zebracloud

EndPoint Protection Suite

New age cyber-attacks are becoming more and more sophisticated. At times, attackers choose to focus on a specific organization after conducting extensive research and successfully breaching the organization's network.

A standard defense system is not always enough to stop an unfamiliar real time attack that can penetrate various defense mechanisms. Using next generation defense with the ability to document the attackers' activities over time and use investigative tools to identify an attack, provides better protection to end users.

ZebraCloud Services was established to provide small and medium sized organizations with access to edge technologies that are generally designed and deployed across large organizations. These small and medium sized organizations present information security needs that require harsh standards and high compatibility demands, based on pay-as-you-go models.

For the first time, ZebraCloud Services presents the Endpoint Protection Suite, designed for organizations with the following needs:

Next generation protection for endpoints, servers and mobile devices from cyber-attacks, viruses, spyware and ransomware. 1

Protection to endpoints via advanced technologies, such as machine learning and behavior monitoring. 2

Protection to on-premises network, including lap tops (using off-premises server). 3

Cloud managed services without the need for server installation or maintenance. 4

Protection to Office 365, file sharing and keeping with regulations. 5

Protection to email from phishing, spam, viruses and ransomware. 6

Endpoint Detection and Response (EDR). 7

"Sandbox" technology for advanced file inspection. 8

XDR abilities for analyzing information security issues in on-premises email and endpoints. 9

Protection to endpoints, servers and devices from cyber attacks

The system provides next generation protection for workstations, computers and Mac and Windows servers. The system also supports protection to iOS and Android wireless devices.

Protection to computers in and off premises network for remote employees

The Endpoint Protection Suite is a cloudbased service, which protects on-premises computers as well as remote employees connected to a home or public network.

Cloud managed services without the need for server installation or maintenance

The Endpoint Protection Pro defense service is a cloud-managed service that does not require the installation of servers. The system undergoes automatic maintenance and updates without the need for IT team intervention.

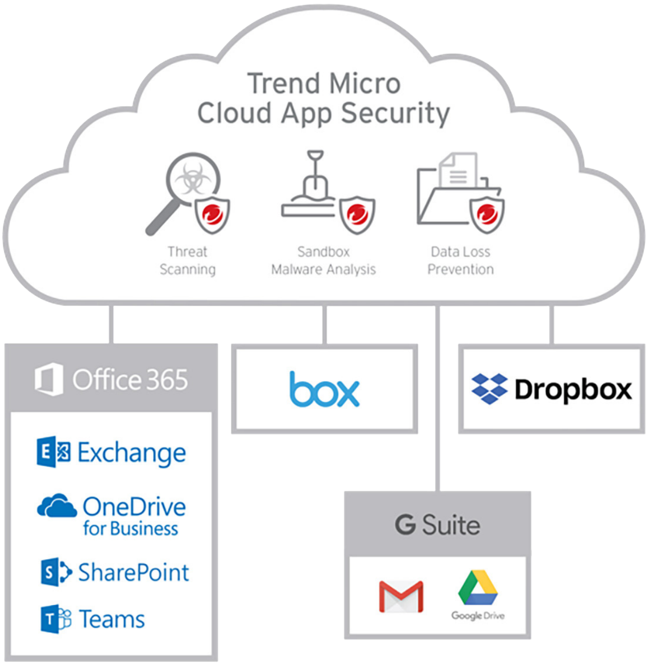
Protection to Office 365, file sharing and keeping with regulations

The Cloud App Security solution is used to protect Office365 via an integrated API. The solution provides protection to email services from phishing, spam, malicious files and Business Email Compromise (BEC), by using advanced machine learning and "sandbox" technologies.

The connection to Office365 allows for monitoring and protection to shared files, such as SharePoint and OneDrive.

The system knows how to interface with other file sharing services, such as Google Drive, Dropbox and Box.

Incoming documents are examined for malware and Data Leak Prevention technology is used to avoid information leakage.



Protection to email from phishing, spam, viruses and ransomware

The need to deal with “Zero Day” threats encouraged information security solution manufacturers to develop advanced identification systems that are not dependable on signature files. These systems .are based on machine learning

The Endpoint protection suite technology incorporates systems based on signature files, reliability rankings and machine learning monitoring behavior. This combination and the use of correct .techniques allows for a reduction of resource consumption and errors

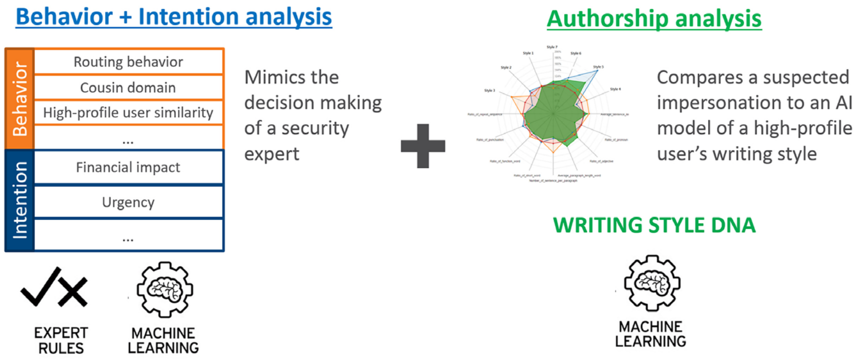
There is a significant improvement in protection from “Zero Day” threats with maximum efficiency .while retaining high performances
The system uses familiar attack identification abilities by advanced machine learning monitoring behavior technologies with predictive machine learning, based on the behavior of the attack, comparison to other attacks and analyses of significant data. The system also uses analysis .techniques for unfamiliar attacks activated in sandbox environment

Business Email Compromise (BEC) and online fraud prevention

Impersonation attacks and money extortion attempts have become very common and more challenging, as their human component makes them difficult to stop. Attacks of this sort can be identified and blocked by using a combination of advanced technologies in the suggested solution.

Examining headings and content of e-mails

Using the “writing style DNA”, the system studies the behavior and nature of e-mails from legitimate senders, such as the CEO or CFO. For example, fonts, spaces and punctuation marks can provide information on whether the email is legitimate or malicious. The system also contains a database of risk indicative words, such as the urgency of the email, a request for fund transfer and the like. Key words: urgent, payment, request.


Behavior + Intention analysis
Behavior
Routing behavior
Cousin domain
High-profile user similarity
...
Intention
Financial impact
Urgency
...
Mimics the decision making of a security expert
EXPERT RULES
MACHINE LEARNING
Authorship analysis
Compares a suspected impersonation to an AI model of a high-profile user’s writing style
WRITING STYLE DNA
MACHINE LEARNING

Endpoint Detect and Response

The EDR system provides a solution for collecting and storing information (values, files) in endpoints and documenting changes made to the activation system. The EDR inspection tool provides a network examination ability using sensors scattered in endpoints, allowing for unique identification, such as hash files, registry values, processes and etc, in order to identify whether the station has been harmed.

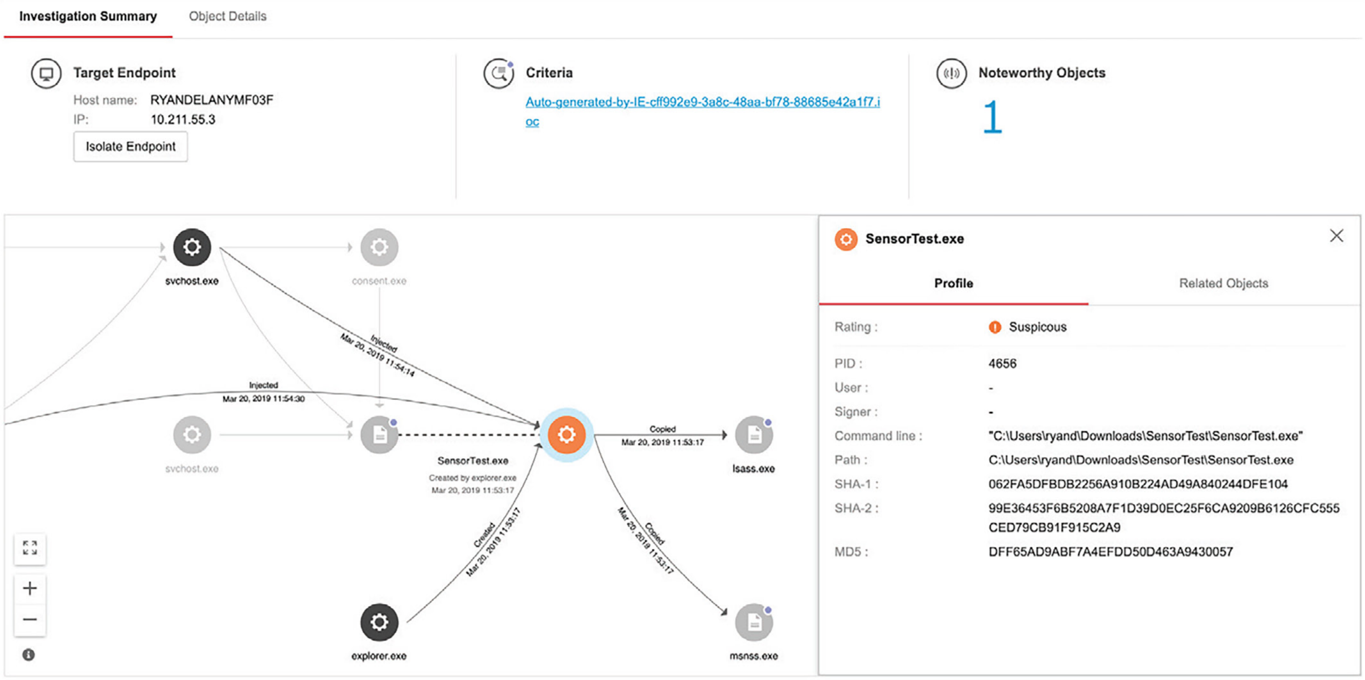
There are a number of questions the organization needs to answer in order to deal with an information security breach.

- How did the attacker manage to penetrate the network?
- When did the attacker penetrate the network and began the malicious conduct?
- What has the attacker done to the network and what are the ramifications?
- Has the attack spread to additional stations/points and servers on the network?

The EDR system provides an answer to these questions by documenting and collecting information (values, files) of the agents in the workstation. Furthermore, the system supports identification of the attackers using open IOC (indicators of compromise). The IOC is used to seek attackers online using a number of known indicators together identifying an attack on the station. The open IOC is an integrative indicator database used to identify attacks.

The EDR system has an automated response ability to identified events, such as, blocking malicious activation files and compartmentalization of a workstation to prevent it from harming the rest of the network while maintaining connection to the server for further inquiry. Responses to events can be manual or automatic. Additionally, a rollback can be performed on files infected by the ransomware attack.

Below is an example of the ability to isolate an event and its related files during the event:



Target Endpoint

Host name: RYANDELANYMF03F
IP: 10.211.55.3

Criteria

Auto-generated-by-IE-cff992e9-3a8c-48aa-bf78-88685e42a1f7.ioc

Noteworthy Objects

1

SensorTest.exe

Rating :	Suspicous
PID :	4656
User :	-
Signer :	-
Command line :	"C:\Users\ryand\Downloads\SensorTest\SensorTest.exe"
Path :	C:\Users\ryand\Downloads\SensorTest\SensorTest.exe
SHA-1 :	062FA5DFBDB2256A910B224AD49A840244DFE104
SHA-2 :	99E36453F6B5208A7F1D39D0EC25F6CA9209B6126CFC555CED79CB91F915C2A9
MD5 :	DFF65AD9ABF7A4EFDD50D463A9430057

zebracloud

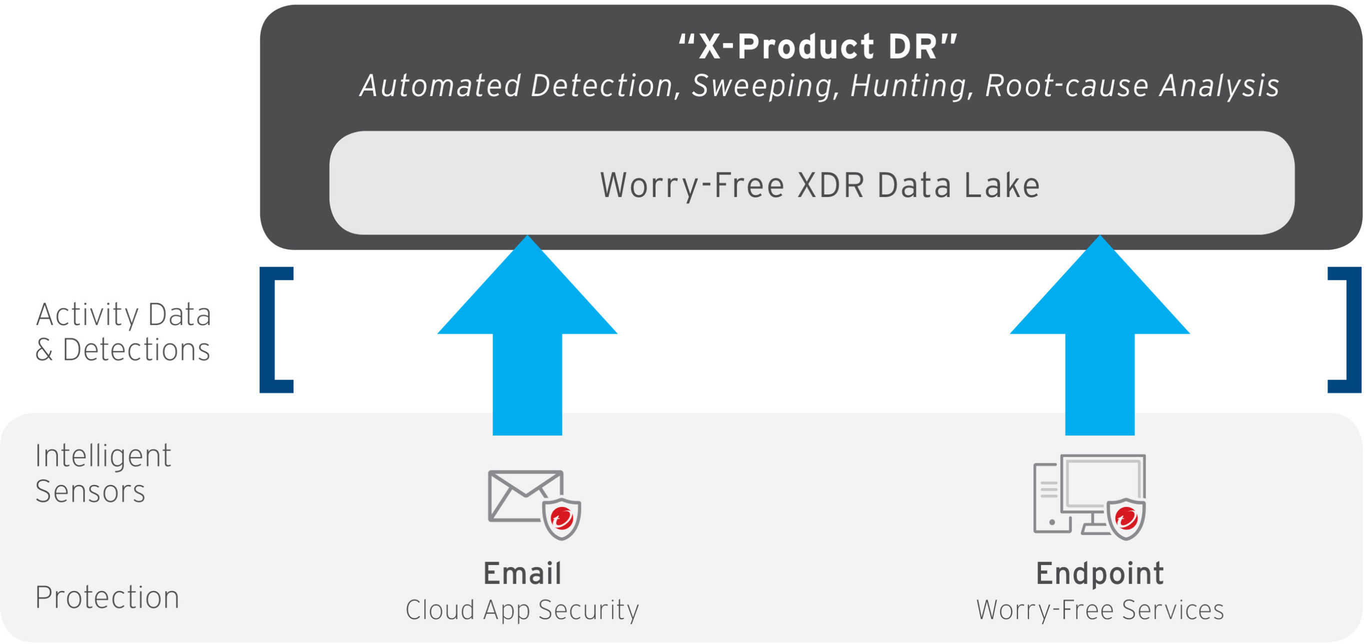
Sandbox as a Service

As attack abilities progress and advance, the need to better the organization's defense and testing array arises. The sandbox service allows to send unfamiliar files for advanced testing using a technology that allows to open the file in a simulated environment, using a number of activation systems, to analyze it and understand whether it is malicious or not. The solution produces detailed reports on the activity of the file in the simulated environment, explaining the decision made in the examination of the file. The technology supports a large number of files, including activation files, Office and PDF.

XDR abilities to analyze information security breaches in on-premises email and endpoints

The Endpoint Protection Suite integrates an investigative ability, automated identification and responses from the e-mail channel and from endpoints, with the following abilities:

- Automated information collection from the agent in the station and from the email.
- Option to automatically search and analyze events online.
- A unified managing interface to inspect events from both e-mail channel and endpoints.
- Identification of advanced attacks using a cloud-based Sandbox engine.



Endpoint Protection Suite system abilities

Protection to end components

Advanced Threat Protection and Web Security.

The system provides safe browsing and protection from advanced attacks.

Mobile Device Security and Management.

Protection to mobile devices from a central managing interface.

User protection

Application control

Blocking the activation of unauthorized apps on computers. Ability to work using “white list” and “black list”.

Web Reputation

Examining websites using the micro trend for secure communication database.

URL Filtering

Ability to filter sites and categories to prevent browsing to unauthorized sites.

Information protection

Data Loss Protection

Avoiding and monitoring leakage of critical information out of the organization.

Device Control

Blocking external devices, including hard drive and disk-on-key.

Ransomware Protection

Protection from ransomware attacks that harm the organization and maintaining functionality.

Encryption Management

Ability to encrypt and manage computers using BitLocker.

Event inspection ability and “Sandbox”

Efficient Endpoint Recording

Saving information regarding changes in files and connections to servers by a worry-free agent, in order to allow for an easy inspection.

IOC Sweeping

The information saved to the system allows a quick inspection, without the need to search for information in endpoints.

Flexible Searching

Search and inspect options of parameters such as specific communication, attackers, registry, user activity and processes. Additionally, there is support in inspection via Open IOC rules.

Root cause analysis

The ability to inspect and analyze events, objects and processes and understand how they reached the network.

Immediate Response Options

An automated response ability to events, including file blockage, station isolations or reconstruction of files harmed by the ransomware.

Protects Office 365 Email from Phishing and Advanced Malware

Protection of Office 365 email from BEC attacks, malware and ransomware.

Protects Internal Email

API interfacing to Office 365 for scanning email on-premises.

DLP and Advanced Malware Protection

The service prevents information leakage and malicious file blockage for OneDrive for Business, Sharepoint, Dropbox, Online Box and Google Drive.

Sandbox

Advanced file examination using the “sandbox” technology, initiating unfamiliar files and links in a simulated environment to identify prior unfamiliar attacks.

File Blocking

Blocking different types of files.

zebracloud

Email Security system abilities

Layered Protection

Mail Gateway solution provides protection from phishing, spam and graymail.

Email Fraud Protection

Protection from BEC attacks, impersonation and fraud while using machine learning technologies and "writing style DNA" in order to identify the user and check the content and components of the message.

Document Exploit Protection

Identification of advanced vulnerabilities in Office and PDF documents via statistical and heuristic testing.

URL Time-Of-Click

Blocking emails containing malicious links prior to reaching the user's mailbox and rechecking the links in real time when clicked on by the user.

Source Verification And Authentication

An ability to verify the identity of the email sender using advanced technologies, such as DMARC, DKIM, SPF.

Threat intelligence

Blocking information security attacks while comparing to Micro TrendTM Smart Protection Network, a large database with email addresses, fields, files and malicious websites.

Email Encryption

The ability to send emails securely to designated email addresses while encrypting the email and using a decoding managing system.

DLP

Identifying sensitive organizational information off-premises via email, using designated forms, such as identification number, credit cards, etc.

Flexible Reporting

Producing recurrent system reports and adaptable editing.

Connected Threat Defense

Interfacing with the central managing system of Apex Central to identify the events in one central location.