Cyber Security – A Case study of Comodo Security Solutions

Anu Varghese[1], Jagadeesha S.N[2]

[1]Research Scholar, College of Computer Science & Information Science, Srinivas University, Mangalore, India.

[1]Assistant Professor, Department of Computer Science, MES M K Mackar Pillay College for Advanced Studies, Aluva, Mahatma Gandhi University, Aluva, Kerala, India.

[2]Research Professor, College of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India.

ABSTRACT

Background/Purpose:

Humans are currently heavily reliant on digital infrastructure and can easily access practically all services. All of these technological advancements have an impact on people, both positively and badly. As risks change in nature, it becomes much more difficult to overcome them. In the digital age, security is crucial. Many firms have serious cybersecurity concerns. We should practice excellent cyber hygiene, double-check our sources, and keep up with official changes if we want to maintain cybersecurity. Xcitium (previously Comodo Security), a cybersecurity-focused organization, runs many tests to improve detection rates. This business specializes in online and computer security.

Objective: Design/Methodology/Approach: *This paper discusses the technological improvement of Comodo Security products*

Findings/Results: This company undergoes much research to improve threat detection and thereby it finds its role in the cybersecurity world. They work in the principle that every single digital transaction must have a layer of trust and security.

Originality/Value: *Journals, annual reports, academic articles, websites, and the internet were some of the secondary sources used in this study to acquire data.*

Paper Type: Company Analysis

Keywords: cyber security, malware, cyber hygiene, comodo solutions

1. INTRODUCTION:

In recent years attackers delivered a wave of threats. Almost all companies involved in cybersecurity have the highest detection rate. According to the reports, Cisco Umbrella received a high detection rate of 96.39% in the industry [1]. As cybercriminals are increasingly using a wide range of techniques, technical and social, to evade the security system. Smishing is used to attack the mobile user. By this, the criminals steal personal information and spread malicious software. For example, a message to pay a bill and thereby steals the financial information. Many cases of smishing reported worldwide and it continues. Many attacks are done through games. Malware is attached what the mobile game app and thereby steals the social media and gaming credentials. Crypto mining is another way of malware attack. Fake messaging apps are also a way off malware attacks. They trick users too premium subscriptions by promising additional features [3].

To avoid malware to an extent we must:

- download apps from the reliable App Store
- Carefully read the request for settings and permissions.
- Update software frequently
- Read carefully the reviews and compare the five-star reviews and one-star reviews 4 get information about the app's real capabilities.
- Use security software.
- Pay attention when our phones or devices behave unusually

Comodo security solutions Now known as XCITIUM founded in 1998 in the United Kingdom. The headquarters is at Clifton, New Jersey, United States. It belongs to the software industry and the different services are offered worldwide. It focuses on computer and internet security. The founder is Melih Abdulhayoglu[2].It is now focused in the area of cybersecurity this company provides many certifications and also offers various products. The various products are Comodo Dragon, Comodo Ice Dragon, Comodo Internet Security, Comodo System Utilities, Comodo Mobile Security, and Comodo Endpoint Protection.

- ***Comodo Dragon*** is a freeware web browser.
- ***Comodo ice dragon*** is a Firefox-based open-source web browser developed for Microsoft Windows.
- ***Comodo Internet Security*** is a free Internet security suite that provides an antivirus program personal firewall sandbox host-based intrusion prevention system and website filtering.
- ***Comodo system utilities*** is a software suite for Internet and network security. It includes cleaning utilities like windows registry cleaner disk cleaner privacy cleaner and saves delete.
- ***Comodo mobile security*** is a mobile application to protect Android devices.

Their focus is on endpoint protection, certificate management, and IT management. Many major clients /partners have entrusted the security provided by them and the number increased. They have won many recognitions like best-managed security, cyber security excellence awards, etc. It offers services like forensic analysis, website malware removal, etc.

The companies under Comodo Cloud Solutions are:

1. Comodo CA Ltd:- Rebranded as Sectigo. It is a digital certificate authority that issues SSL and other digital certificates. It is based in the UK
2. Comodo Security Solutions, Inc: -develops security software for commercial and consumer use. It is based in Clifton.
3. DNS.com: -It provides managed DNS services. It is based in the US.

2. RELATED WORKS:

There are many works done in association with the research group of comodo/using the dataset from them. The following are some of the journals /articles that describe their work using the dataset of comodo during the period 2015-2022:

Table1: Scholarly articles related to Comodo Cloud Security

Sl. No.	Title of Study	Emphasis	Reference
1.	DeepAM: a heterogeneous deep learning framework for intelligent malware detection	A heterogeneous deep learning framework composed of an AutoEncoder stacked up with multilayer restricted Boltzmann machines and a layer of associative memory to detect newly unknown malware.	Ye et al., 2017 [5]
2.	HinDroid: An Intelligent Android Malware Detection System Based on a Structured Heterogeneous Information Network	Analyses the relationships between API calls by constructing HIN	Hou et al., 2017 [6]
3.	DroidDelver: An Android Malware Detection System Using Deep Belief Network Based on API Call Blocks	a comprehensive experimental study is performed to compare various malware detection approaches.	Hou et al., 2016 [7]
4.	SecureDroid: Enhancing Security of Machine Learning-based Detection against Adversarial Android Malware Attacks	an ensemble learning approach (named SecENS) by aggregating the individual classifiers that are constructed using our proposed feature selection method SecCLS	Chen et al., 2017 [8]
5.	DroidEye: Fortifying Security of Learning-Based Classifier Against Adversarial Android Malware Attacks	count featurization to transform the binary feature space into continuous probabilities encoding the distribution in each class	Chen et al., 2018 [9]
6.	Deep Neural Networks for Automatic Android Malware Detection	categorize the extracted API calls which belong to some method in the smali code into a block. Based on the generated API call blocks, explore deep neural networks (i.e., Deep Belief Network (DBN) and Stacked Autoencoders (SAEs)) for newly unknown Android malware detection.	Deep Neural Networks for Automatic Android Malware Detection, n.d [10]
7.	A Comprehensive Study of DNS Operational Issues by Mining DNS Forums	assess DNS operational failures from another data source, the	Liao et al., 2022 [11]

		supporting forums built by DNS service providers.	
8.	Artificial Intelligence for Cybersecurity: Recent Advancements, Challenges, and Opportunities	Focuses on the use of AI in cyber-security, its application, various challenges, and opportunities	Zhang et al., 2021 [12]
9.	Toward accurate and intelligent detection of malware	explores the transition of malware detection from traditional to AI-based techniques.	Afreen et al.,2021[13]
10.	A Systematic Evaluation of Android Anti-Malware Tools for Detection of Contemporary Malware	classifies anti-malware tools, according to their analysis methodology along with their protection capabilities, performance, accuracy rate, usability, and ability to classify malware families	Muhammad et al.,2021[14]

3. OBJECTIVES:

- To understand the organization's history
- To discuss the various products and services offered by the company
- To discuss the role of Comodo cloud security in the research field

4. RESEARCH AGENDA:

- To recognize the importance of Comodo in the world of cybersecurity
- To compare with the company's main competitors.

5. METHODOLOGY:

Data was collected from secondary sources like the company website, annual reports, the internet, various journals from google scholar, research gate, etc.

6. INDUSTRY PERFORMANCE ANALYSIS:

Comodo Cloud Security is a software company in the starting and now become a leader in the world of cybersecurity. It is the company that offers cloud-based cybersecurity services, and a DNS resolver is included, which performs security-based filtering on the DNS requests and responses [11]. They are a part of much research in cybersecurity. Many studies are undergoing continuously to find out the flaws and improve security by rectifying the drawbacks. Table 2 & Table 3 shows a detailed comparison between Comodo and its competitors.

Table 2: Comparison between Comodo & the main Competitors

	Comodo Dragon Enterprise	**Fsecure**	**Esetprotect**	**Virsec**	**Trendmicro apex one**	**Symantec**	**Sophos Intercept x advanced with EDR & MTR**
EPP Capabilities							
Signature-based anti-malware protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Machine learning/algorithmic file analysis on the endpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Machine learning for process activity analysis	Yes	Yes	Yes	Yes	No	No	Yes
Process isolation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Memory protection and exploit prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protection against undetected malware	Yes	No	No	Yes	No	No	No
Application whitelisting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local endpoint sandboxing/endpoint emulation	Yes	No	No	Yes	No	No	No
Script, pE, or fileless malware protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integration with on-premises network/cloud sandbox	Yes	Yes	Yes	Yes	Yes	Yes	Require additional products
Real-time IoC search capabilities	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Retention period for full access to data	No Limit	1 Month	1 month	-	1 month	1 month	1 month
Endpoint firewall	Yes	Yes	Requires additional products	Yes	Yes	Yes	Yes
FW learning mode	Yes	No	Requires Addition	No	No	No	No

			al Products				
Automatically creates network traffic rules	Yes	No	Requires Additional Products	No	No	No	No
URL filtering	Yes	Yes	Requires Additional Products	No	Yes	Yes	Yes
Host-based IPS	Yes	Yes	Requires Additional Products	No	Yes	Yes	Yes
USB device control	Yes	Yes	Yes	No	Yes	Yes	Yes
Full device control(Device Control based on device class product ID, vendor ID, and device name)	Yes	No	Yes	No	Yes	Yes	Yes
Agent self-protection/remediation or alerting when there is an attempt to disable, bypass or uninstall it	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ransomware protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protect / block ransomware when “Offline” or Disconnected” from the internet?	Yes	No	No	Yes	Yes	No	No
VDI support	Yes	Yes	Yes	No	Yes	Yes	Yes
Manage, and maintain, an application control database of known "trusted" applications.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-tenant cloud-based service	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EPP management console available as an on-premises virtual or	Yes	Yes	Yes	Yes	Yes	Yes	No

physical server /application							
Consolidated EPP management console to report on, manage, and alert for windows macOS clients and mobile	Yes	Yes	Yes	No	Yes	Yes	Yes
Data loss prevention	Yes	No	Requires Additional Products	No	Yes	Requires Additional Products	Yes
Mobile device management	Yes	Requires Additional Products	Yes	No	No	Requires Additional Products	Requires Additional Products
Mobile threat defense	Yes	Require Additional Products	Yes	No	No	Requires Additional Products	Requires Additional Products
Vulnerability and patch management	Yes	Yes	Requires Additional Products	No	Yes	Requires Additional Products	Requires Additional Products
Network/sandboxing	Cloud Sandbox	Cloud Sandbox	Requires Additional Products	No	Cloud Sandbox	No	Requires Additional Products
Security orchestration, Analysis, and response (SOAR) Integration	Yes	No	Yes	No	Yes	Yes	YES
Network discovery tool	Yes	No	Yes	No	Requires Additional Products	No	No

Remote Access	Yes	No	No	No	No	Require Additional Products	No
Remote scripting capabilities	Yes	No	Yes	No	Yes	Require Additional Products	No
Default deny security with default allow usability(Containment)							
Run unknown files with auto-containment protection	Yes	No	No	No	No	No	No
Create a virtual environment for any unknowns	Yes	No	No	No	No	No	No
Virtualize file system, registry, and COM on real endpoints	Yes	No	No	No	No	No	No
Telemetry (EDR observables)							
Interprocess memory access	Yes	Yes	Yes	No	Yes	Yes	Yes
Windows/win event hook	Yes	Yes	Yes	No	Yes	Yes	Yes
Device driver installations	Yes	Yes	Yes	No	Yes	Yes	Yes
File Access/modification/deletion)	Yes	Yes	Yes	No	Yes	Yes	Yes
Registry access/modification/deletion	Yes	Yes	Yes	No	Yes	Yes	Yes
Network connection	Yes	Yes	Yes	No	Yes	Yes	Yes
URL Monitoring	Yes	Yes	Yes	No	Yes	Yes	Yes
DNS Monitoring	Yes	Yes	Yes	No	Yes	Yes	Yes
Process creation	Yes	Yes	Yes	No	Yes	Yes	Yes
Thread creation	Yes	Yes	Yes	No	Yes	Yes	Yes
Inter-process communication(named pipes, etc)upto this	Yes	Yes	Yes	No	Yes	Yes	Yes

Telemetry data itself can be extended in real-time	Yes	No	No	No	No	No	No
Event chaining and enrichment on the endpoints	Yes	No	No	No	No	No	No
Detection/Hunting/Reporting							
Adaptive Event modeling	Yes	No	Yes	No	No	No	No
Behavioural analysis(analysis over active memory, OS activity, user behaviour, process/application behaviour, etc)	Yes	Yes	Yes	No	Yes	No	Yes
Static analysis of files using capabilities such as machine learning (not including signature-based malware detection)	Yes	Yes	Yes	No	Yes	Yes	Yes
Time-series analysis	Yes	No	No	No	No	No	Yes
Integration with automated malware analysis solutions(sandboxing)	Yes	Yes	Yes	No	No	No	No
Threat hunting interface or API for searching with YARA/REGEX/ElasticSearch/IOC	YES without YARA	No	IOC & regex YARA Requires additional products	No	IOC & Regex only	IOC & Regex only	IOC & Regex only
Support for matching against private IOC	YES	No	No	No	Yes	Yes	Yes
Threat intelligence integration(TIP, upload, web service connector, etc)to enrich and contextualize alerts	YES	YES	Yes	No	Yes	Yes	Yes
Linking telemetry(observable data) to recreate a	YES	YES	Requires additional products	No	Yes	Yes	Yes

sequence of events to aid the investigation							
Process /attack Visualization	YES	YES	Yes	No	Yes	Yes	Yes
Incident response Platform(IRP) or orchestration integration?	YES	YES	Yes	No	Yes	Yes	Yes
Vulnerability reporting(ex. reporting on unpatched CVEs)	YES	YES	Requires addition al products	No	Yes	Yes	Yes
Alert prioritization based on confidence, able to define thresholds for alerting	YES	YES	Yes	No	Yes	Yes	Yes
Alert prioritization factors system criticality	YES	YES	Yes	No	Yes	Yes	Yes
Able to monitor risk exposure across the environment organized by local asset groups	YES	YES	Yes	No	Yes	Yes	Yes
Reporting interface identifies frequent alerts that may be appropriate for automating response	YES	YES	Yes	No	Yes	Yes	Yes
Response							
Remote scripting capabilities	YES	No	Yes	No	No	No	No
Quarantine and removal of files	YES	YES	Yes	Yes	Yes	Yes	Yes
Kill processes remotely	YES	YES	Yes	Yes	Yes	Yes	Yes
File retrieval	YES	YES	Yes	Yes	Yes	Yes	Yes
Network isolation	YES	YES	Yes	Yes	Yes	Yes	Yes
File system snapshotting	YES	YES	Requires addition al products	Yes	Yes	Yes	Yes
Memory snapshotting	YES	YES	Requires addition al products	Yes	Yes	Yes	Yes

Managed endpoints (MDR)							
Manage customer endpoints and policies	YES	YES	Yes	No	Yes	No	No
Incident investigation & response	YES	YES	Yes	No	Yes	No	Yes
Preemptive containment	YES	No	No	No	No	No	No
Application profiling(AI support)	YES	YES	Yes	No	No	No	Yes
Customizable policy creation	YES	No	Yes	No	Yes	No	No
Central monitoring of all endpoints	YES	YES	Yes	No	Yes	No	Yes
Live remote inspection	YES	No	No	No	Yes	No	Yes
Tuning of monitoring rules for reduction of false positives	YES	YES	Yes	No	Yes	No	No
Forensic analysis	YES	YES	Requires additional products	No	yes	No	Yes
MANAGED network(XDR)							
Cloud-based SIEM and big data analytics	YES	Requires additional products	Requires additional products	No	Yes	No	No
Log data collection /correlation	YES	Requires additional products	Requires additional products	No	Yes	No	No
Threat intelligence integration	YES	Requires additional products	Requires additional products	No	Yes	No	No

Network profiling(AI support	YES	Requires additional products	Requires additional products	No	No	No	No
Available as virtual or physical	YES	Requires additional products	Requires additional products	No	Yes	No	No
Integrated file analysis(cloud sandbox)	YES	Requires additional products	Requires additional products	No	Yes	No	No
Full packet capture	YES	Requires additional products	Requires additional products	No	No	No	No
Protocol analyzers for 40+ different protocols such as TCP, UDP,DNS<DHCP<HTTP , etc w/full decoding capability	YES	Requires additional products	Requires additional products	No	Yes	No	No
MANAGED CLOUD							
Includes ready-to-use cloud application connectors for :							
AZURE	YES	No	Requires additional products	No	Yes	Yes	Requires additional products
Google cloud platform	YES	No	No	No	Yes	Yes	Requires additio

							nal products
Office 365	YES	Requires additional products	Requires additional products	No	Yes	Yes	Requires additional products
AWS	YES	No	No	No	Yes	Yes	Requires additional products
Threat detections for cloud applications	YES	No	No	No	Yes	No	No
Log collection from cloud environments	YES	No	No	No	Yes	No	Requires additional products
Generating actionable incident response from cloud application	YES	No	Requires additional products	No	Yes	No	No
THREAT INTELLIGENCE AND VERDICT							
InHolistic security approach combined network, endpoint, cloud	YES	No	No	No	Yes	No	No
Internal security sensor logs(IOCs)	YES	Yes	Yes	No	Yes	Yes	Yes
Expert Human Analysis	YES	No	Requires additional products	No	No	No	No
ML & behavioral analysis and verdict	YES	Yes	Yes	No	Yes	Yes	Yes
Open-source threat intelligence feeds	YES	No	No	No	Yes	No	Yes

Information sharing with the industry	YES	Yes	Yes	No	Yes	Yes	Yes
Clean web(phishing sites,keyloggers,spam)	YES	Yes	Yes	No	Yes	Yes	Yes
Deep web(C&C servers,TOR browsers,database platform archives—paste bins)	YES	No	Yes	No	No	Yes	Yes
Cyber adversary characterization	YES	No	Yes	No	Yes	No	No
SECURITY OPERATIONS CENTER(SOC)							
Global,real-time support(24/7/365)	YES	Yes	Yes	No	Yes	Yes	Yes
Dedicated cybersecurity expert	YES	No	No	No	Yes	No	Yes
Breach(case)management	YES	No	No	No	Yes	No	Yes
Security monitoring	YES	Yes	Yes	No	Yes	No	Yes
Incident analysis	YES	Yes	Yes	No	Yes	No	Yes
Incident response(handling)	YES	Yes	Yes	No	Yes	No	Yes
Extensive threat hunting(scenario-based)	YES	Yes	Yes	No	Yes	No	Yes

Table 3: Comparison between Comodo & the main Competitors

	Sophos endpoint protection	**Mcafee Mvision EDR, MDR & EPO**	**Kaspersky**	**Cylance**	**CrowdStrike**	**Checkpoint**	**BitDefender**
EPP Capabilities							
Signature-based anti-malware protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Machine learning/algorithmic file analysis on the endpoint	Yes	Yes	Yes	Yes	No	Yes	Yes

Machine learning for process activity analysis	No	No	Yes	Yes	Yes	No	Yes
Process isolation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Memory protection and exploit prevention	No	Yes	Yes	Yes	Yes	Yes	Yes
Protection against undetected malware	No	No	No	No	No	No	No
Application whitelisting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local endpoint sandboxing/endpoint emulation	No	No	No	No	No	No	No
Script, pE, or fileless malware protection	No	Yes	Yes	Yes	Yes	Yes	Yes
Integration with on-premises network/cloud sandbox	No	Yes	Requires additional products	No	No	Yes	Yes
Real-time IoC search capabilities	No	Yes	Yes	Yes	Yes	Yes	Yes
Retention period for full access to data	1 month	1 month	1 month	1 month	1 month	1 month	1 month
Endpoint firewall	Yes	Yes	Yes	No	Yes	Yes	Yes
FW learning mode	No	No	No	No	No	Yes	Yes
Automatically creates network traffic rules	No	No	No	No	No	No	No
URL filtering	Yes	Yes	Yes	For Malicious Domain Only	No	Yes	Yes
Host-based IPS	Yes	Yes	Yes	Yes	No	Yes	Yes
USB device control	Yes	Yes	Yes	Requires Aditional Products	Yes	Yes	Yes
Full device control(Device Control based on device class	Yes	Yes	Yes	Requires Aditional Products	No	Yes	Yes

product ID, vendor ID, and device name)							
Agent self-protection/remediation or alerting when there is an attempt to disable, bypass or uninstall it	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ransomware protection	No	Yes	Yes	Yes	Yes	Yes	Yes
Protect / block ransomware when “Offline” or Disconnected” from the internet?	No	No	No	No	No	Yes	No
VDI support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Manage, and maintain, an application control database of known "trusted" applications.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-tenant cloud-based service	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EPP management console available as an on-premises virtual or physical server /application	Yes	Yes	Yes	No	No	Yes	No
Consolidated EPP management console to report on, manage, and alert for windows macOS clients and mobile	Yes	Yes	Yes	Yes	No	Yes	Yes
Data loss prevention	No	Requires Additional Products	Requires Additional Products	Requires Additional Products	No	Requires Aditional Products	Require Additional Products
Mobile device management	No	Requires Additional	Requires Additional	Requires Additional Products	No	Requires Aditional Products	Require Additional Products

		Products	Products				
Mobile threat defense	No	Requires Additional Products	Requires Additional Products	Requires Additional Products	No	Requires Aditional Products	Require Additional Products
Vulnerability and patch management	No	Requires Additional Products	Yes	Vulnerability Management Only	Vulnerability Management Only	Requires Aditional Products	YES
Network/sandboxing	No	No	Cloud Sandbox	No	No	Network/ Cloud Sandbox	Cloud Sandbox
Security orchestration, Analysis, and response (SOAR) Integration	No	YES	YES	YES	YES	YES	YES
Network discovery tool	No	No	YES	No	No	No	N (Unmanaged Computers Only)
Remote Access	No	Requires Additional Products	No	Requires Additional Products	No	Yes	Require Additional Products
Remote scripting capabilities	No	Requires Additional Products	No	Requires Additional Products	No	YES	Require Additional Products
Default deny security with default allow usability(Containment)							

Run unknown files with auto-containment protection	No	No	No	No	No	No	No
Create a virtual environment for any unknowns	No	No	No	No	No	No	No
Virtualize file system, registry, and COM on real endpoints	No	No	No	No	No	No	No
Telemetry (EDR observables)							
Interprocess memory access	No	No	Yes	Yes	Yes	No	Yes
Windows/win event hook	No	Yes	Yes	Yes	Yes	Yes	Yes
Device driver installations	No	Yes	Yes	Yes	Yes	Yes	Yes
File Access/modification/deletion)	No	Yes	Yes	Yes	Yes	Yes	Yes
Registry access/modification/deletion	No	Yes	Yes	Yes	Yes	Yes	Yes
Network connection	No	Yes	Yes	Yes	Yes	Yes	Yes
URL Monitoring	No	Yes	Yes	Yes	Yes	Yes	Yes
DNS Monitoring	No	Yes	Yes	Yes	Yes	Yes	Yes
Process creation	No	Yes	Yes	Yes	Yes	Yes	Yes
Thread creation	No	Yes	Yes	Yes	Yes	Yes	Yes
Inter-process communication(named pipes, etc)upto this	No	Yes	Yes	Yes	Yes	Yes	Yes
Telemetry data itself can be extended in real-time	No	No	No	No	No	No	No
Event chaining and enrichment on the endpoints	No	No	No	No	No	No	No
Detection/Hunting/Reporting							
Adaptive Event modeling	No	No	No	No	No	No	No

Behavioural analysis(analysis over active memory, OS activity, user behaviour, process/application behaviour, etc)	No	No	Yes	Yes	Yes	Yes	Yes
Static analysis of files using capabilities such as machine learning (not including signature-based malware detection)	No	Yes	Yes	Yes	Yes	Yes	Yes
Time-series analysis	No	No	No	Yes	No	No	No
Integration with automated malware analysis solutions(sandboxing)	No	No	No	Yes	No	Yes	No
Threat hunting interface or API for searching with YARA/REGEX/Elastic Search/IOC	No	IOC & YARA	IOC & YARA	IOC & YARA	IOC & Regex only	IOC & Regex only	IOC & Regex only
Support for matching against private IOC	No	Yes	No	Yes	No	Yes	Yes
Threat intelligence integration(TIP, upload, web service connector, etc)to enrich and contextualize alerts	No	Yes	Yes	Yes	Yes	Yes	Yes
Linking telemetry(observable data) to recreate a sequence of events to aid the investigation	No	Yes	Yes	Yes	Yes	Yes	Yes
Process /attack Visualization	No	Yes	Yes	Yes	Yes	Yes	Yes
Incident response Platform(IRP) or orchestration integration?	No	Yes	Yes	Yes	Yes	Yes	Yes
Vulnerability reporting(ex. reporting on unpatched CVEs)	No	Yes	Yes	Yes	Yes	Yes	Yes

Alert prioritization based on confidence, able to define thresholds for alerting	No	Yes	Yes	Yes	Yes	Yes	Yes
Alert prioritization factors system criticality	No	Yes	Yes	Yes	Yes	Yes	Yes
Able to monitor risk exposure across the environment organized by local asset groups	No	Yes	Yes	Yes	Yes	Yes	Yes
Reporting interface identifies frequent alerts that may be appropriate for automating response	No	Yes	Yes	Yes	Yes	Yes	Yes
Response							
Remote scripting capabilities	No	No	No	Requires additional products	No	No	No
Quarantine and removal of files	No	Yes	Yes	Yes	Yes	Yes	Yes
Kill processes remotely	No	Yes	Yes	Yes	Yes	Yes	Yes
File retrieval	No	Yes	Yes	Yes	Yes	Yes	Yes
Network isolation	No	Yes	Yes	Yes	Yes	Yes	Yes
File system snapshotting	No	Yes	Yes	Yes	Yes	Yes	Yes
Memory snapshotting	No	Yes	Yes	Yes	Yes	Yes	Yes
Managed endpoints (MDR)							
Manage customer endpoints and policies	No	Only through partners	Yes	No	No	No (IR only)	Only through partners
Incident investigation & response	No	Only through partners	Yes	Yes	No	No (IR only)	Only through partners
Preemptive containment	No	No	No	No	No	No (IR only)	No

Application profiling(AI support)	No	No	Yes	Yes	Yes	No (IR only)	Yes
Customizable policy creation	No	No	Yes	No	No	No (IR only)	Yes
Central monitoring of all endpoints	No	Yes	Yes	Yes	No	No (IR only)	Yes
Live remote inspection	No	Only through partners	No	Yes	No	No (IR only)	Only through partners
Tuning of monitoring rules for reduction of false positives	No	Only through partners	No	No	No	No (IR only)	Only through partners
Forensic analysis	No	Only through partners	Requires additional products	No	No	No (IR only)	Only through partners
MANAGED network(XDR)							
Cloud-based SIEM and big data analytics	No	Requires additional products	Requires additional products	No	No	No	Yes
Log data collection /correlation	No	Requires additional products	Requires additional products	No	No	No	Yes
Threat intelligence integration	No	Requires additional products	Requires additional products	No	No	No	Yes

Network profiling(AI support	No	Requires additional products	Requires additional products	No	No	No	No
Available as virtual or physical	No	Requires additional products	Requires additional products	No	No	No	Yes
Integrated file analysis(cloud sandbox)	No	Requires additional products	Requires additional products	No	No	No	Yes
Full packet capture	No	Requires additional products	Requires additional products	No	No	No	No
Protocol analyzers for 40+ different protocols such as TCP, UDP,DNS<DHCP<HTTP, etc w/full decoding capability	No	Requires additional products	Requires additional products	No	No	No	Yes
MANAGED CLOUD							
Includes ready-to-use cloud application connectors for :							
AZURE	No	Yes	Requires additional products	No	Yes	Require additional products	Yes

Google cloud platform	No	Yes	Requires additional products	No	No	Require additional products	No
Office 365	No	Yes	Requires additional products	No	No	Require additional products	Yes
AWS	No	Yes	Requires additional products	No	Yes	Require additional products	Yes
Threat detections for cloud applications	No	No	No	No	No	No	No
Log collection from cloud environments	No	No	Requires additional products	No	No	Require additional products	No
Generating actionable incident response from cloud application	No	No	No	No	No	No	No
THREAT INTELLIGENCE AND VERDICT							
InHolistic security approach combined network, endpoint, cloud	No	No	No	No	No	No	Yes
Internal security sensor logs(IOCs)	No	Yes	Yes	Yes	Yes	Yes	Yes
Expert Human Analysis	No	No	Requires additional	No	No	No	No

			products				
ML & behavioral analysis and verdict	No	Yes	Yes	Yes	Yes	Yes	Yes
Open-source threat intelligence feeds	No	No	Yes	Yes	No	Yes	No
Information sharing with the industry	No	Yes	Yes	Yes	Yes	Yes	Yes
Clean web(phishing sites,keyloggers,spam)	No	Yes	Yes	Yes	No	Yes	No
Deep web(C&C servers,TOR browsers,database platform archives—paste bins)	No	Yes	Yes	No	No	Yes	No
Cyber adversary characterization	No	No	Yes	Yes	Yes	No	Yes
SECURITY OPERATIONS CENTER(SOC)							
Global,real-time support(24/7/365)	No	Only through partners	Yes	Yes	Yes	No(IR only)	Only through partners
Dedicated cybersecurity expert	No	Only through partners	Yes	No	No	No (IR only)	Only through partners
Breach(case)management	No	Only through partners	Yes	No	No	No	Only through partners
Security monitoring	No	Only through partners	Yes	Yes	Yes	No	Only through partners
Incident analysis	No	Only through	Yes	Yes	No	No	Only through partners

		partners					
Incident response(handling)	No	Only through partners	Yes	Yes	No	No	Only through partners
Extensive threat hunting(scenario-based)	No	No	Yes	Yes	No	No	No

7. IMPACT OF COVID-19 PANDEMIC ON THE CYBERSECURITY INDUSTRY:

The pandemic year made the field of cybersecurity more difficult to navigate as a result of everyone being compelled to rely on the digital world. Everything, including paying bills, learning, and other services, went completely digital. Hackers and attackers were motivated to look for other ways to put a threat to the cyber world by this. In a recent international survey that was carried out by SailPoint Technologies Holdings, Inc., an information technology company based in the United States, 48 percent of American respondents stated that they had received phishing emails, phone calls, or texts over the course of the previous six months while working from home. In addition, ten percent of people who participated in the survey from Europe, the Middle East, and Africa (EMEA), in addition to persons from Australia and New Zealand (ANZ), stated that they discovered phishing attempts at least once every week [15].

According to a list published by Security Magazine, there will be six primary worries, threats, and areas of concentration for those working in the field of cyber security in the year 2021.

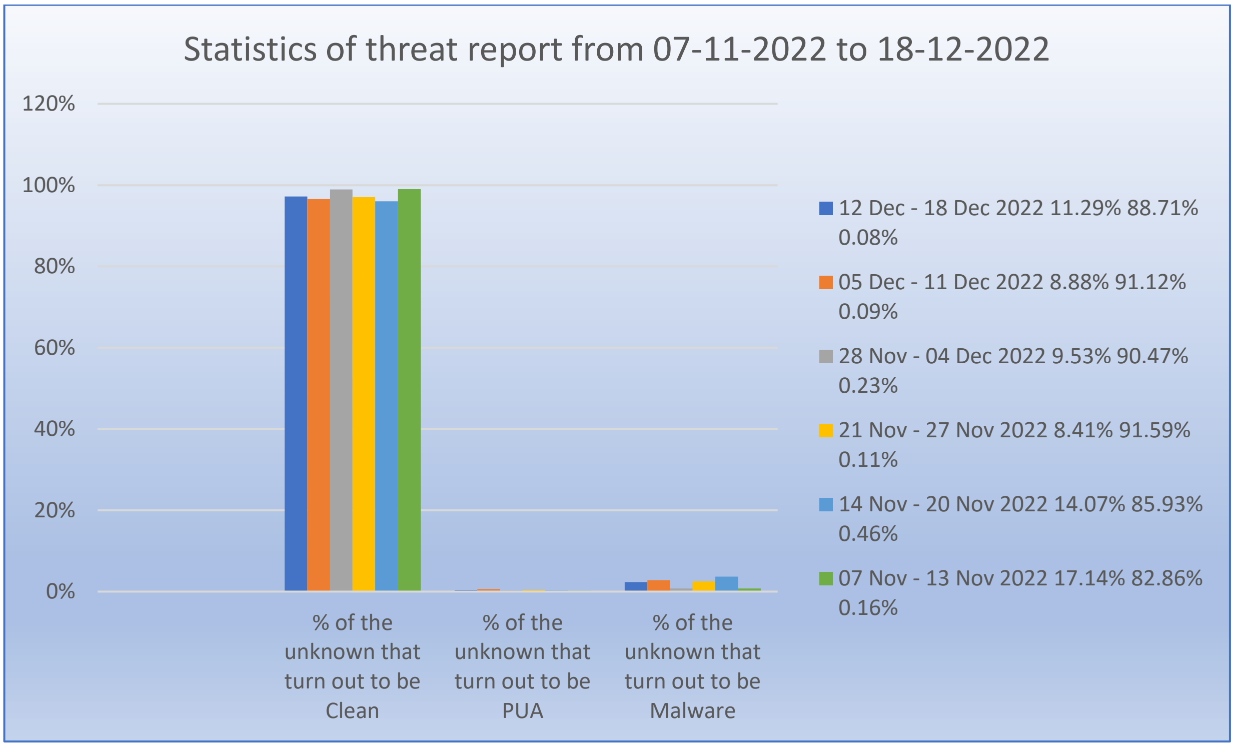
1. Cybercriminals often focus their attention on remote workers: As a direct result of the COVID-19 lockdowns, millions of employees throughout the world are now working from home. Since many employers were unprepared for the security hazards, one in four businesses has been forced to pay unanticipated costs associated with security breaches and malware. For instance, 82% of organizations allowed employees and other stakeholders to use their equipment, while 72% lacked effective protection against malware.
2. Organizations that rely on obsolete security architecture, such as virtual private networks (VPNs), are among those that have been singled out for attack. During the epidemic, many employees used VPN technology to continue working remotely even as their companies went into lockdown. They are putting themselves in danger since it is so simple for hackers to accomplish this.
3. As expenditures for security continue to be reduced, privacy experts will look to integrated security solutions: In 2019, it is anticipated that the decline in IT investment that occurred in 2020 would continue at around the same rate. The leaders of organizations will most likely turn to technologies such as secure access service edge to streamline their security management requirements and save money (SASE).
4. Concerns regarding security in the healthcare industry could lead to the loss of life. Hospitals are prime targets for hackers who recognize that now is the perfect time to hold them ransom by destroying their computer systems because they are being inundated with COVID-19 patients. This could result in fatalities. If a hospital does not have sufficient cyber security measures, it may be an easy target for hackers.

5. The number of data breaches in the financial industry is likely to increase. In 2019, financial companies were responsible for only 7% of data breaches, but they were responsible for 62% of the records that were compromised. The introduction of 5G technology in 2021 will give cybercriminals an advantage, which is why the financial services industry needs to investigate more powerful cybersecurity measures as soon as possible. An already well-underway move to remote work has been hastened by the COVID-19 epidemic.
6. The epidemic will hasten the adoption of cloud computing and artificial intelligence (AI) technology by businesses. In 2021, organizations will work to improve their ability to modify cybersecurity solutions in response to the ongoing transition.
7. More people will be affected by data theft as a direct result of increased internet usage and the rise in the number of jobs that may be done from home.

8. FINDINGS FROM THE ANALYSIS :

From the reported statistics by the company, the detection rate of malicious code has improved evidently. On the other side, the attackers are trying to evade systems with sophisticated tools. A race is going on in parallel between the attackers and defenders. The Comodo cloud solutions provide services like endpoint protection, IT management, etc. It became a leader in the cybersecurity world. It works hard to make the users work with the internet with trust and confidence in data protection. It participates in many research works to find out more ways to improve the detection rate and reduce data loss. The table shows the recent statistics of the company.

Table 2 shows the statistics of the threat report from 07-11-2022 to 18-12-2022



9. CONCLUSION:

The Comodo Cloud Security company is a leader in the cyber security world. The research department of the company works hard to face new challenges in the field of cyber security. They work to ensure that people trust the cyber world. It rectifies their drawbacks and improves the detection rate so that people can work in the digital world without the fear of data loss. It gives tough competition to other popular security providers like Kaspersky, Bitdefender, etc.

10. REFERENCES:

1. https://umbrella.cisco.com/info/av-test-rates-cisco-umbrella-best-in-threat-detection
2. https://en.wikipedia.org/wiki/Comodo_Cybersecurity
3. https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2022.pdf
4. https://en.wikipedia.org/wiki/Comodo_Dragon
5. Ye, Y., Chen, L., Hou, S., Hardy, W., & Li, X. (2017, May 9*). DeepAM: a heterogeneous deep learning framework for intelligent malware detection.* Knowledge and Information Systems, 54(2), 265–285. https://doi.org/10.1007/s10115-017-1058-9 Researchgate♂
6. Hou, S., Ye, Y., Song, Y., & Abdulhayoglu, M. (2017, August 13). *HinDroid*. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. https://doi.org/10.1145/3097983.3098026 GoogleScholar♂
7. Hou, S., Saas, A., Ye, Y., & Chen, L. (2016). *DroidDelver: An Android Malware Detection System Using Deep Belief Network Based on API Call Blocks*. Web-Age Information Management, 54–66. https://doi.org/10.1007/978-3-319-47121-1_5 Springer♂
8. Chen, L., Hou, S., & Ye, Y. (2017, December 4). *SecureDroid*. Proceedings of the 33rd Annual Computer Security Applications Conference. https://doi.org/10.1145/3134600.3134636 GoogleScholar♂
9. Chen, L., Hou, S., Ye, Y., & Xu, S. (2018, August). *Droideye: Fortifying security of learning-based classifier against adversarial android malware attacks*. In 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 782-789). IEEE. GoogleScholar♂
10. Hou, S., Saas, A., Chen, L., Ye, Y., & Bourlai, T. (2017, July). *Deep neural networks for automatic android malware detection*. In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017 (pp. 803-810). GoogleScholar♂
11. Liao, X., Xu, J., Zhang, Q., & Li, Z. (2022). *A Comprehensive Study of DNS Operational Issues by Mining DNS Forums*. IEEE Access, 10, 110807-110820. GoogleScholar♂
12. Rani, V., Kumar, M., Mittal, A., & Kumar, K. (2022). *Artificial Intelligence for Cybersecurity: Recent Advancements, Challenges, and Opportunities*. Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities, 73-88. springer♂
13. Arfeen, A., Khan, Z. A., Uddin, R., & Ahsan, U. (2022). *Toward accurate and intelligent detection of malware*. Concurrency and Computation: Practice and Experience, 34(4), e6652. Researchgate♂
14. Muhammad, Z., Amjad, M. F., Abbas, H., Iqbal, Z., Azhar, A., Yasin, A., & Iesar, H. (2021, October*). A Systematic Evaluation of Android Anti-Malware Tools for Detection of Contemporary Malware*. 2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC). https://doi.org/10.1109/euc53437.2021.00025 googlescholar♂
15. Hou, S., Saas, A., Chen, L., & Ye, Y. (2016, October). *Deep4MalDroid: A Deep Learning Framework for Android Malware Detection Based on Linux Kernel System Call Graphs*. 2016 IEEE/WIC/ACM International Conference on Web Intelligence Workshops (WIW). https://doi.org/10.1109/wiw.2016.040 Semantic Scholar♂

16. https://innovationatwork.ieee.org/how-the-covid-19-pandemic-is-impacting-cyber-security-worldwide/
17. https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/