eventus

TREND MICRO

SOCaaS

WEEKLY REPORT

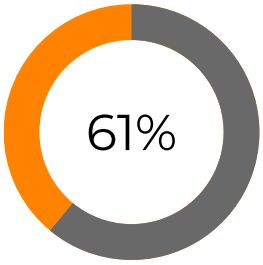
Client Name

09th October 2023 to
15th October 2023

TABLE OF CONTENTS

EXECUTIVE SUMMARY

- A total number of **106 attacks** were observed during the time frame of **09th October 202X** to **15th October 202X**.
- **Risk Index:**

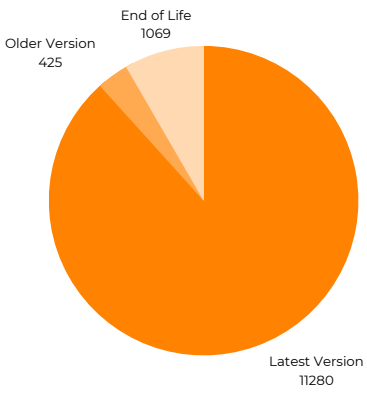


The Risk Index is a comprehensive score based on the dynamic assessment of risk factors inclusive of exposure, attack risk, and security configurations risk.

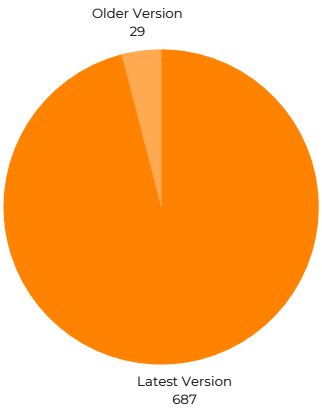
- **992 Highly exploitable unique CVEs** noted in all Endpoints.
- **01 Incident** Closed without customer resolution.
- **Top 05 Incidents:** Highest(47) Incidents triggered on **11th October 2023**.

Incident Names	Data Source from V1
Possible Spear Phishing Attack via Link	TM Email Sensor
Spear Phishing Email with Known Phishing Behaviors	TM Email Sensor
Suspicious Mailbox Rule Forwards All Email to an Untrusted External Location	Azure AD
Possible CVE-2021-44228 Apache Remote Code Execution Vulnerability	Trend C1 Workload Security
Unknown Threat Detection via Predictive Machine Learning	Trend C1 Workload Security

- **Agent Life Cycle**



Apex One



Workload Security

Please ensure that the most recent operating system version is installed on all endpoints and servers to address any open vulnerabilities and effectively detect real threats.

- **Top 05 Endpoint with Highest Observed Attack Technic Detection and Severity**

Endpoints Name	Number of Detection with Severity	Action Taken from SOC Team
XYZDTUN90479(192.168.2.126)	5139 Medium	The SOC team is actively developing and testing observed attack methods on the specified endpoint, while also prioritizing their efforts to respond to and communicate with the client.
ECHR0-PC1(172.30.116.171)	4598 Medium	
ESOFO-20013595(192.168.0.105)	4466 Medium	
XNAUSAMB2(192.168.23.139)	2132 Medium	
DTRIM2950(10.1.132.11)	1668 Medium	

- **Endpoint Protection: Apex One as Service** *(Need to deploy apex one on remaining endpoint to decrease attack surface and improve overall security)*

13490/14770 Agent Deployed

- **Endpoint Sensor: Trend V1 - XDR Endpoint Sensor** *(Kindly enable the endpoint sensor on remaining endpoints to increase the endpoint behavior visibility)*

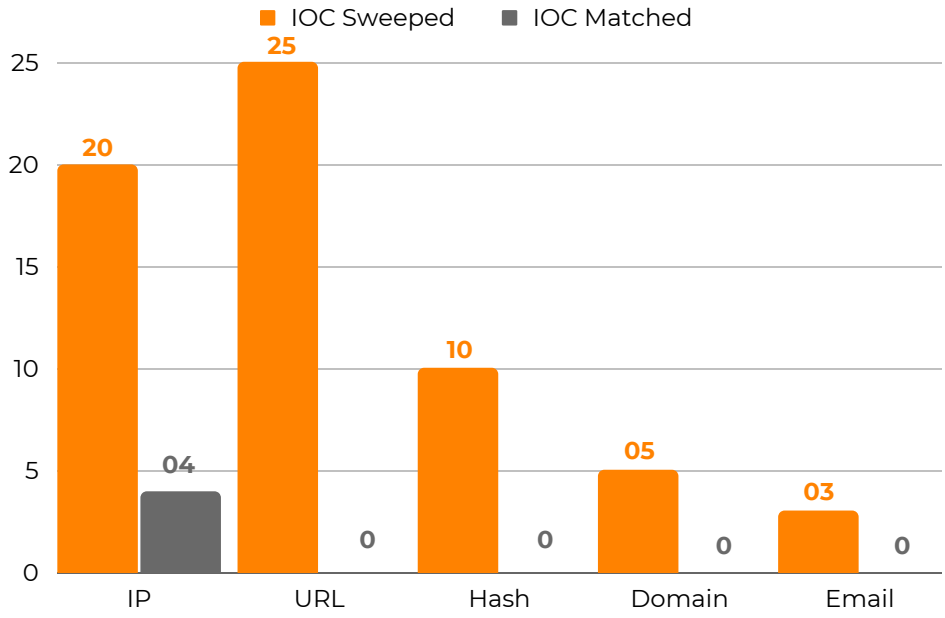
12010/14770 Sensor Enabled

THREAT INTEL SUMMARY

It refers to the process of collecting, analyzing, and disseminating information about potential and current cyber threats.

Sr. No	Advisory Name	Matched IOC Type	Matched IOC Details	No of Endpoints / Email
1.	Kinsing Malware	IP	152[.]89[.]198[.]113, 162[.]142[.]125[.]215, 167[.]248[.]133[.]36	03
2.	InfoStealer Campaign	IP	188[.]114[.]96[.]0	05

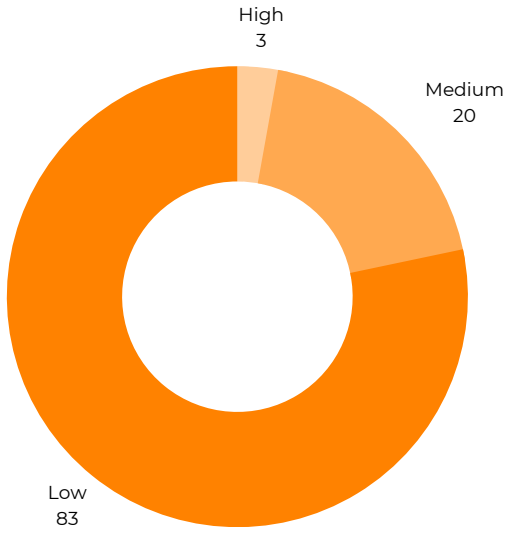
INDICATORS OF COMPROMISE (IOC) MATCH SUMMARY



Recommendation:

- During the Manual Sweeping of threat advisory Kinsing Malware and InfoStealer Campaign, we found matched IOCs in the form of IP.
- We recommend you to kindly block the matched IPs at your perimeter or gateway.

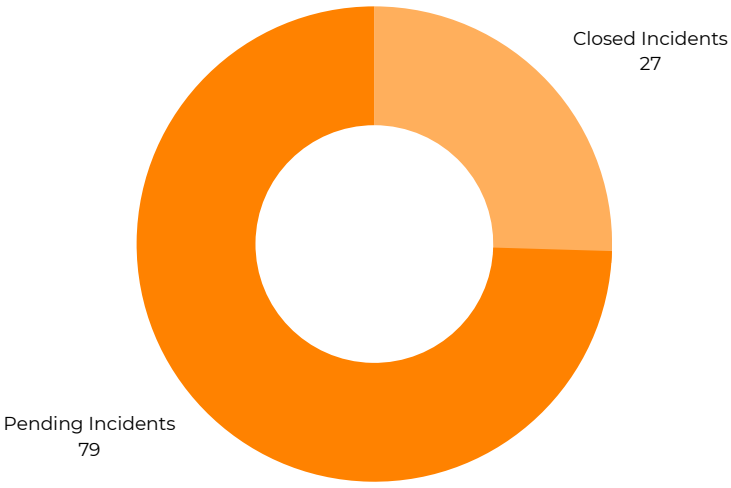
INCIDENT SUMMARY BY SEVERITY



RECOMMENDATION:

- An incident summary by severity is categorizes and describes cybersecurity incidents based on their level of impact and potential harm.
- Her 03 High Severity cases are there so we recommend you to take remediation steps to decrease it.

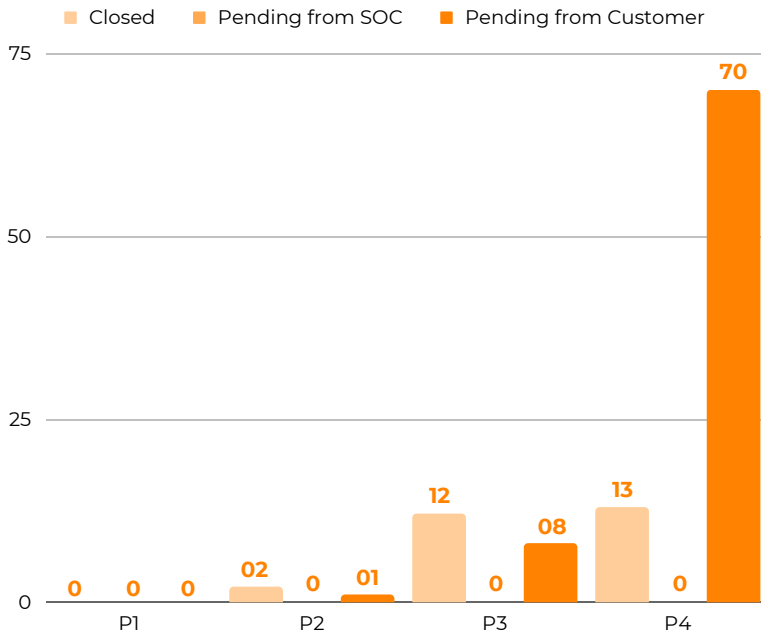
INCIDENT SUMMARY BY STATUS



RECOMMENDATION:

- An incident summary by status in cybersecurity provides an overview of the current state or stage of various security incidents within an organization.
- Kindly update the status for the 79 pending incidents.

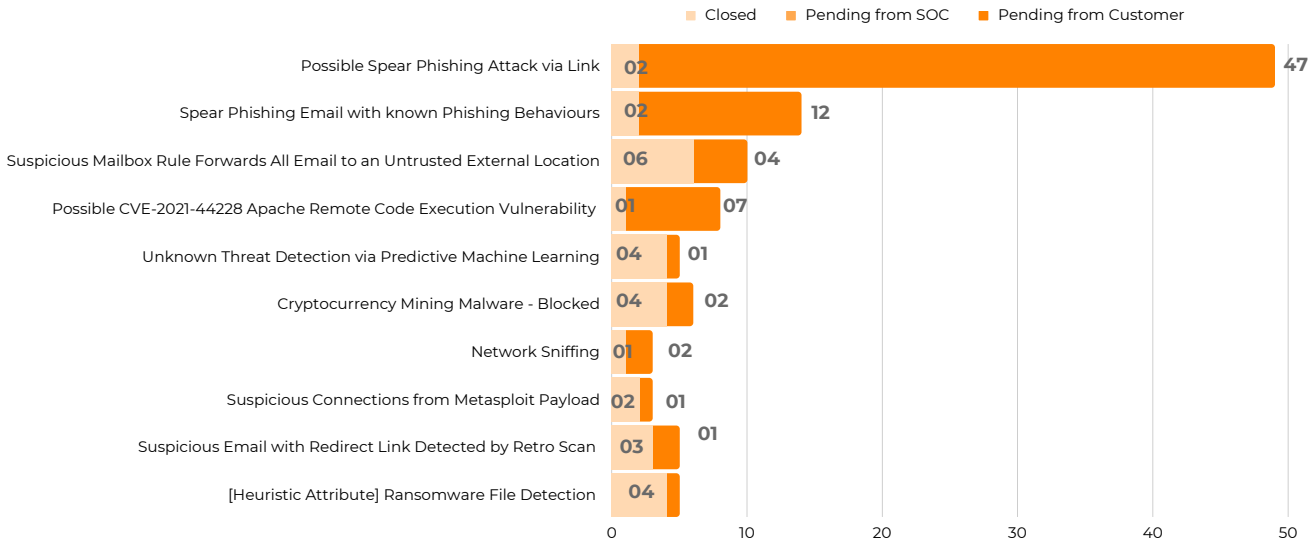
INCIDENTS SUMMARY BY PRIORITY



RECOMMENDATION:

- An incident summary by priority is used to classify and detail cybersecurity incidents according to their level of severity or priority.
- Here, Critical incident was not triggered.
- And out of 03 High Priority incidents, 02 incidents closed and remediated and 01 is remaining from TM Team

TOP 10 INCIDENTS SUMMARY BY CATEGORY

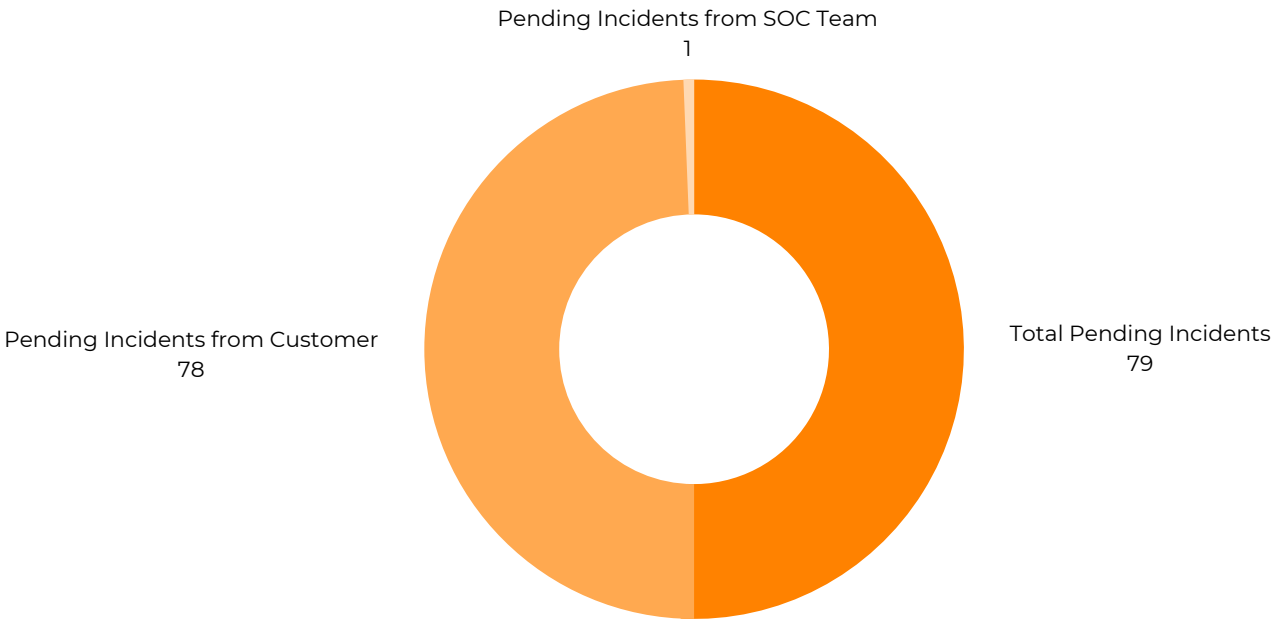


RECOMMENDATION:

- An incident summary by Category is used to classify and arrange cybersecurity incidents according to classifications.
- Kindly respond us on alert name Possible Spear Phishing Attack via Link and kindly don't click on any random link.

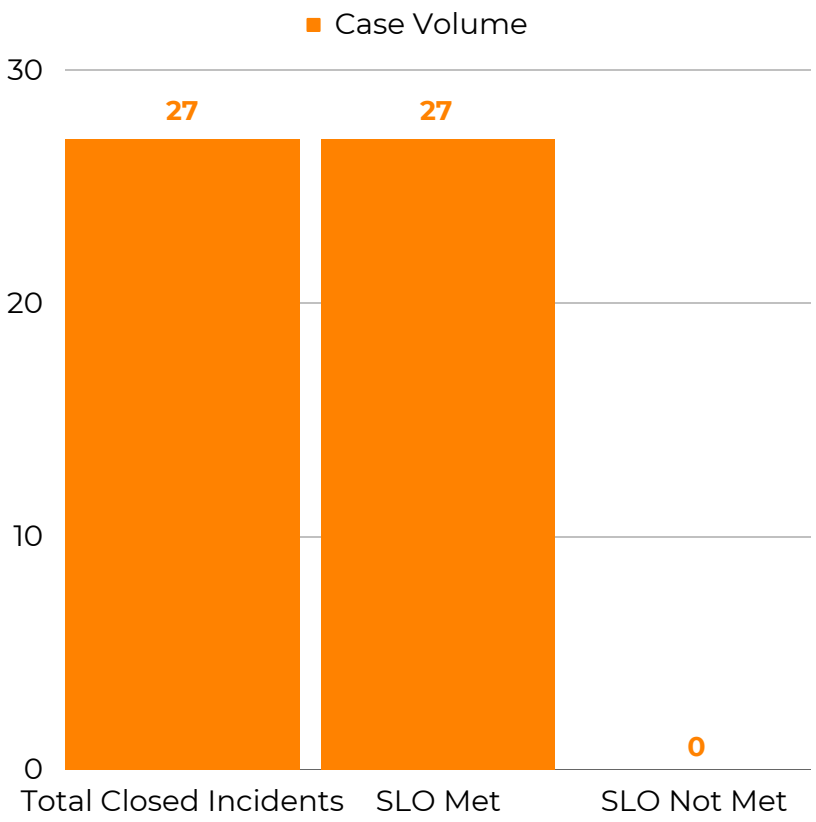
PENDING INCIDENTS SUMMARY

- **Total Pending Incidents: 79**
- **Pending Incidents from Customer: 78**
- **Pending Incidents from SOC Team: 01**



Note: Kindly Respond on the incidents pending from your side and for remaining one TM Team is working on it.

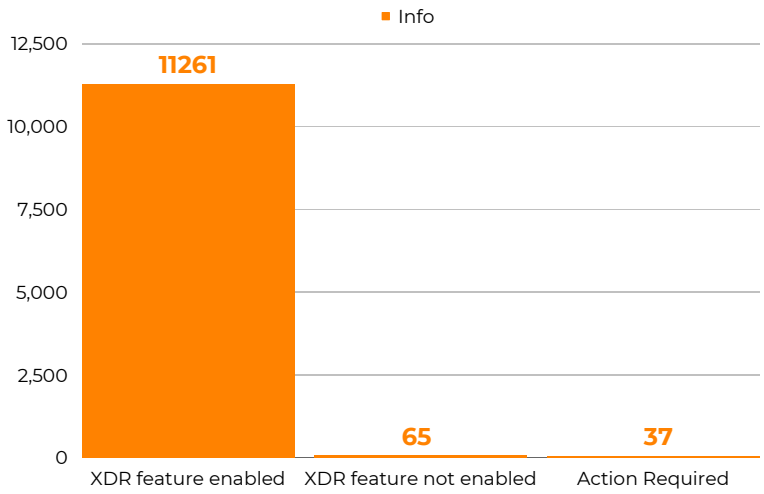
SLO SUMMARY



SLO DETAILS

Priority	Description	Response Time
1	Incidents that have a severe impact on customer operations. This event is a concern, such as attack formations or potential breaches	01 Hour
2	Incidents that have a significant impact, or the potential to have a severe impact, on operations.	04 Hours
3	Incidents that have a minimal impact with the potential for escalate if not contained causing significant impact on operations.	24 Hours
4	Incidents that do not have direct impact on Customer operations but violates Customer security Baseline.	48 Hours

ENDPOINT INVENTORY



Note: Kindly perform required action and enable XDR Sensor to decrease attack risk and secure the digital assets.

CONNECTED PRODUCTS AND LICENSE INFORMATION

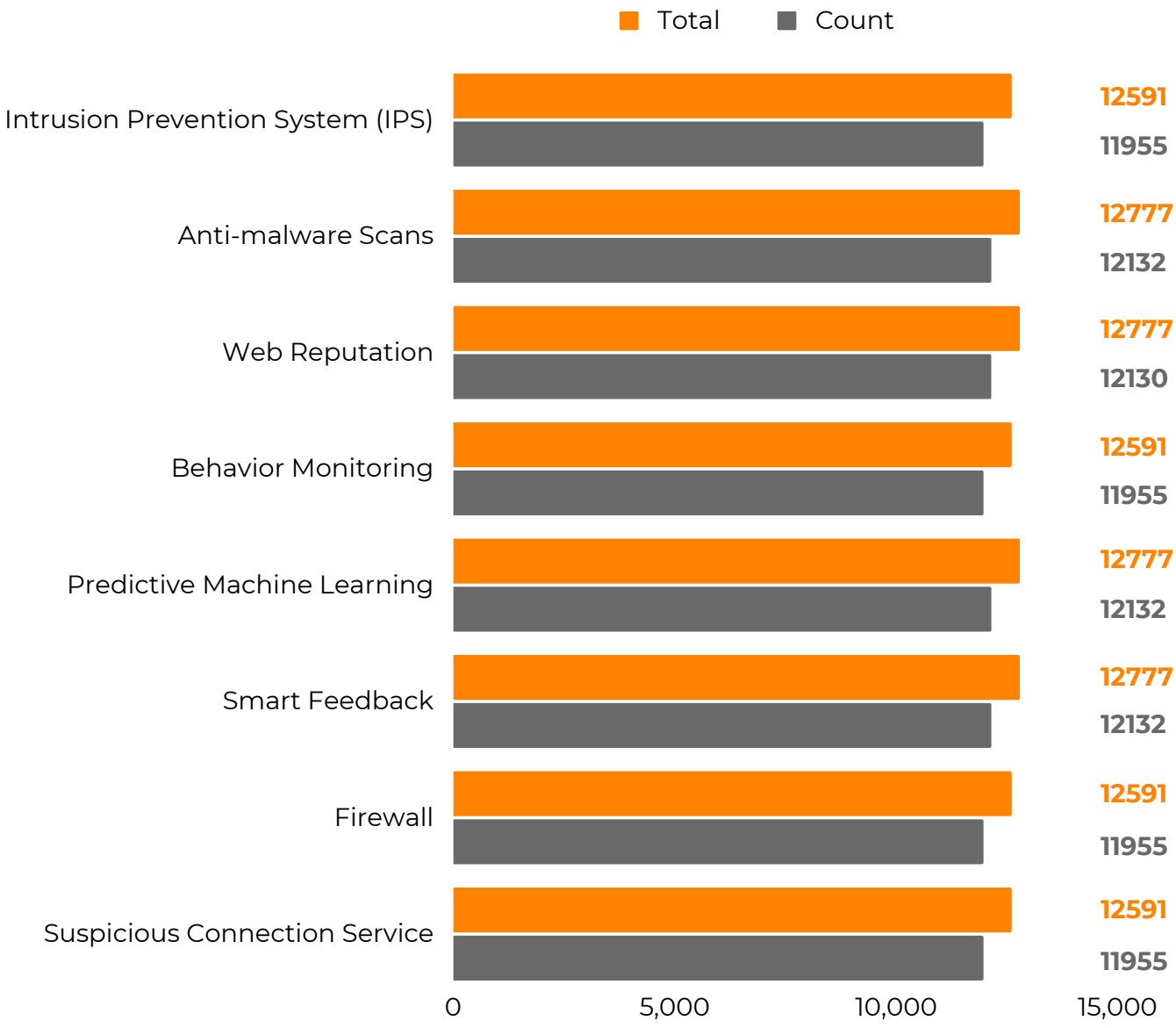
- **License Information:**

Status	Product
Normal	Trend Micro Cloud One – Workload Security
Normal	Trend Micro Apex One™ as a Service
Normal	Trend Vision One XDR Add-on: Cloud App Security

- **Products Connected:**

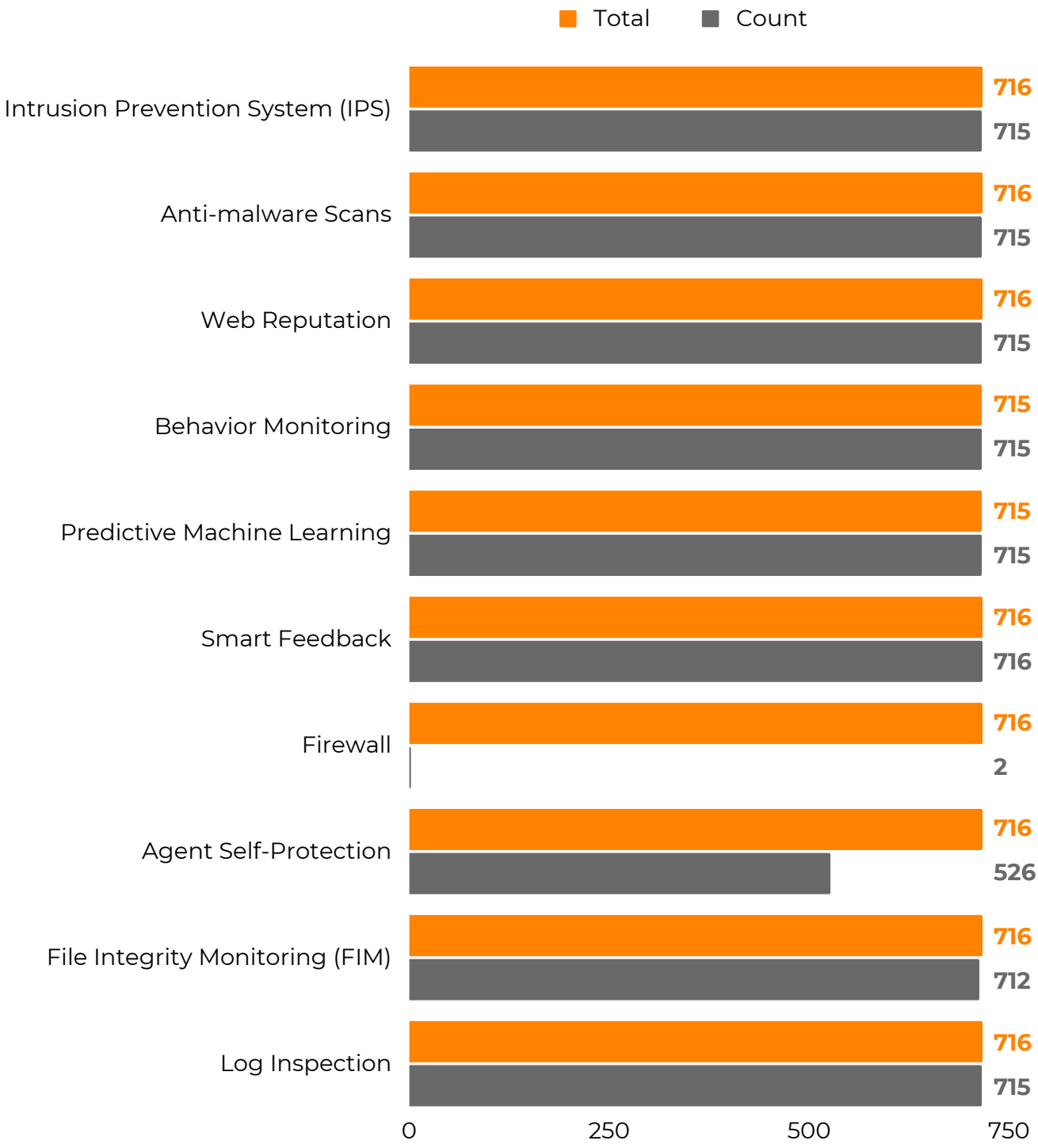
Status	Product
Connected	Trend Micro Apex One as a Service
Connected	Trend Micro Cloud App Security
Connected	Trend Micro Cloud One

KEY FEATURE ADOPTION RATE OF APEX ONE



Note: Kindly enable the remaining features in apex one to protect the endpoints in network infrastructure.

KEY FEATURE ADOPTION RATE OF CLOUD ONE WORKLOAD SECURITY



Note: Kindly enable the agent self protection features 190 servers from cloud one workload security to prevent the threat.