Sattrix®

SECURITY INTELLIGENCE ADVISORY

25th Sept 2022 - 24th Oct 2022

INTENT

This report is intended to help quantify the scope of that risk as organizations' struggle to balance their cyber security policies and protections against the needs of their employees for access to the Web and its resources.

BACKGROUND

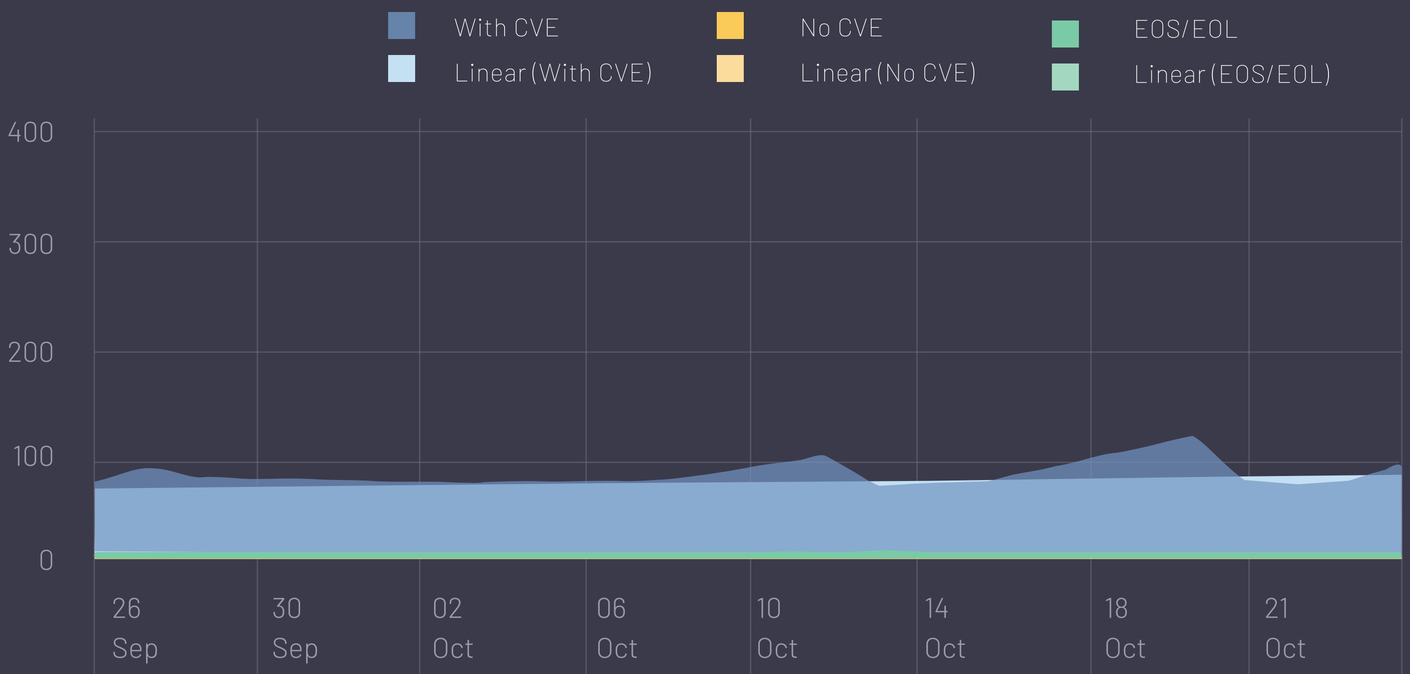
Every organization – large, medium and small has a huge risk and a typical challenge of managing vulnerabilities present in the operating systems, Vulnerabilities that are not attended possess a very high risk and can cost your organization various threats and damage. There is threat from users within the system, competitors who want to know accurate details about your business model etc. There is a certain way to identify and update patches for your vulnerabilities to avoid all these serious threats and curb the damage thereof. There's also a method in which specialists get into your system and run a check to identify how strong the system is. Performing vulnerability assessments guarantee all normal system vulnerabilities are taken into consideration. When assessments are conducted regularly, new threats are identified quickly.

WHAT DOES THE VULNERABILITY ADVISORY COVER?

- We monitor around 2000 applications, appliances and operating systems, and tests and verifies the vulnerabilities reported in them.
- We are focusing each vulnerability disclosed in those 2000 products.
- The systems and applications monitored by Sattrix Research Team are those in use in the environment of the customers.
- In the instance of customers using products that aren't already being monitored by our team, these products can be submitted to us and we will initiate monitoring them the next business day. We only monitor public or commercially available solutions.
- The Vulnerability Database covers vulnerabilities that can be exploited in all types of products – software, hardware, firmware, etc.
- The vulnerabilities verified by our team are described in client database as an Advisory and listed in the Sattrix Vulnerability Reports, detailing what IT Security teams need to know to mitigate the risk posed by the vulnerability in their environment.
- The Vulnerability Database covers vulnerabilities that can be exploited in all types of products and also, we cover zero days and eos/eol.
- We create daily and weekly reports including all the details of that vulnerability and total vulnerability count in last week and provide it to customer as well.
- The Sattrix Advisory descriptions include severity, under investigation product, Affected Product, cve id, Sattrix score, reference links and remediations.
- Sattrix researchers monitor the vulnerabilities within 5 business working days.

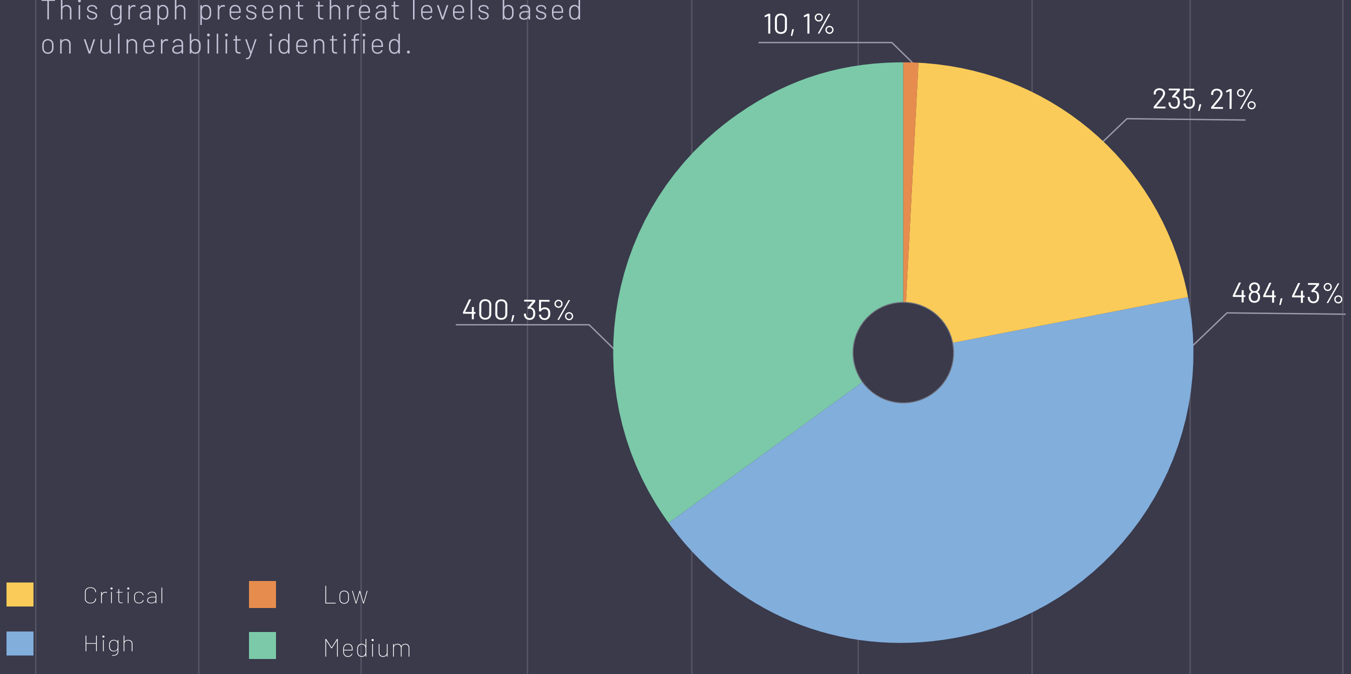
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



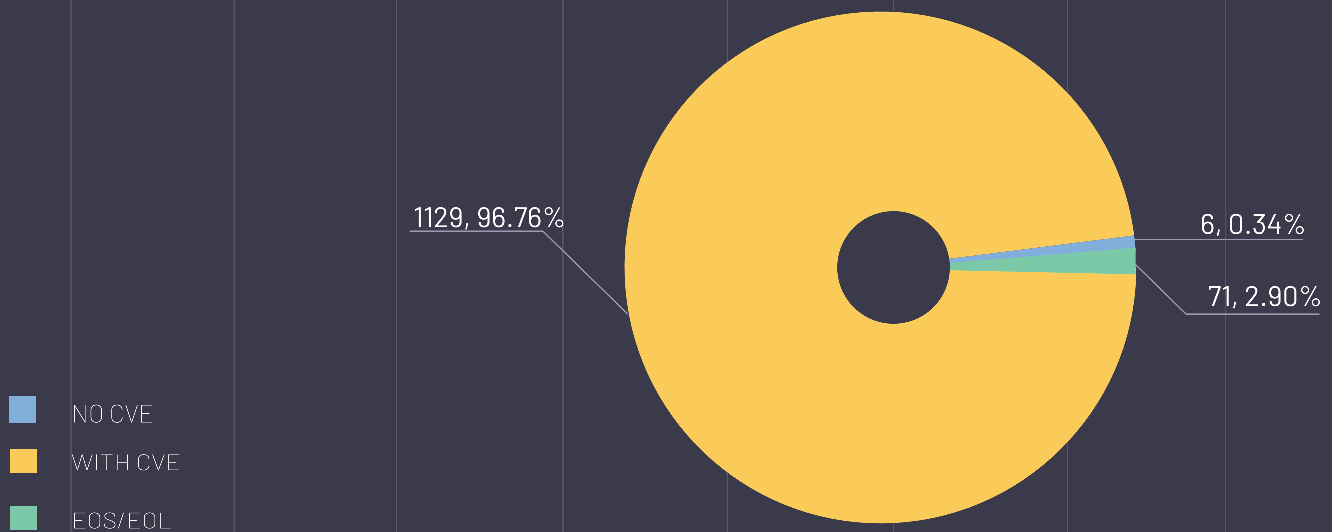
Released Vulnerabilities and severity wise count low severity count

This graph present threat levels based on vulnerability identified.

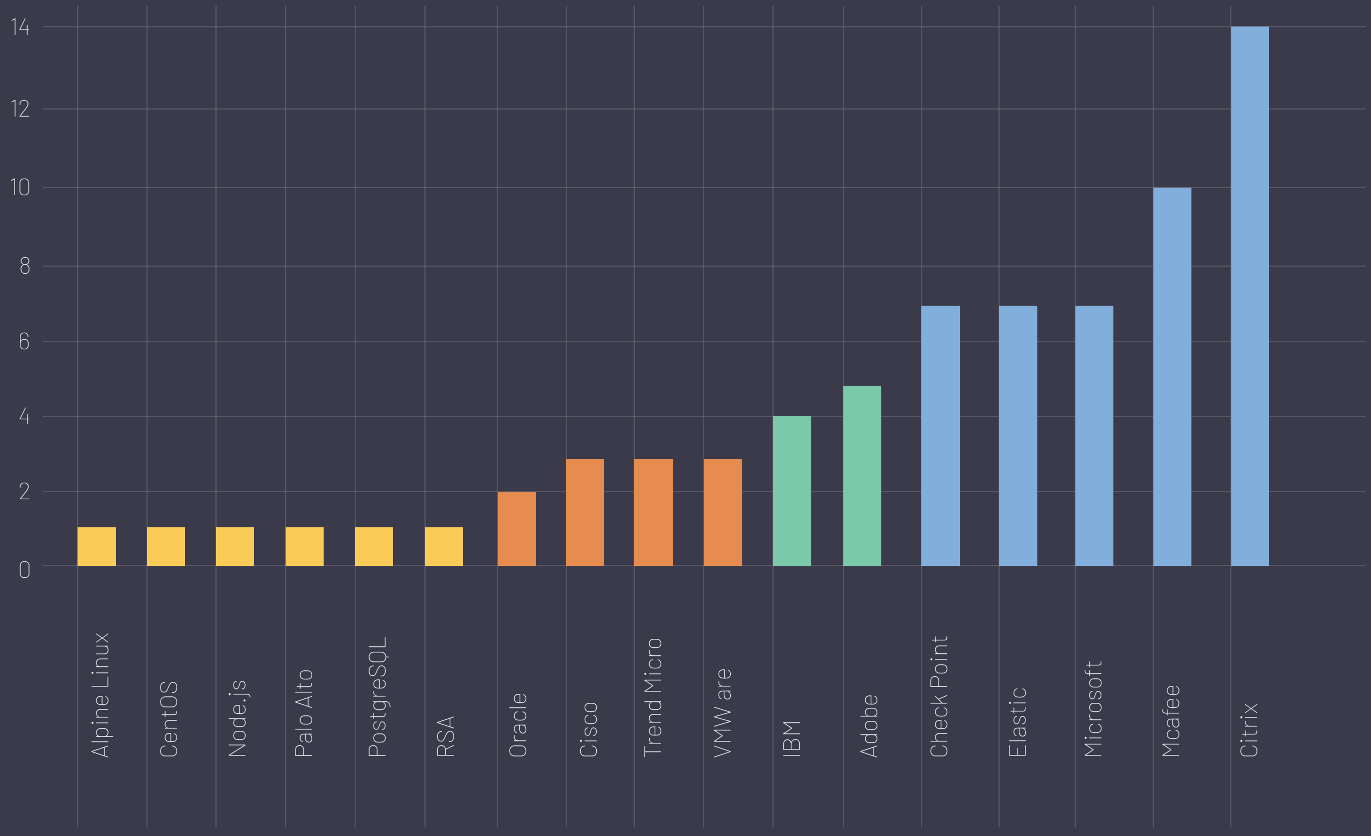


EXECUTIVE SUMMARY

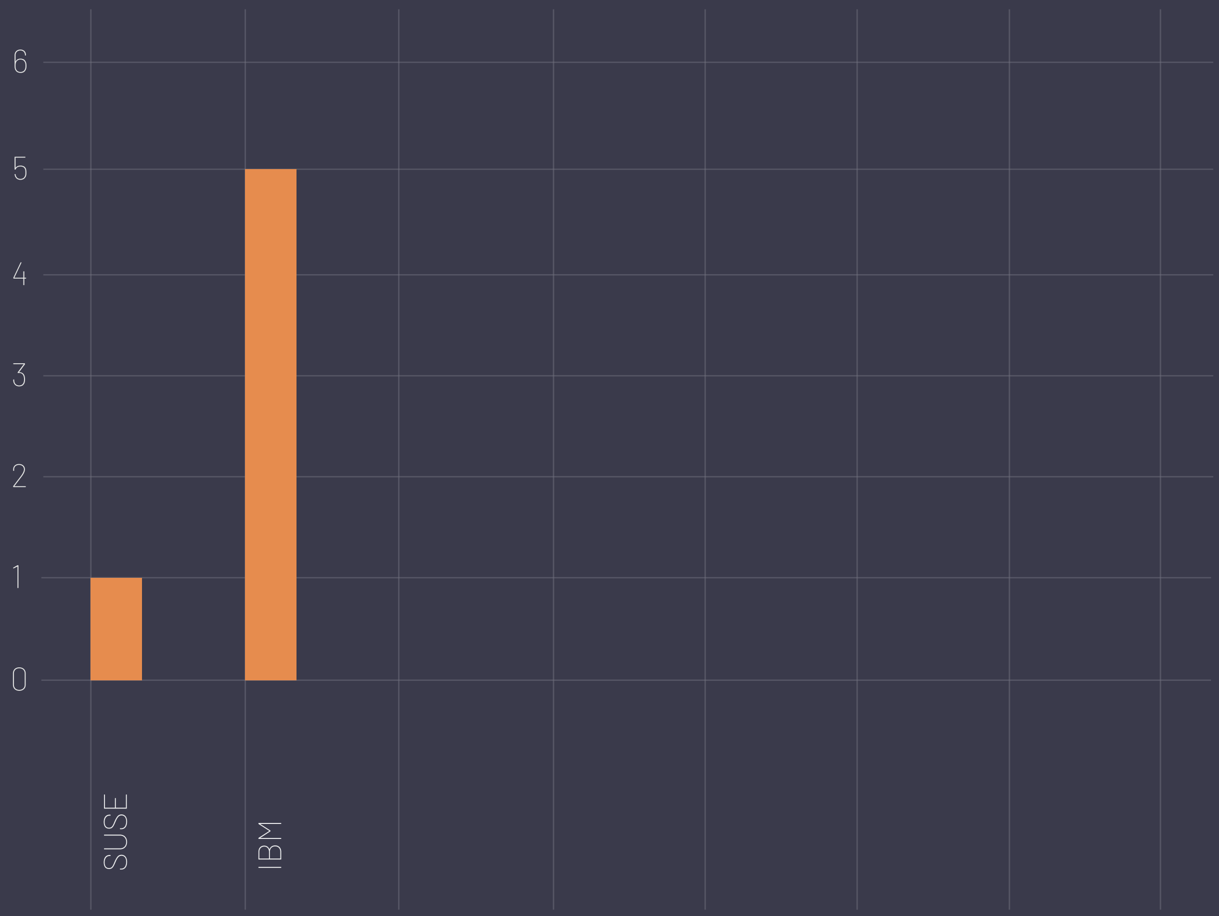
This graph present total released vulnerabilities including Zero-day vulnerability and EOS/EOL with their count.



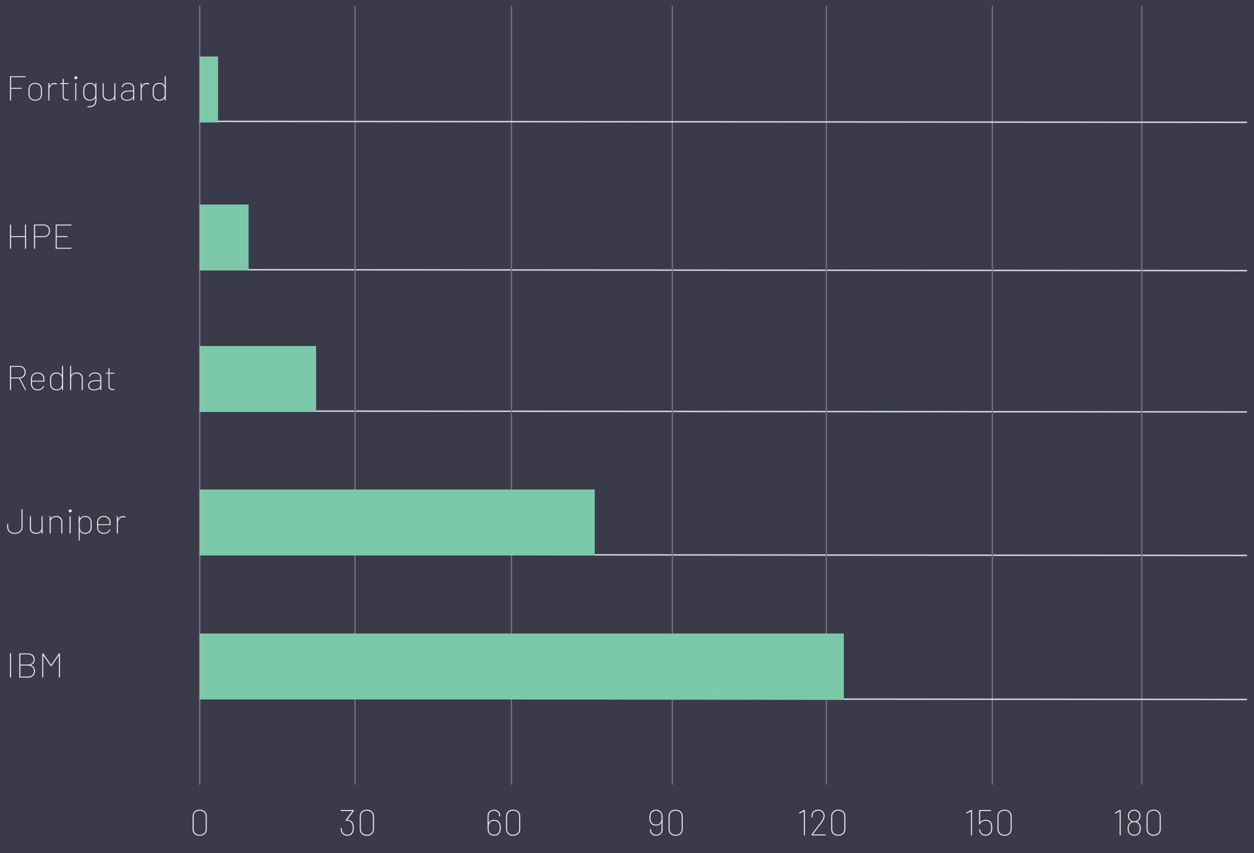
Product wise Released EOS/EOL count



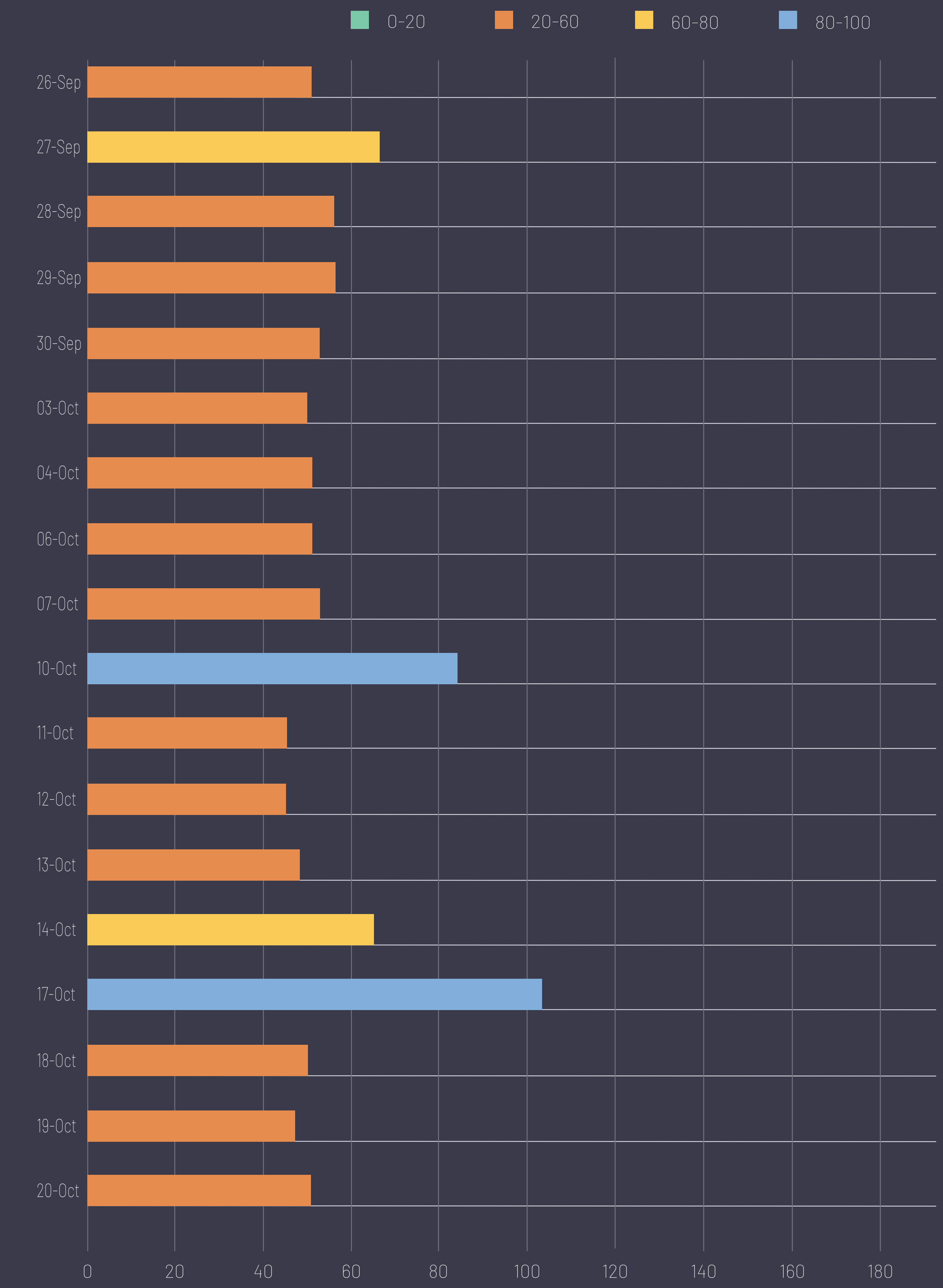
Product wise Released Non-CVE ID or Zero Day vulnerabilities Count

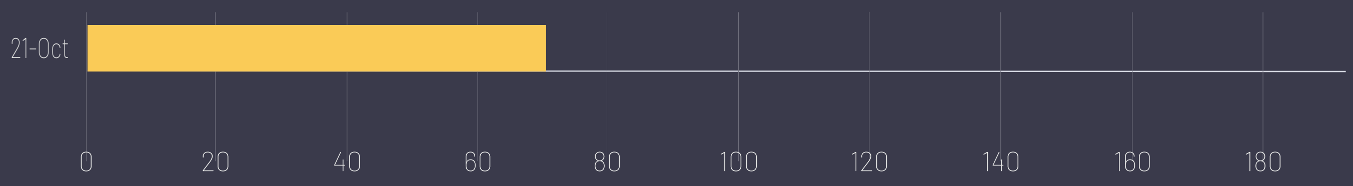


Critical CVE count

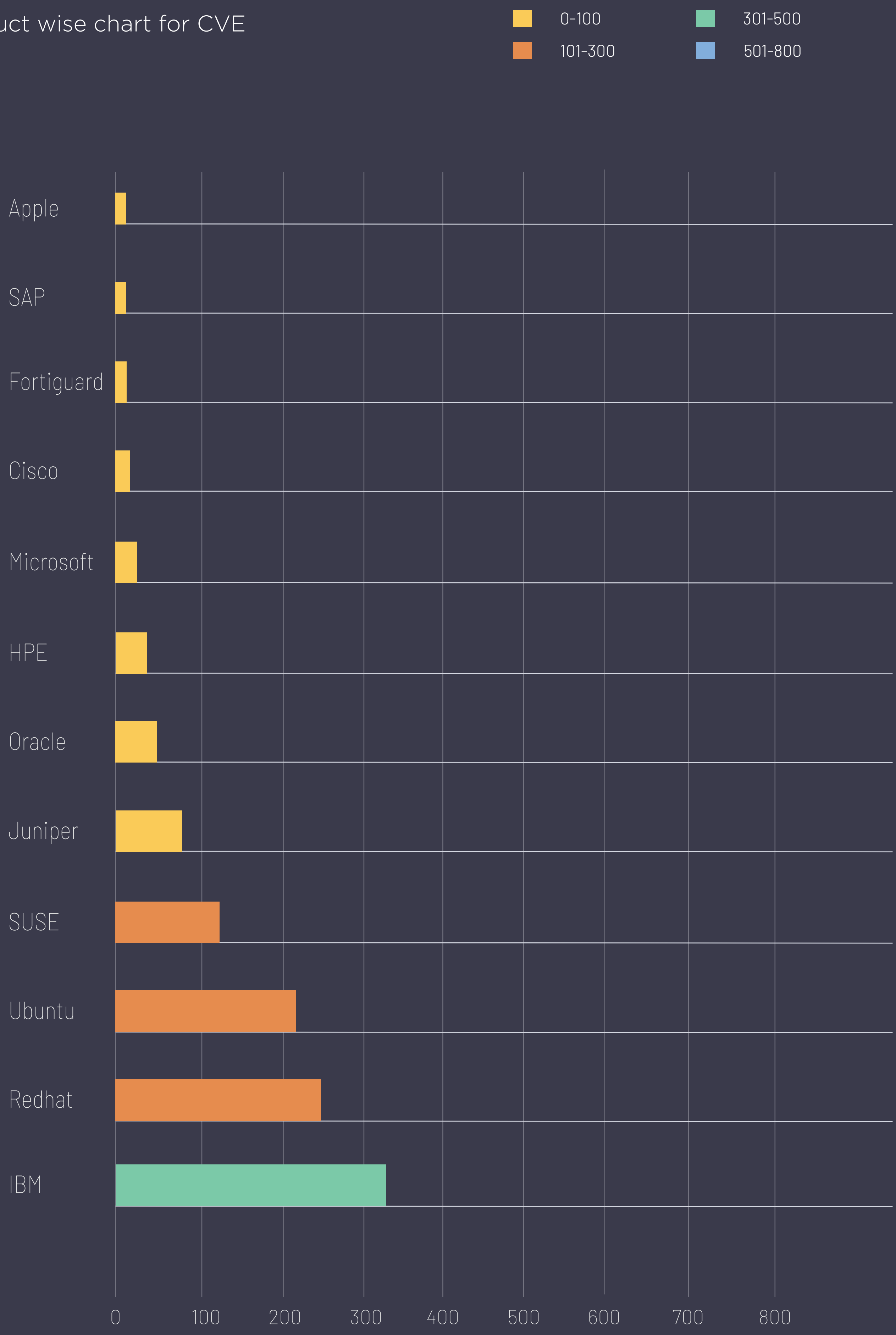


Datewise Releasd Vulnerabilities Count, Fortnightly Summarized




21-Oct
0
20
40
60
80
100
120
140
160
180

Product wise chart for CVE



TOP VULNERABILITIES OF THE WEEK

Data	CVE ID	Vendor	Product	Summary	Recommendation
29-09-22	CVE-2015-20107 CVE-2021-40528 CVE-2022-0391 CVE-2022-1292 CVE-2022-1586 CVE-2022-1785 CVE-2022-1897 CVE-2022-1927 CVE-2022-2068 CVE-2022-2097 CVE-2022-2526 CVE-2022-21123	Redhat	Red Hat Advanced Cluster Management for Kubernetes 2 for RHEL 8 x86_64 Red Hat Advanced Cluster Management for Kubernetes 2 for RHEL 7 x86_64	Red Hat Advanced Cluster Management 2.4.6 security update and bug fixes	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2022:6696
30-09-22	CVE-2017-16028 CVE-2021-37712 CVE-2021-32804 CVE-2021-37701 CVE-2021-32803 CVE-2021-37713 CVE-2018-3745 CVE-2019-10746 CVE-2018-3719 CVE-2020-7788 CVE-2019-10747 CVE-2022-0235	IBM	IBM Tivoli Netcool/OMNIbus_GUI8.1.0 FP27 and earlier	Multiple vulnerabilities in React, webpack and Node.js modules affect Tivoli Netcool/OMNIbus WebGUI	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-react-webpack-and-node-js-modules-affect-tivoli-netcool-omnibus-webgui/
03-10-22	CVE-2022-27780 CVE-2022-27781 CVE-2022-27778 CVE-2022-27782 CVE-2022-30115 CVE-2022-27779 CVE-2022-27776 CVE-2022-27775 CVE-2022-27774	IBM	IBM MaaS360 Cloud Extender Agent 2.106.500.011 and prior IBM MaaS360 Cloud Extender Base 2.106.500 and prior	IBM MaaS360 Cloud Extender Agent and Base Module use libcurl with multiple known vulnerabilities	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-ibm-maas360-cloud-extender-agent-and-base-module-use-libcurl-with-multiple-known-vulnerabilities/

Data	CVE ID	Vendor	Product	Summary	Recommendation
04-10-22	CVE-2022-0778 CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-25235 CVE-2022-25236 CVE-2022-25315 CVE-2022-27191	IBM	IBM Robotic Process Automation for Cloud Pak21.0.2	Multiple Security Vulnerabilities may affect IBM Robotic Process Automation for Cloud Pak	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-multiple-security- vulnerabilities-may-affect-ibm-robotic-process-automation-for-cloud-pak-5/
10-10-22	CVE-2019-12086 CVE-2018-5968 CVE-2019-16943 CVE-2017-15095 CVE-2020-11620 CVE-2020-36187 CVE-2018-19361 CVE-2018-14720 CVE-2020-36180 CVE-2019-12384 CVE-2019-10202	IBM	z/Transaction Processing Facility 1.1	z/Transaction Processing Facility is affected by multiple vulnerabilities in the jackson-databind, jackson-dataformat-xml, jackson-core, slf4j-ext, and cxf-core packages	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-z-transaction-processing-facility-is-affected-by-multiple-vulnerabilities-in-the-jackson-databind-jackson-dataformat-xml-jackson-core-slf4j-ext-and-cxf-core-packages/
12-10-22	CVE-2022-23302 CVE-2020-9488 CVE-2022-23307 CVE-2019-17571 CVE-2021-4104 CVE-2020-9493 CVE-2022-23305	IBM	InfoSphere Information Server 11.7	IBM InfoSphere Information Server may be affected by vulnerabilities in Apache log4j 1.x version	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-ibm-infosphere-information-server-may-be-affected-by-vulnerabilities-in-apache-log4j-1-x-version-2/
17-10-22	CVE-2008-5161 CVE-2015-9262 CVE-2016-2124 CVE-2016-4658 CVE-2018-10689 CVE-2018-20532 CVE-2018-20533 CVE-2018-20534 CVE-2018-25032 CVE-2019-12735 CVE-2019-18282 CVE-2019-19532 CVE-2019-20811	Juniper	Juniper Networks Session Smart Router: All versions prior to 5.4.7; 5.5 versions prior to 5.5.3.	Session Smart Router: Multiple vulnerabilities resolved	Updates are available please see below reference link: https://supportportal.juniper.net/s/article/2022-10-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved?language=en_US

Data	CVE ID	Vendor	Product	Summary	Recommendation
18-10-22	CVE-2022-37885 CVE-2022-37886 CVE-2022-37887 CVE-2022-37888 CVE-2022-37889 CVE-2022-37890 CVE-2022-37891	HPE	Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below * Aruba InstantOS 6.5.x: 6.5.4.23 and below * Aruba InstantOS 8.6.x: 8.6.0.18 and below * Aruba InstantOS 8.7.x: 8.7.1.9 and below * Aruba InstantOS 8.10.x: 8.10.0.1 and below * ArubaOS 10.3.x: 10.3.1.0 and below	Aruba Access Points, Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04371en_us
19-10-22	CVE-2022-33873	Fortiguard	* FortiTester version 7.1.0 * FortiTester version 7.0.0 * FortiTester version 4.2.0 * FortiTester version 4.1.0 through 4.1.1 * FortiTester version 4.0.0 * FortiTester version 3.9.0 through 3.9.1 * FortiTester version 3.8.0 * FortiTester version 3.7.0 through 3.7.1 * FortiTester version 3.6.0 * FortiTester version 3.5.0 through 3.5.1 * FortiTester version 3.4.0 * FortiTester version 3.3.0 through 3.3.1 * FortiTester version 3.2.0 * FortiTester version 3.1.0	FortiTester - Unauthenticated command injection	Updates are available please see below reference link: https://www.fortiguard.com/psirt/FG-IR-22-237
20-10-22	CVE-2022-40684	Fortiguard	FortiOS versions 5.x, 6.x are NOT impacted. * FortiOS version 7.2.0 through 7.2.1 * FortiOS version 7.0.0 through 7.0.6 * FortiProxy version 7.2.0 * FortiProxy version 7.0.0 through 7.0.6 * FortiSwitchManager version 7.2.0 * FortiSwitchManager version 7.0.0	FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface	Updates are available please see below reference link: https://www.fortiguard.com/psirt/FG-IR-22-377

Disclaimer: The information in this document is subject to change without notice and should not be construed as a commitment by Sattrix Information Security (P) Ltd. Sattrix provides no warranty, express or implied, including warranties of merchantability and information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Sattrix or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if Sattrix or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from Sattrix, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners © Copyright 2013-2022 Sattrix. All rights reserved.

Limitation of Liability: IN NO EVENT SHALL Sattrix, Sattrix AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF Sattrix HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Global Presence

USA / Sattrix Information Security Incorportation
UK/ EU / Sattrix Info Security Ltd
MEA / Sattrix Information Security DMCC
India / Sattrix Information Security (P) Ltd

Office Address

1 Parklane Blvd, Ste 729 E;
Dearborn, MI 48126

Golbal SOC

516, 517 Shivalik Shilp,
Iscon Cross Road, S G Highway, Ahmedabad

+1 416-917-8344   info@sattrix.com   **www.sattrix.com**