machine Learning-Modelle abrufbar sind.	Ahmt verschiedene Hardware- und Software-Komponenten nach und führt das fragliche Sample in einer virtuellen Umgebung aus, um Metadaten zum Verhalten zu extrahieren. Eine tiefergehende Verhaltensanalyse wird nicht durchgeführt. Ziel ist, schnell Ergebnisse zu liefern, nicht, komplexe Malware zu analysieren.	Eingeschränkte VM ähnlich VirtualBox, jedoch ohne irgendeine Form von Malwareanalyse-Funktionen. Es wird lediglich verhindert, dass die laufende Anwendung dauerhafte Änderungen am Betriebssystem vornimmt.
Priorität der Sample-Analyse	Hoch	Hoch	Niedrig	-	-
API-Verbindung	Die Aktivitäten der ESET Dynamic Threat Defense lassen sich per ESMC-API verwalten.	There is *API* available for ETI.	Keine	-	-
Oberfläche	Web-Konsole des ESMC	ETI web portal	Keine	-	-
Unterstützte ESET Produkte	Siehe Übersicht unterstützte Sicherheitsprodukte. Zur Abfrage der Analyseergebnisse wird das ESET Security Management Center benötigt.	ETI can be used independently of any ESET products.	Alle ESET Produkte.	-	-
Automatischer Schutz für das gesamte Unternehmen	Ja	Nein	Nein	-	-

FAQ – Probleme und Themen

Mangel an Ressourcen/Zeit für die Vorbereitung einer EDTD Upsell-Kampagne:

Kunden sind der Meinung, dass APTs oder Zero Days für sie keine Rolle spielen

- EDTD erhöht nicht nur den Schutz gegenüber APT oder gezielten Angriffen. Auch andere, bisher unbekannte Samples werden schneller als bösartig identifiziert und unschädlich gemacht. Auch wenn der zentrale Benefit der Schutz vor APTs oder Zero Days ist: EDTD verbessert die Abwehr aller Arten von Gefahren.
- Stichwort WannaCry: Ist den Angesprochenen egal, ob ihre sensiblen Daten in unbefugte Hände gelangen oder gelöscht oder verschlüsselt werden, ist EDTD sicher nichts für sie. Hardware-Komponenten (z.B. Intel CPUs) sind leichte und daher beliebte Beute – das Unternehmen ist den Angreifern dabei relativ egal. Für das Unternehmen bedeutet ein erfolgreicher Angriff jedoch Betriebsausfälle mit teils hohen Verlusten.

Wir (Partner/Niederlassungen) brauchen Argumente zur Kundenansprache, warum die aktuelle Sicherheitslösung des Kunden für Mails oder Endpoints eventuell nicht alle Sicherheitsvorfälle abdecken kann.

- Die Bedrohungslage entwickelt sich stetig weiter, ebenso wie ihre Abwehr. EDTD leistet hier einen wichtigen Beitrag, Unternehmen dauerhaft bestens abzusichern.

Unsere Kunden fragen, warum ESET Endpoint Security als „umfassende Mehrschichtlösung" verkauft wird, wenn das eindeutig nicht der Fall ist. Werden die Produkte für Mail und Endpoint Security durch EDTD zur „Economy Class" degradiert?

- Nicht wirklich. Die Aussage „umfassende Mehrschichtlösung" hat nichts von ihrer Gültigkeit verloren. Nichtsdestotrotz gibt es Malware, die innerhalb der engen Grenzen des Endpoints nicht als solche erkannt werden kann. Hierfür bedarf es beispielsweise einer externen Cloud Sandbox. Wird die ESET-eigene Sandbox EDTD verwendet, arbeitet sie nahtlos mit den bestehenden Lösungen für Endpoint und Mail Security zusammen und kann komfortabel per ESMC verwaltet werden.

Die Kunden erwarten von ihrem Endpoint/Mail Security-Produkt, dass es sie vor Ransomware schützt.

- Das ist von der Situation abhängig. Aktuell ergänzt EDTD unsere Endpoint/Mail Security-Lösungen und sorgt so für modernste Sicherheit.

Preisgestaltung: Durch EDTD steigen die Preise von ESET Mail und Endpoint Security-Lösungen, im Fall der Mail Security sogar um das Doppelte

- Fragen Sie, welchen Mehrwert Sicherheit Ihren Kunden bietet. Wie wertvoll sind die Daten, die er im Fall eines Ransomware-Angriffs durch Verschlüsselung verlieren würde? Fragen Sie auch nach bestehenden Backup- oder anderen Absicherungsstrategien. Warum wurden diese eingesetzt – wenn nicht, um wertvolle Daten zu schützen?

Effizienz von EDTD

- EDTD erweitert den ESET Schutz um eine zusätzliche Schicht und sorgt dafür, dass auch unbekannte Malware keine Chance hat. Dieser Mehrwert lässt sich nur schwer in Zahlen ausdrücken – ist doch kaum absehbar, wann eine unbekannte Gefahr auftritt. Es geht also weniger darum, wie konkret EDTD den Schutz erhöht, sondern darum, ob ich in Zukunft auch gegenüber unbekannten Bedrohungen sicher sein möchte.

Gibt es EDTD Use Cases? Kundenerfahrungen aus der Praxis?

- Im Schnitt wäre jede 1000ste Datei, die bei der EDTD eingereicht wird, von den Endpoint Lösungen nicht als verdächtig erkannt werden.

Können wir verlängerte Trials anbieten (z.B. 90 Tage)?

- Ja

Die meisten Kunden haben nur wenig Budget für Sicherheitsausgaben zur Verfügung

- Arbeiten Sie mit der Ransomware- und Cloud Sandbox-Kampagne für Ihre Argumentation. Hier werden beispielsweise Umfrageergebnisse genannt, nach denen Unternehmen Ransomware als das höchste Risiko für ihre Datensicherheit einschätzen.

Cloud Sandbox in der EU – Bedanken beim Versand von Daten ins Ausland

- Die EDTD-Server stehen im ESET HQ (Bratislava, Slowakei). Keine einzige Datei wird an andere Server gesendet. Zusätzlich können die Nutzer festlegen, ob eine eingereichte Datei sofort nach der Analyse, 30 Tage später oder niemals gelöscht wird.

Minimum 250 Seats

- Wir haben entschieden, dass das 250+Segment unsere Zielgruppe ist. Verkäufe unter 250 Seats sind möglich, erfordern aber einen gesonderten Prozess. Bitte befolgen Sie die darin festgeschriebenen Regeln.

Können wir Gratis-Lizenzen im Austausch für Case Studies herausgeben (an Krankenhäuser, Bildungseinrichtungen usw.)?

- Ja