SanerNow Risk Assessment Report Solution Brief

The modern IT landscape is constantly changing and possesses numerous security risks. Starting from vulnerabilities, security misconfigurations, shadow IT, and failed security controls to missing patches, these risks could potentially be exploited to cause harm to the organizations. If the security teams do not have clear visibility over all the prevalent risks in their network, they might focus their efforts in the wrong areas, leaving the real threats behind.

If these risk insights are scattered in different places, it gets tedious to perform a comprehensive assessment and understand the organization's risk exposure clearly. Security teams need a comprehensive risk assessment report, from which they can obtain a complete picture of the risks in their network and manage them effectively.

Benefits of a Comprehensive Risk Assessment Report

Plan mitigation activities & strengthen the security posture

It will help you identify different security risks and understand weak security measures. You can assess the trending date, plan the risk mitigation activities, and enhance your organization's security posture.

Review existing security controls

You can review the efficacy of your existing security controls and update them where necessary. This will increase the effectiveness of your security attack prevention program.

Achieve compliance goals

Meeting industry security compliance is an important goal for organizations. If your organization fails to comply, you may face undesirable financial and reputation loss. With comprehensive risk assessment, you can assess and align against your compliance goals and ensure your organization meets the requisite security guidelines.

1 1 01 0 1 00 011 0101

SanerNow's Risk Assessment Report

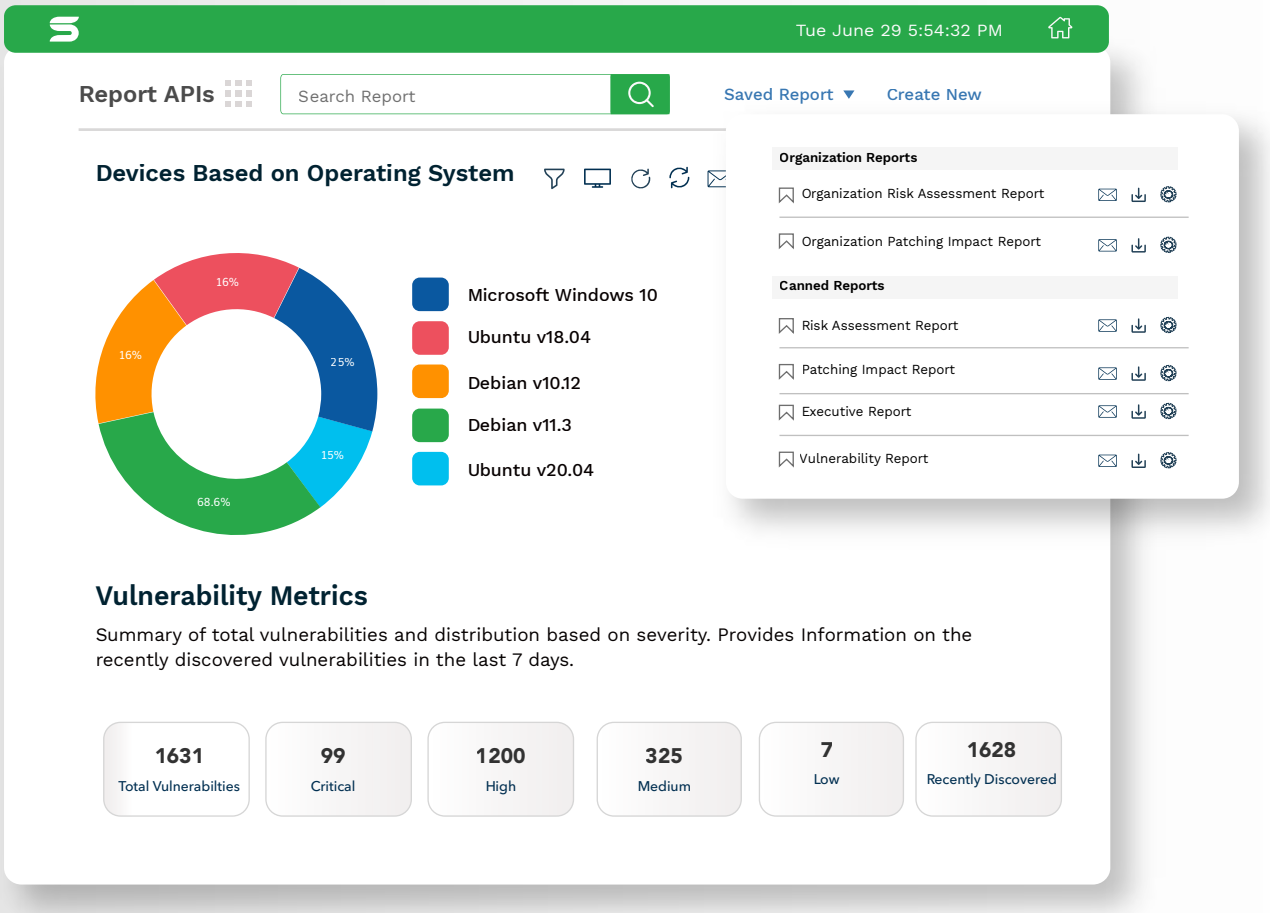
SecPod SanerNow's Risk Assessment Report provides comprehensive insights into the risk exposure of all your IT assets, vulnerabilities, patches, and misconfigurations in one single place. This report will enable security teams to seamlessly assess different security risks and plan their mitigation efforts smartly. SanerNow Risk Assessment Report gives you real-time visibility into security risks lurking in your organization's IT network. The report can be generated on-demand anytime and anywhere. You can also view the trending data of this report to analyze information for a period.

Overview of the risk insights covered in the report:

The report consists of five sections

Overall Summary

This section provides the overall summary of the risks prevalent in your network. You can view details on the devices based on groups and operating systems, recently discovered vulnerabilities based on their severity, number of compliant and non-compliant devices, patch details based on their severity, vulnerability, misconfiguration, and patch trend details over the last 90 days. The details provided here will let you understand the overall risk exposure in your IT infrastructure and plan risk mitigation activities smartly.



Vulnerabilities

This section provides details on the vulnerabilities in your network based on their severity, operating systems, and organization groups. To understand your network's vulnerability exposure and their potential risks clearly, this report also provides insight on the top 10 metrics of the following:

Top 10 vulnerabilities by CVSS (Common Vulnerability Scoring System) score

Vulnerabilities in your network are categorized based on the CVSS score and ranked in the top 10 order. This will enable you to identify the most critical vulnerabilities in your network.

Top 10 Vulnerabilities by CVSS Score

Top vulnerabilities reported with high severity across assets

Critical	High	Medium	Low
9.0 - 10.0	7.0 - 8.9	4.0 - 6.9	0.1 - 3.9

CVE-ID	Title	CVSS Score	Severity	Total Assets
CVE- 2015 - 4844	Unspecified Vulnerability in Oracle...	10	Critical	3
CVE - 2015 - 4479	Multiple Integer Overflows in Libstag...	10	Critical	2
CVE - 2015 - 4760	Unspecified Vulnerability in Oracle...	10	Critical	3
CVE - 2016 - 0494	Unspecified Vulnerability in the Java...	10	Critical	3
CVE - 2015 - 4473	Multiple Specified Vulnerabilities...	10	Critical	2
CVE - 2015 - 4486	The decrease_ref_count function in...	10	Critical	2
CVE - 2015 - 4485	Heap_based buffer overflow in the...	10	Critical	2
CVE - 2015 - 2590	Unspecified Vulnerability in Oracle...	10	Critical	2
CVE - 2016 - 0483	Unspecified Vulnerability in Oracle...	10	Critical	2
CVE - 2015 - 2739	The Array Buffer Builder::append...	10	Critical	1

Top 10 vulnerabilities across Hosts

Vulnerabilities that affect the maximum number of devices with high severity are specified here. This will help you identify the vulnerabilities which affect most of your devices and help you remediate them quickly to minimize the attack surface.

Top 10 Vulnerabilities Across Hosts

Top vulnerabilities reported with high severity across hosts.
These vulnerabilities impact the maximum number of devices.

Critical	High	Medium	Low
9.0 - 10.0	7.0 - 8.9	4.0 - 6.9	0.1 - 3.9

CVE-ID	Title	CVSS Score	Severity	Total Assets
CVE- 2015 - 7201	Multiple Unspecified Vulnerabilities in...	10	Critical	2
CVE - 2015 - 2739	The Array Buffer Builder::append...	10	Critical	2
CVE - 2015 - 4485	Heap_based buffer overflow in the...	10	Critical	2
CVE - 2015 - 2724	Multiple Unspecified Vulnerabilities in...	10	Critical	2
CVE - 2015 - 2731	Use-after-free Vulnerability in the CSP...	10	Critical	2
CVE - 2015 - 4473	Multiple Unspecified Vulnerabilities in...	10	Critical	2
CVE - 2015 - 2738	The YCbCrImageDataDeserializer::To...	10	Critical	2
CVE - 2015 - 2590	Use-after-free Vulnerability in the Can...	10	Critical	2
CVE - 2015 - 2733	The decrease_ref_countfunction in li...	10	Critical	2
CVE - 2015 - 4486	The Array Buffer Builder::append...	10	Critical	2
CVE - 2015 - 7205	Integer Underflow in the RTPReceiver...	10	Critical	2

Top 10 vulnerabilities Hosts

This section shows the devices with the most number of vulnerabilities. With this, you can identify the devices with a high vulnerability count and quickly remediate them.

Top 10 Vulnerable Hosts

Top Devices with high number of vulnerabilities

Host Name	Operating System Name	Group	Vulnerabilties	Critical	High	Medium	Low
qa-ubuntu-14-04-x64	Ubuntu v14.04 architecturex86...	ubuntu	3271	608	1275	1325	63
centos-6.7-qa	CentOS v6.7 architecturex86_64	centos	1230	268	470	446	46
bk-testubuntu	Ubuntu v16.04 architecturex86...	Ubuntu_Benchmark	198	12	126	60	0
rhel-7.9-x64	Red HatEnterprise Liux v7.9 a...	red hat	162	18	73	76	5
desktop-jdn034t	Microsoft Windows10v220H2 ar...	windows10	125	15	55	65	0
centos-6.7-a	CentOS v6.7 architecturex86_64	centos	50	6	30	25	3
ak-ubuntu	Ubuntu v16.04 architecturex86...	Ubuntu_Benchmark	12	2	14	14	4
rhel-7.0-x64	Red HatEnterprise Liux v7.9 a...	red hat	5	3	10	6	0
desktop-ajdn034t	Microsoft Windows10v220H2 ar...	windows10	2	1	3	3	2
rhel	Red HatEnterprise Liux v7.9 a...	red hat	1	0	1	1	0

Top 10 highly exploited vulnerabilities

This section provides details on the top 10 vulnerabilities that are exploited in the wild. These vulnerabilities are highly exploited, and you can plan your remediation task to fix them immediately.

Top 10 Highly Exploited Vulnerabilities

Top highly exploited vulnerabilities reported across devices. These vulnerabilities are being exploited in the wild.

CVE-ID	Title	MVE-ID	CVSS Score	Severity	Hosts
CVE-2019-11708	Firefox Active Exploits(MVE-000276)	Insufficient vetting of parameters p...	10	Critical	1
CVE-2015-2590	Sofacy APT28(MVE-000118)	Unspecified vulnerability in Oracle...	10	Critical	1
CVE-2017-5375	Disdain Exploit Kit (MVE-000016)	JIT code allocation can allow for a...	9.8	Critical	1
CVE-2017-7494	EternalRed(MVE-000483)	Samba since version 3.5.0 and before...	9.8	Critical	1
CVE-2017-3289	Neptune Exploit Kit(MVE-00015)	Vulnerability in the JAVA SE, JAVA S...	9.6	Critical	1
CVE-2019-11707	Firefox ACtive Exploits(MVE-000276)	A type confusion vulnerability in IonMo...	8.8	Critical	1
CVE-2019-17026	Gh0stRAT Trojan(MVE-000133),Mozil...	A type confusion vulnerability can o...	8.8	Critical	1
CVE-2016-9078	Disdain Exploit Kit(MVE-000016)	Redirection from an HTTP connection...	8.8	Critical	1
CVE-2020-12351	BleedingTooth(MVE-000409)	Improper input alidation in BlueZ...	8.8	Critical	1
CVE-2020-8616	NXNSAttack(MVE-000336)	Denial of service vulnerability in bin...	8.6	Critical	1

Top 10 recommended remediation

This section provides the remediation recommendations on the top 10 vulnerable assets with a high number of risks. You can look out for these assets and fix their vulnerabilities to prevent potential attacks.

Top 10 recommended remediation

Top vulnerable assets with high number of risks which can be mitigated

Remediation-ID	Asset Name	Patch	Vendor	Identified Date	Risk Count	Hosts
ERI-18874	firefox	firefox	mozilla	2022-03-25 06:38:55 AM UTC	655	1
ERI-18874	linux-image-generic	linux-image-generic	linux	2022-03-25 06:39:51 AM UTC	395	1
ERI-18874	linux-image	linux-image	linux	2022-04-08 02:09:58 PM UTC	305	1
ERI-18874	liboxideqtcore0	liboxideqtcore0	oxide-qt	2022-03-25 06:38:51 AM UTC	236	1
ERI-18874	tcpdump	tcpdump	redhat	2022-03-25 06:38:55 AM UTC	139	1
ERI-18874	libtiff5	libtiff5	libtiff	2022-03-25 06:38:55 AM UTC	101	1
ERI-18874	oxideqt-codecs	oxideqt-codecs	oxide-qt	2022-03-25 06:38:55 AM UTC	96	1
ERI-21361	Google Chrome	Google Chrome	google	2022-03-25 06:38:55 AM UTC	80	1
ERI-18874	xuli-ext-ubufox	xuli-ext-ubufox	mozilla	2022-03-25 06:38:05 AM UTC	72	1
ERI-18874	libssl1.0.0	libssl1.0.0	openssl	2022-04-25 06:38:55 AM UTC	70	1

Misconfigurations

The Misconfigurations section of the report provides detailed insights on the missing security configurations and deviations in compliance. The report provides details on the compliance benchmark deviations by operating systems, organization groups, and the percentage of rules in a benchmark that are successfully implemented and failed in your network. With this, you can understand the configuration deviations in your network, harden system configurations, and abide by industry compliance benchmarks.

The report also provides the top 10 metrics of your compliance and misconfiguration details to keep you aware of the high risks in your network. The top 10 metrics are provided for the following:

Top 10 Non-compliant Devices

Provides the details of the top 10 devices with the most number of compliance deviations. With this, you can quickly lookout for these critical devices and fix their misconfigurations.

Top 10 Non-compliant Devices

Top devices with most number of compliance deviations.

Host Name	Operating System Name	Group	Benchmark	Total Deviations
rhel-7.9 x64	Red Hat Enterprise Linux v7.9 are...	redhat	RHEL General Benchmark	126
bk-test-ubuntu	Ubuntu 16.04 architecturex86_64	Ubuntu_Benchmark	Ubuntu_GeneralCompliance	78
desktop-jdn034t	Microsoft Windows 10 v20...	windows 10	SecPod default	46
qa-ubuntu 14-04-x64	Ubuntu 14.04 architecture x86_64	ubuntu	SecPod default	26
centos-6.7-qa	CentOS v6.7 architecturex86...	centos	SecPod default	20
ak-ubuntu	Ubuntu 16.04 architecturex86_64	Ubuntu_Benchmark	Ubuntu_GeneralCompliance	15
desktop-ajdn034t	Microsoft Windows 10 v20...	windows 10	SecPod default	11
qa-ubuntu	Ubuntu 14.04 architecture x86_64	ubuntu	SecPod default	5
centos-6.7	CentOS v6.7 architecturex86...	centos	SecPod default	3
rhel	Red Hat Enterprise Linux v7.9 are...	redhat	RHEL	1

Top 10 Non-compliant Rules

Provides the details of the top 10 non-compliant rules deviated in your network. This will help you assess the non-compliant rules in the security benchmarks and work on them immediately.

Top 10 Non-Compliant Rules

Rules that are deviating for a compliance benchmark across devices.

CCE-ID	Rule Name	Benchmark	Hosts
CCE-26282.4	Set SSH Client Alive Count	CENTOS6_COMPLIANCE_DEFAULT	1
CCE-26555-3	Use Only Approved Ciphers	CENTOS6 COMPLIANCE_DEFAULT	1
CCE-28995-2	Set Password Maximum Age	CENTOS6_COMPLIANCE_DEFAUL	1
CCE-27002-5	Set Password Minimum Length in login.dets	CENTOS6_COMPLIANCE_DEFAULT	1
CCE-27013-2	Set Password Minimum Age	MS_WIN 1D_COMPLIANCE_DEFAULT	1
CCE 41504-2	Interactive logon: Prompt user to changepas...	MS_WIN1D_COMPLIANCE_DEFAULT	1
CCE-41561-2	Interactive logon Machine account lockout thr...	MS_WIN10_COMPLIANCE_DEFAULT	1
CCE-41676-8	Require a Password When a Computer Wakes...	MS WIND COMPLIANCE_DEFAULT	1
CCE-41679-2	Minimum password length	MS_WIN10_COMPLIANCE_DEFAULT	1
CCE-41763-4	System cryptography. Force strong key protecti...	MS_WIN10_COMPLIANCE_DEFAULT	1

Top 10 Recommended Misconfiguration Remediations

Provides details on the Top 10 misconfiguration remediations recommended for your network. Using this, you can quickly mitigate the risks and achieve compliance in your network.

Top 10 Recommended Mis-configuration Remediation

Top mis-configuration remediation available across devices which can be mitigated

Remediation ID	Asset Name	Patch	Risks Count	Risks	Hosts
ERI-9925	Red Hat Enterprise Linux 7	cce-90823-6-patch.sh	1	CCE-90823-6	1
ERI-9892	Red Hat Enterprise Linux 7	cce-90988-7-patch.sh	1	CCE-90988-7	1
ERI-9789	Red Hat Enterprise Linux 7	cce-90654-5-patch.sh	1	CCE-90654-5	1
ERI-12948	Ubuntu 16.04	cce-91912-6-patch.sh	1	CCE-91912-6	1
ERI-20057	Red Hat Enterprise Linux 7	cce-95519-5-patch.sh	1	CCE-95519-5	1
ERI-9735	Red Hat Enterprise Linux 7	cce-90920-C-patch.sh	1	CCE-90920-0	1
ERI-12877	Ubuntu 16.04	cce-91955-5-patch.sh	1	CCE-91955-5	1
ERI-18623	Ubuntu 16.04	cce-95694-6-patch.sh	1	CCE-95694-6	1
ERI-12935	Ubuntu 16.04	cce-91959-7-patch.sh	1	CCE-91959-7	1
ERI-9950	Red Hat Enterprise Linux 7	cce-90895-4-patch.sh	1	CCE-90895-4	1

Missing Patches

Patches are critical to fixing the vulnerabilities and security misconfiguration risks in your network. This section of the report provides detailed insights into the missing patches in your network. You can view the missing security patches information based on Operating Systems and Organization Device Groups. The report also provides certain top 10 metrics of the missing security patches, which include the following:

Top 10 missing security patches

Provides the list of the top 10 missing security patches which pose the highest number of risks. This will enable you to apply these security patches effectively and mitigate the security risks.

Top 10 Missing Security Patches

Missing security patches with highest number of risks.

Asset Name	Risks	Vendor	Identified Date	Severity	Hosts
firefox	655	mozilla	2022-03-25 06:38:55 AM UTC	Critical	1
linux-image-generic	395	linux	2022-03-25 06:39:51 AM UTC	Critical	1
liboxideqtcore	236	oxide-qt	2022-03-25 06:39:51 AM UTC	Critical	1
tcpdump	139	redhat	2022-03-25 06:39:52 AM UTC	Critical	1
libtiff5	101	libtiff	2022-03-25 06:39:51 AM UTC	Critical	1
oxideqt-codecs	96	oxide-qt	2022-03-25 06:39:51 AM UTC	Critical	1
Google Chrome	80	google	2022-04-26 06:39:05 AM UTC	Critical	1
xul-ext-ubufox	72	mozilla	2022-03-25 06:39:52 AM UTC	Critical	1
libss1.0.0	70	openssl	2022-03-25 06:39:51 AM UTC	Critical	1
libxml2	46	xmlsoft	2022-03-25 06:38:55 AM UTC	Critical	1

Top 10 Missing Security Patches across Devices

Provides the list of the top 10 missing security patches with the highest number of risks for the most number of devices. With this, you can identify the assets which pose huge risks across the maximum number of devices in your network and apply the required patches.

Top 10 Missing Security Patches Across devices

Missing security patches with highest number of risks for most number of devices.

Asset Name	Patch	Risks	Severity	Hosts
sudo	sudo	3	High	2
libxml2	libxml2	48	Critical	2
gstreamer 1.0-plugins-good	gstreamer 1.0-plugins-good	7	Critical	1
bind	bind	6	High	1
libplist1	libplist1	1	Medium	1
Libxrender 1	Libxrender 1	1	Critical	1
polkit	polkit	1	High	1
nss	nss	12	Critical	1
qpdf	qpdf	14	High	1
libgtk 3-0	libgtk 3-0	1	High	1

Top 10 Devices with Missing Security Patches

Provides the list of the top 10 devices in your network with the highest number of missing security patches. You can quickly detect these devices and apply security patches to prevent potential attacks.

Top 10 devices by Missing Security Patches

Devices with highest number of missing security patches.

Host Name	Operating System Name	Group	Family	Security Patches
qa-ubuntu-14-04-x64	Ubuntu v14.04 architecture x86_64	ubuntu	unix	144
centos-6.7-qa	CentOS v6.7 architecture x86 64	centos	unix	91
rhel-7.9-x64	Red Hat Enterprise Linux v7.9 arch...	red hat	unix	29
bk-testubuntu	Ubuntu v16.04 architecture x86_64	Ubuntu_Benchmark	unix	18
desktop-jdn034	Microsoft Windows 10 v20H2 archi...	windows 10	windows	12
qa-ubuntu	Ubuntu v14.04 architecture x86_64	ubuntu	unix	10
centos-6.7	CentOS v6.7 architecture x86 64	centos	unix	8
rhel	Red Hat Enterprise Linux v7.9 arch...	red hat	unix	5
bk-ubuntu	Ubuntu v16.04 architecture x86_64	Ubuntu_Benchmark	unix	2
desktop	Microsoft Windows 10	windows 10	windows	1

Asset Exposure

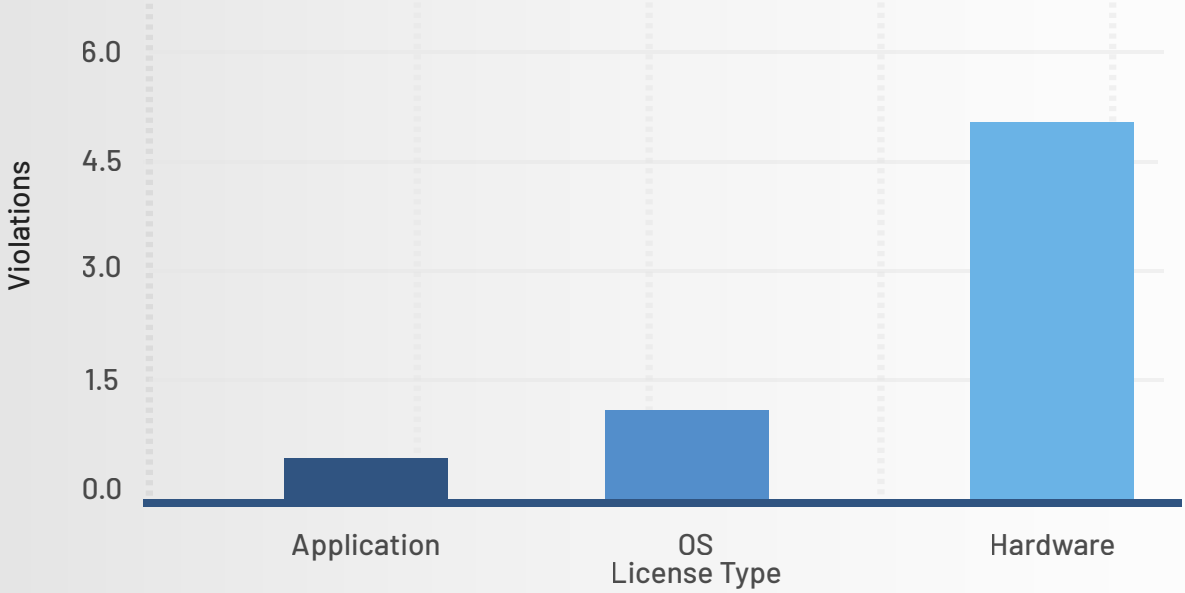
To safeguard your network, you need complete visibility over your IT assets and their exposure to potential attacks. The Asset Exposure section of the report provides detailed insights into your organization's IT assets, license violations, and outdated operating systems and applications to help you identify the risks in your organization's IT assets.

Insights on License Violations

Get detailed insights on the software assets that violate license policies and application and operating system license details, including the installation count, cost utilization, and violations.

License Violations

Software assets that are violating license policy.



Outdated Operating Systems

Outdated operating systems are a threat to organizational security. The report provides details on the devices which runs on the outdated operating systems in your network.

Outdated Operating System

Number of devices with outdated operating systems.

Operating System Name	Hosts
centOS-6	1
Ubuntu 14.04	1
Ubuntu 16.04	1

Outdated Applications

Outdated and end-of-life applications are the attacker's favorite target. The report provides details on the outdated applications installed on your network systems and the number of devices that have those applications.

Outdated Applications

Number of devices with outdated or end of life applications

Applications	Hosts
Microsoft Interner Explorer 11	1
Microsoft XML Core Services 3.0	1
Microsoft XML Core Services 6.0	1
VBScript 5.8	1

About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on computing environment. Our product helps implement cyber hygiene measures, so attackers have tough time piercing through.

Our SanerNow CyberHygiene platform provides continuous visibility to computing environment, identifies vulnerabilities and misconfigurations, mitigate loopholes to eliminate attack-surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better.

Contact Us

Email us on:info@secpod.com
Call us at:India - (+91) 80 4121 4020 / USA - (+1) 918 625 3023