IOT SECURITY CHECKUP

CHECK POINT IOT PROTECT FOR ENTERPRISE

Check Point IoT Protect

Prevent • Adapt • Everywhere

CHECK POINT™

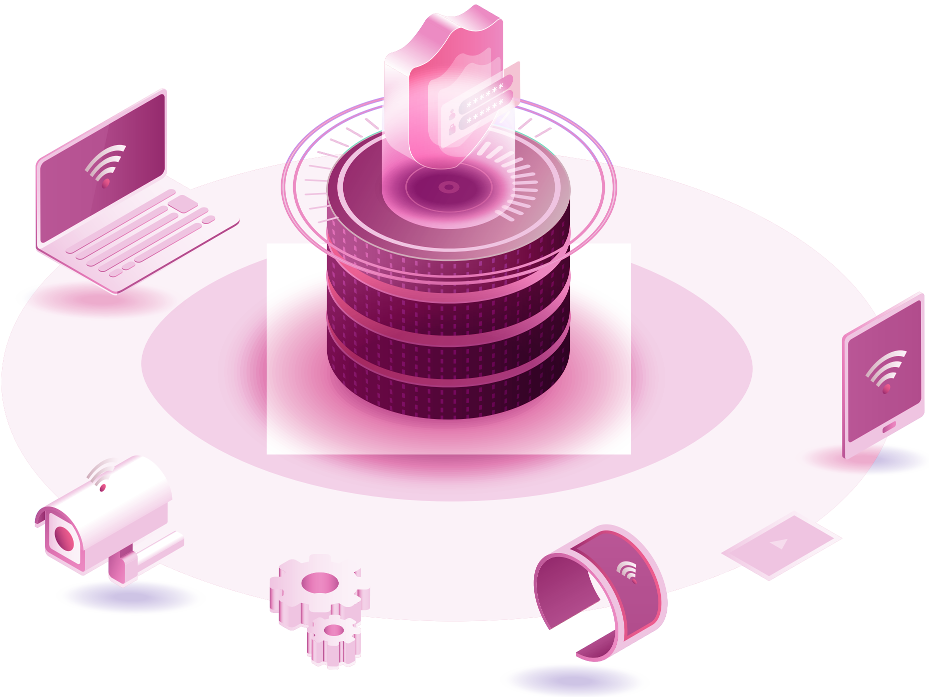
CHECK POINT IOT PROTECT FOR ENTERPRISE
SEE EVERYTHING

We are witnessing an explosion of unmanaged devices in the workplace – a digital transformation bigger than the PC and mobile revolutions combined, spanning traditional devices like laptops and smartphones to new unmanaged devices like smart TVs, security cameras, smart lighting, digital assistants, HVAC systems, medical devices, manufacturing devices and more.

Every year, the number of unmanaged and IoT devices that make their way into the enterprise grows by nearly 31%. As of 2020, the number of these devices in the enterprise is expected to be up to five times that of traditional computers. Although these connected devices help achieve greater productivity, they also create greater risk.

The vast majority of these devices have no built-in security, are hard or impossible to update, and businesses have no way to see or manage them. Traditional firewalls, network security, and EDR solutions fall short of addressing this ever-expanding cyberphysical attack surface.

How can this risk be mitigated?



CHECK POINT IOT PROTECT FOR ENTERPRISE
PLATFORM

Check Point IoT Protect for Enterprise is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Check Point IoT Protect for Enterprise discovers every managed, unmanaged, and IoT device on and off your network, analyzes device behavior to identify risks or attacks, and protects your critical business information and systems. Check Point IoT Protect for Enterprise is agentless and integrates easily with your existing security products.

CHECK POINT IOT PROTECT FOR ENTERPRISE
DEVICE SECURITY AND RISK ASSESSMENT

In this report, you will find your Device Risk and Security Assessment for your environment and the devices in and around it. This report provides a Device Security Risk (DSR) score and detailed information about the device and any security exposures. This report includes information based on a specific monitoring period and a specific portion of your network.

THE ENGAGEMENT

Check Point IoT Protect for Enterprise conducted a Device Security and Risk Assessment for Acme Corp to evaluate the following organizational risks:

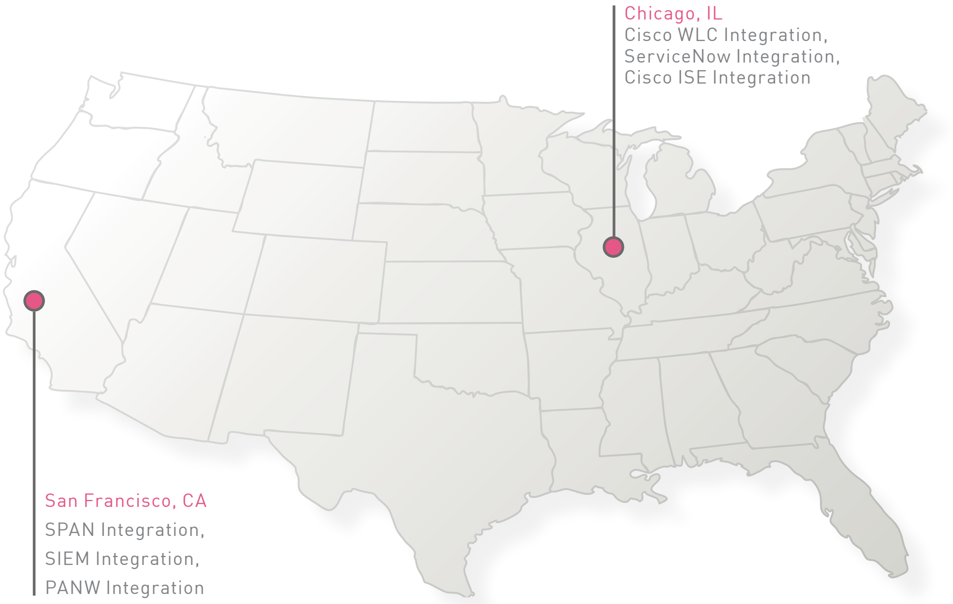
- A need for complete asset discovery of unmanaged devices
- The ability to identify unmanaged devices
- The need to understand what each device type was doing
- The inherent lack of protection of these devices
- Any potential exposure or vulnerabilities these devices pose to the business

REPORT TIMEFRAME

29 Days, November 05, 2021 - December 04, 2021

LOCATIONS

Check Point IoT Protect for Enterprise was deployed in Acme Corp's environment in the following locations using the indicated integration methods:



SCOPE OF ACCESS AND VISIBILITY

Check Point IoT Protect for Enterprise was only provided with visibility into limited parts of each site and networks, and did not have a complete view across all of Acme Corp's network, environment, and offices. Additional access across more networks and offices will yield more detailed findings, and likely, additional exposures.

OVERALL DISCOVERY SCORE SUMMARY

DEVICE DISCOVERY

			Impact	Value
Total Devices on Network				2,285
Total Unmanaged & IoT Devices	page 5	30.3% of Total	High	693
Total OT Devices				65

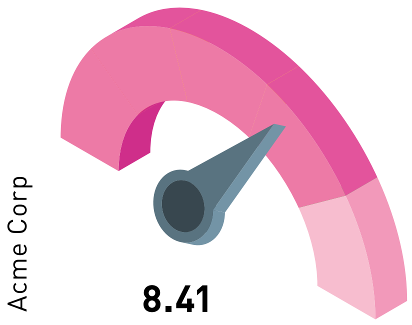
RISKS AND VULNERABILITIES

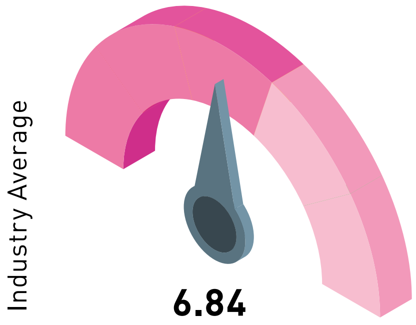
			Impact	Value
High-Risk Devices	page 8	6.17% of Total	Medium	141
Devices with Critical Vulnerabilities	page 10	15.9% of Total	High	363
Devices with Incidents	page 14	2.06% of Total	Medium	29

INCIDENTS AND THREATS

		Impact	Value
Incidents Detected	page 14	High	197
Abnormal Behavior Detected			61
High Severity Policy Violations Detected	page 15	High	83

ORGANIZATIONAL DEVICE SECURITY RISK SCORE



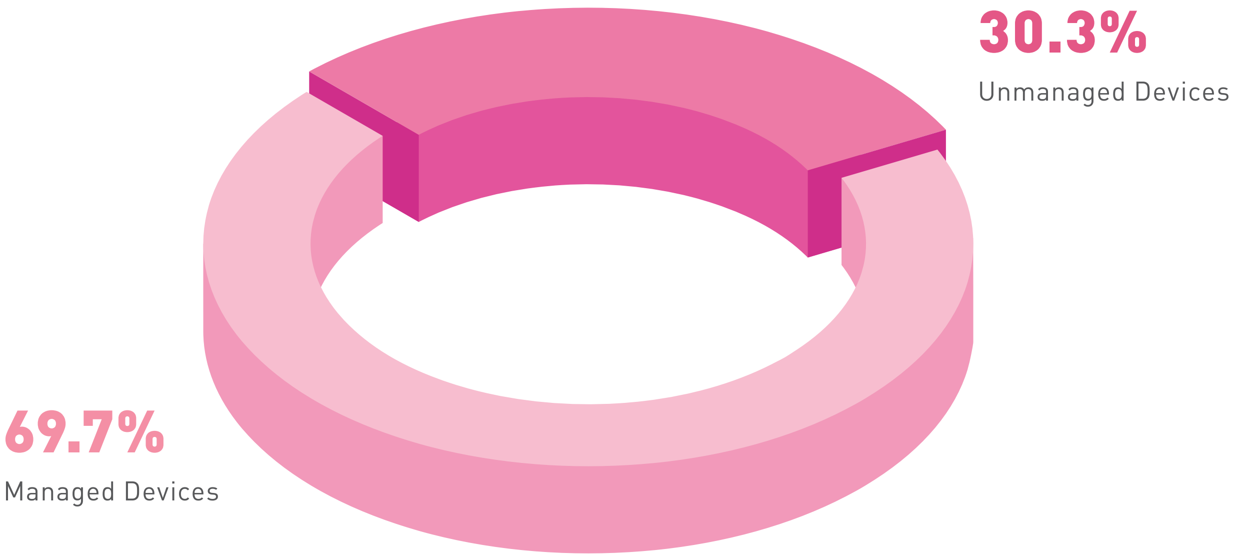


DEVICES DISCOVERED

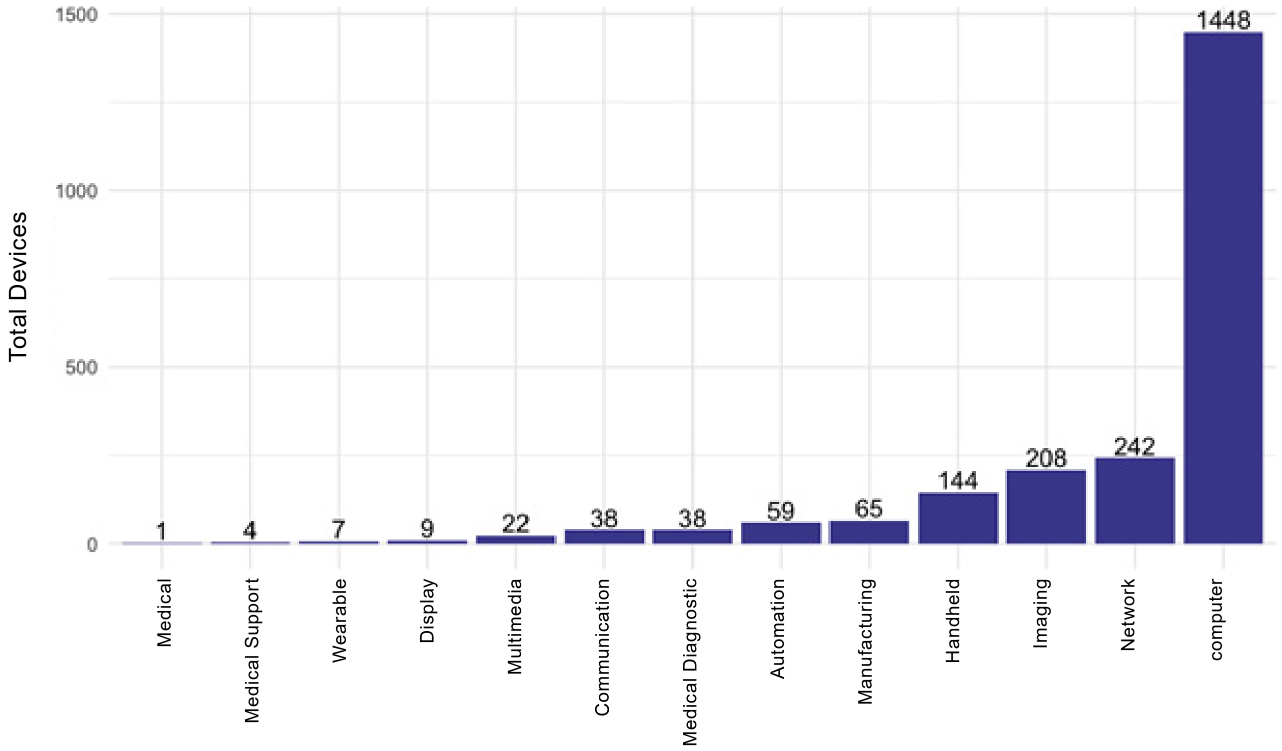
Check Point IoT Protect for Enterprise can discover all of the devices across an environment to which it has access. Beyond traditional devices like laptops and servers, there are numerous device types like smartphones, printers, smart TVs, IP phones, access points, as well as different types of IoT devices. The critical distinguishing factor is that these devices are all unmanaged. These are devices that can't host a security or management agent and therefore pose a potential risk.

The charts below include a number of devices that fall into the unmanaged device category. This includes infrastructure devices like routers and switches which have a large number of noted vulnerabilities. It also includes more mainstream IoT devices like smart TVs, smartwatches and VoIP phones, among others.

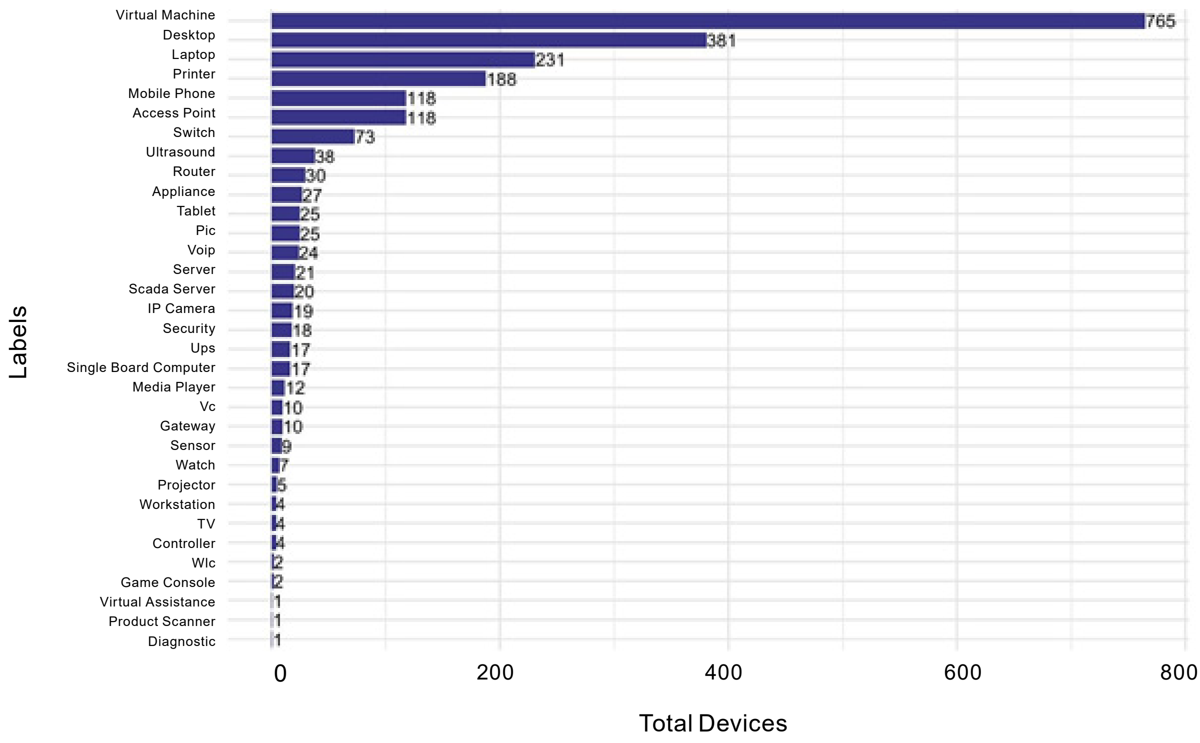
OVERALL NETWORK: MANAGED VERSUS UNMANAGED DEVICES DISCOVERED



DEVICE CATEGORIES DISCOVERED



DEVICE TYPES DISCOVERED



EXAMPLE OF DEVICES

Having discovered 2,285 devices in the Acme Corp environment, IoT Protect for Enterprise has highlighted the following devices as noteworthy examples due to rareness and/or potential risk.

Item	Information
Device	android-132q2roiy
Risk	High
MAC Address	fb:29:67:b4:ge:94
IP Address	192.0.2.10
Category	Handheld
Type	Product Scanner
Manufacturer	Zebra Technologies
Model	TC700H
OS	Android
OS Version	4.4.3
Risks	Vulnerable Bluetooth Connectivity, DNS Rebinding Vulnerability, Operating System 'Android' installed

Item	Information
Device	1756-EN2T
Risk	High
MAC Address	00:1d:9c:cc:as:b9
IP Address	192.0.2.76
Category	Manufacturing
Type	Plc
Manufacturer	Rockwell Automation
Model	1756-EN2T
OS	Rockwell Automation/Allen-Bradley OS
OS Version	20.13
Risks	Urgent 11" Vulnerability" - VxWorks, DNS Rebinding Vulnerability

Item	Information
Device	L989876
Risk	High
MAC Address	00:0c:29:88:er:3d
IP Address	192.0.2.99
Category	Medical Support
Type	Workstation
Manufacturer	GE Healthcare
Model	Viewer
OS	Windows
OS Version	7
Risks	Unencrypted Traffic: DICOM, Vulnerability Score, Unencrypted Traffic: SMB

Item	Information
Device	haggertys
Risk	High
MAC Address	b8:27:eb:12:0a:17
IP Address	192.0.2.45
Category	Computer
Type	Single Board Computer
Manufacturer	Raspberry Pi Foundation
Model	Raspberry Pi
OS	Linux
OS Version	4.14.98-v7+
Risks	Possible Port Scan, Malicious domain 'cegutotof.ru' used (Botnet C2), Policy Violation

HIGH-RISK DEVICES

During the assessment timeframe, 137 high-risk devices were found on Acme Corp's network. Below are the top 10 high-risk devices.

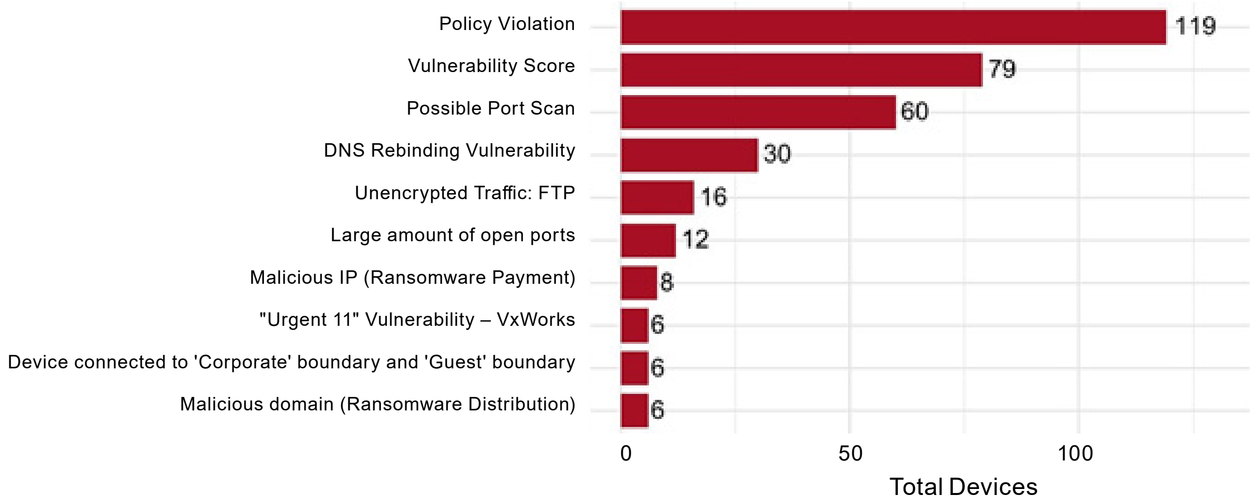
HIGH RISK MANAGED DEVICES

Risk	IP Address	Name	Category	Type	Model
High	192.0.2.102	dave-MBP	Computer	Laptop	MacBookPro
High	192.0.2.10	android-132q2roiy	Handheld	Product Scanner	TC700H
High	192.0.2.68	DC01HYDFG	Computer	Virtual Machine	VMware device
High	192.0.2.109	DC02LNBT	Computer	Virtual Machine	VMware device
High	192.0.2.24	Domainator	Handheld	Mobile Phone	iPhone XR
High	192.0.2.189	DC01-67hq3	Computer	Server	Poweredge R640
High	192.0.2.67	DC02LAER	Computer	Virtual Machine	VMware device
High	192.0.2.13	Jill-iPhone	Handheld	Mobile Phone	iPhone 7
High	192.0.2.176	DC01LASD	Computer	Virtual Machine	VMware device
High	192.0.2.34	maria-MBP	Computer	Laptop	MacBookPro

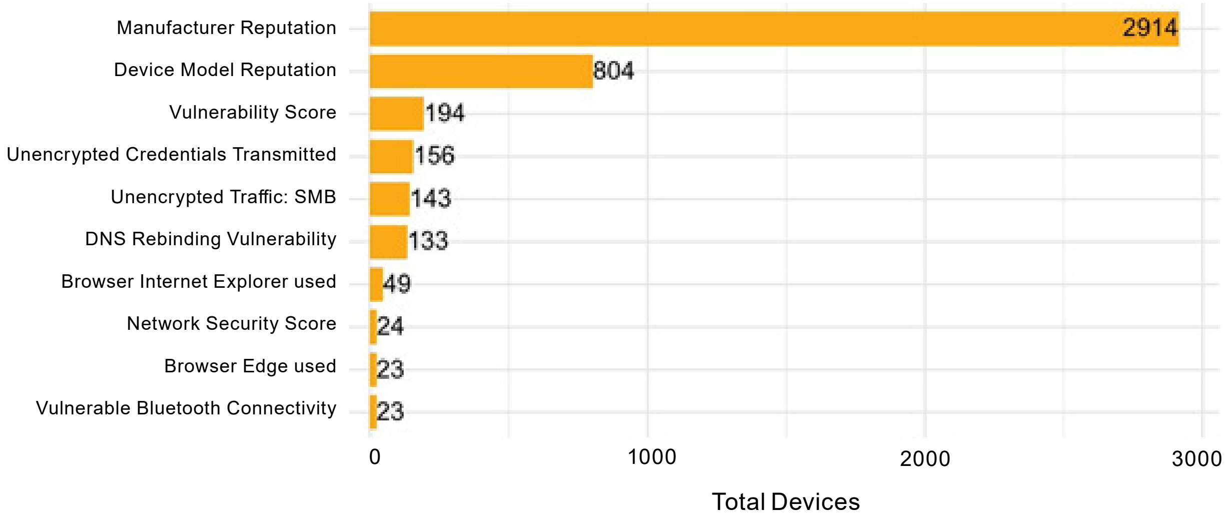
HIGH RISK UNMANAGED DEVICES

Risk	IP Address	Name	Category	Type	Model
High	192.0.2.168	SurgeryRoom1	Automations	HVACs	RPM Control
High	192.0.2.99	L989876	Medical Support	Workstations	GE Healthcare
High	192.0.2.251	PanelView Plus	Manufacturing	Scada Server	PanelView Plus
High	192.0.2.76	1756-EN2T	Manufacturing	Plc	1756-EN2T
High	192.0.2.100	Crestron device	Automations	Controller	PRO
High	192.0.2.2	e0cbbc99a1b6	Network	Access Point	Meraki MR33 Cloud Managed AP
High	192.0.2.199	CAM01	Imaging	IP Cameras	M3044-V
High	192.0.2.171	HOSPMRI01	Medical Diagnostic	MRIs	Optima MR450
High	192.0.2.11	ConfRoomTV	Display	Tv	Q60R QLED Smart 4K UHD TV (2019)
High	192.0.2.134	PRLDG1	Imaging	Printer	OfficeJet Pro 8720

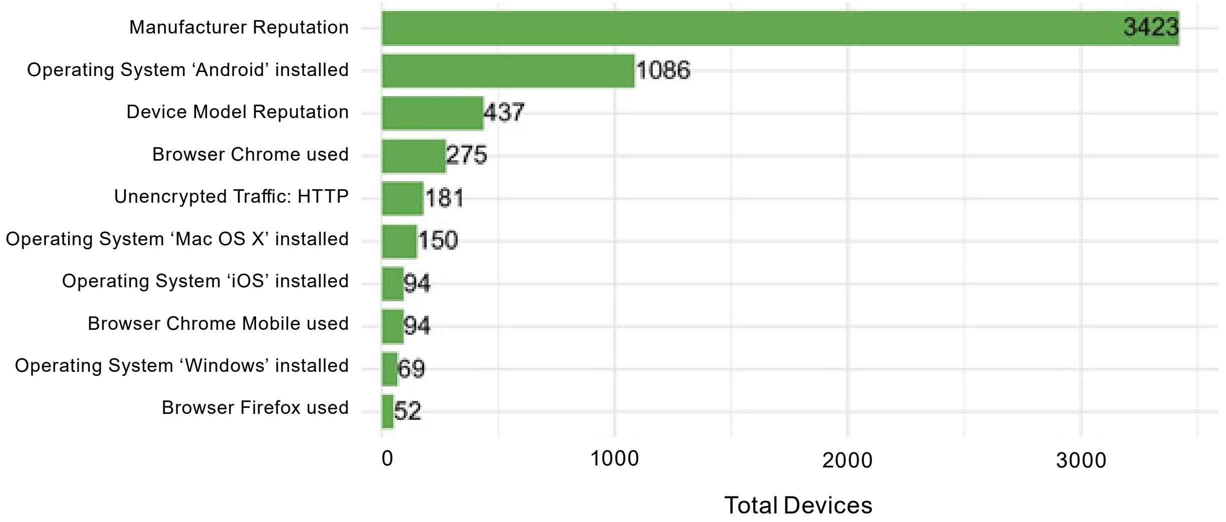
TOP 10 HIGH RISK FACTORS



TOP 10 MEDIUM RISK FACTORS



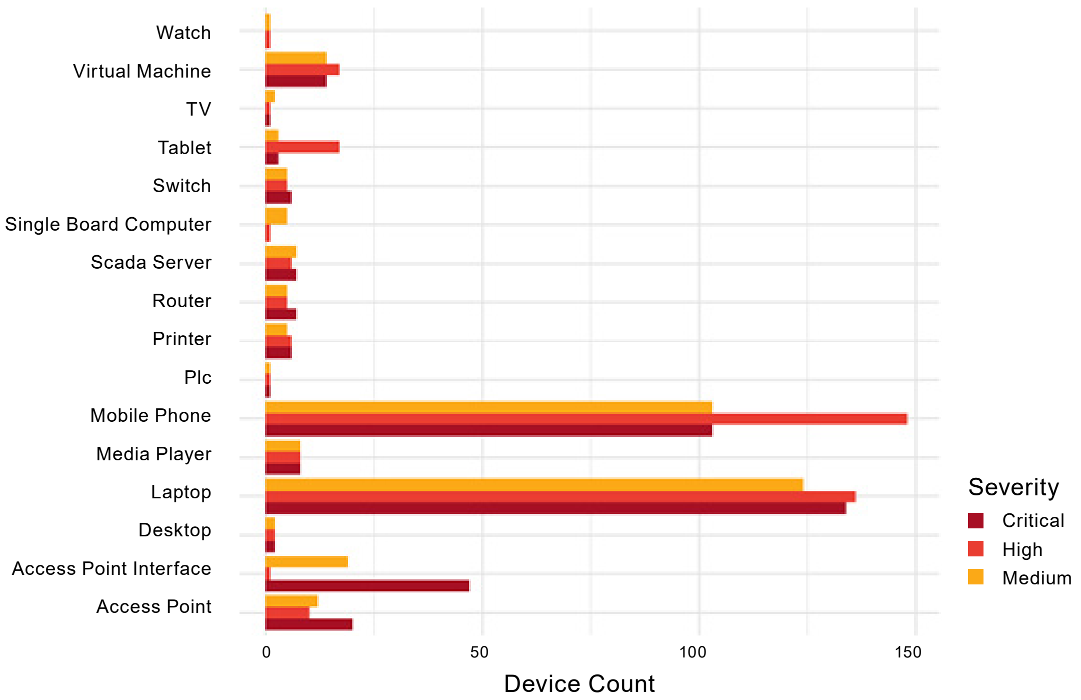
TOP 10 LOW RISK FACTORS



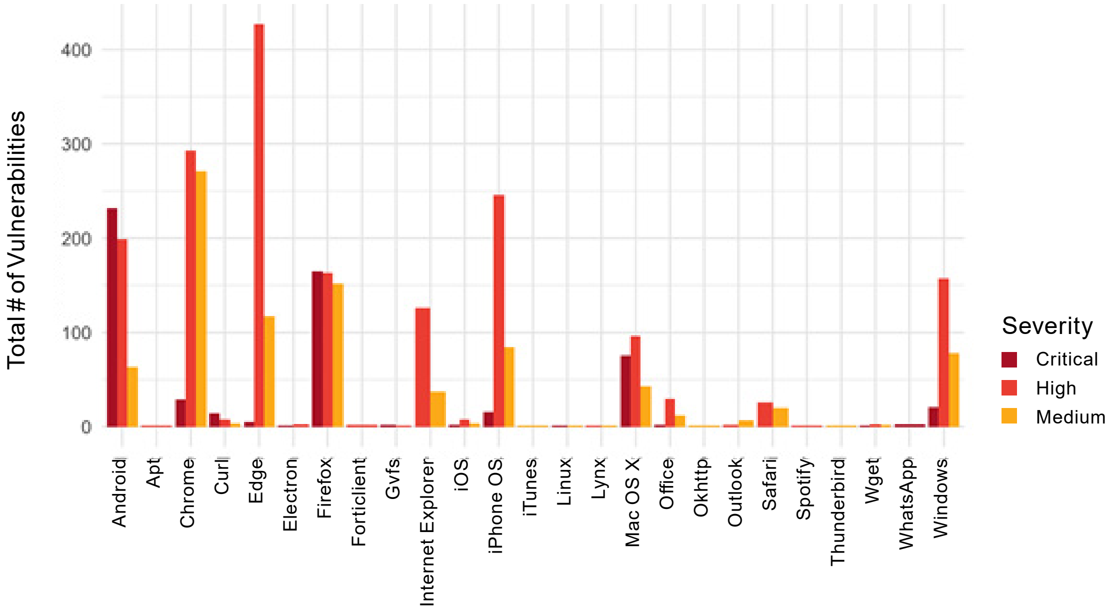
VULNERABILITIES

Unmanaged devices represent more risk to the environment as dwell time for vulnerabilities is much longer than for managed devices that receive OS and software updates. During the report timeframe, in Acme Corp's network 439 devices were found to have unpatched vulnerabilities, with a total of 3,263 unique CVEs.

TOTAL DEVICES WITH VULNERABILITIES BY DEVICE TYPE



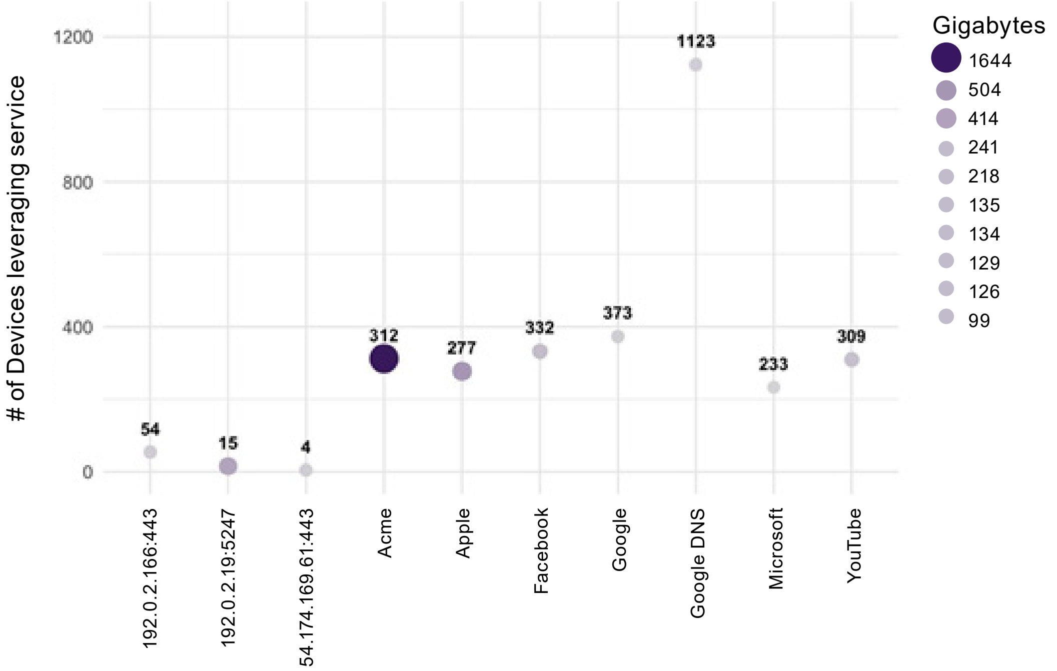
VULNERABILITIES BY ENTITY



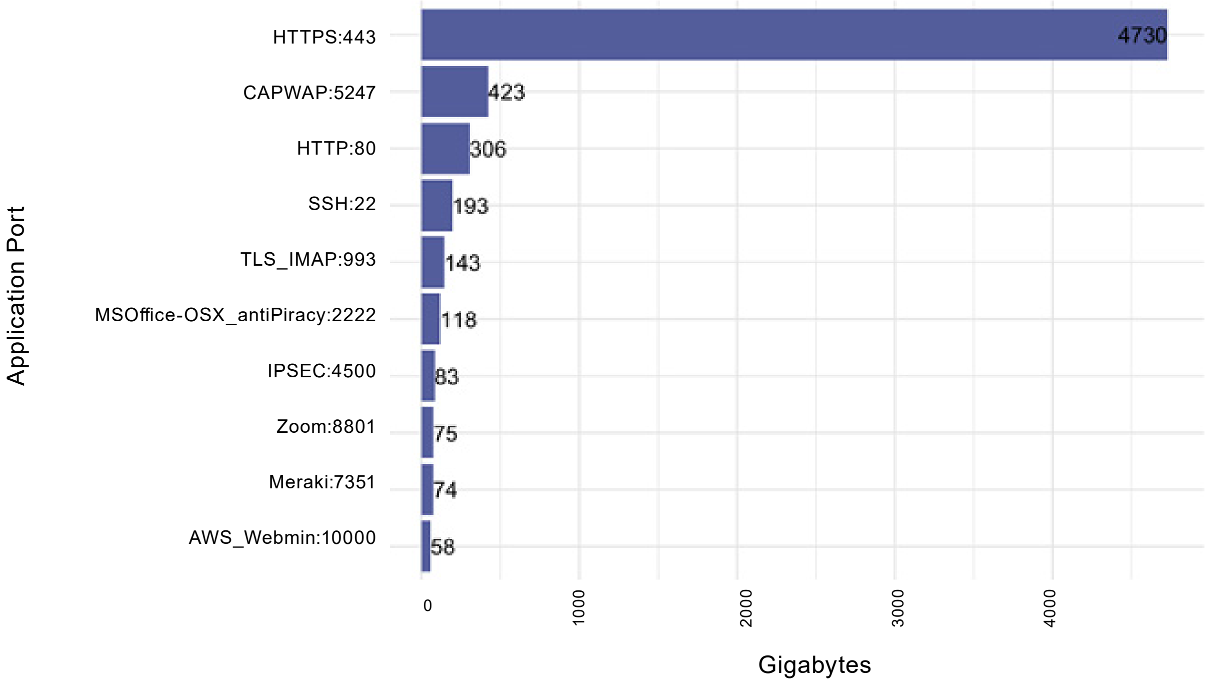
SERVICES

IoT Protect for Enterprise keeps a forensic history of all device communications. Traffic destined for another device on the network or to the Internet is referred to as a service. Below are examples of the top desination services and ports leveraged by devices in the Acme Corp network.

TOP 10 SERVICE DESTINATIONS



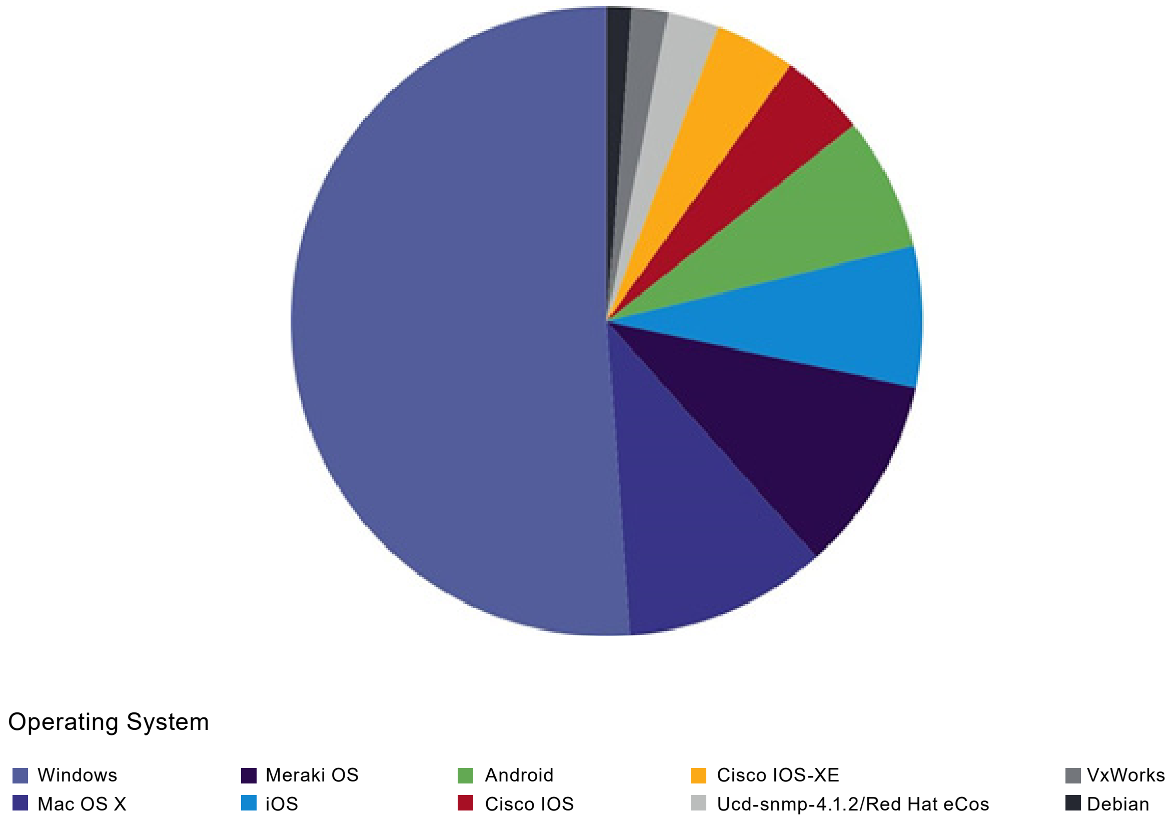
TOP 10 APPLICATION PORTS



OPERATING SYSTEMS

The table and graph below show the top 10 operating systems observed on devices connected to Acme Corp's network.

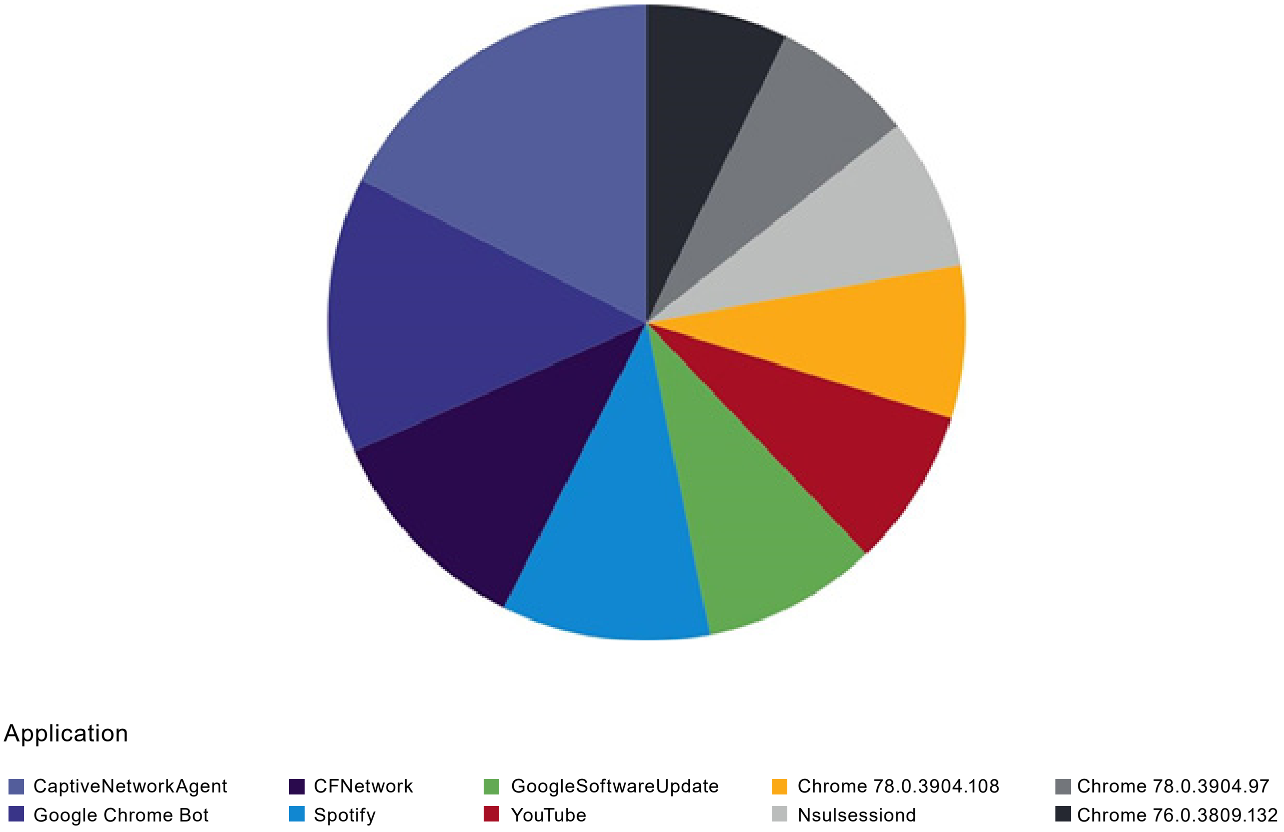
OS	Total
Windows	523
Mac OS X	106
Meraki OS	103
iOS	74
Android	70
Cisco IOS	45
Cisco IOS-XE	42
ucd-snmp-4.1.2/Red Hat eCos	27
VxWorks	19
Debian	13



APPLICATIONS

The table and graph below show the top 10 applications most commonly used by devices connected to Acme Corp’s network.

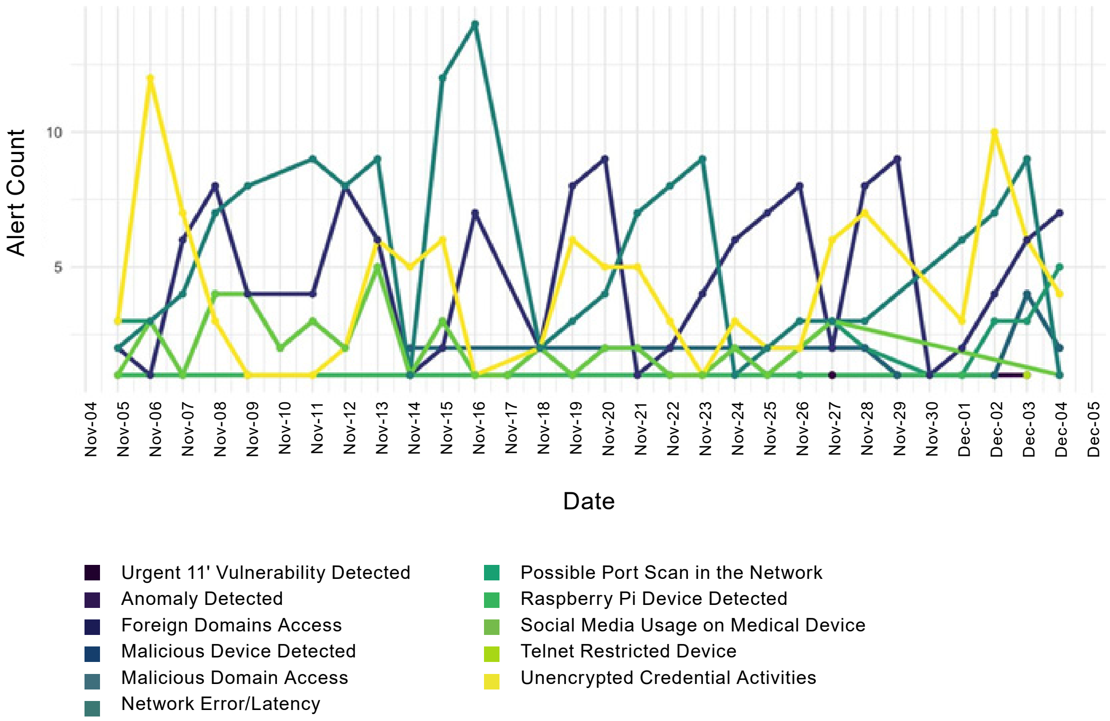
Application	Devices
CaptiveNetworkAgent	281
Google Chrome Bot	224
CFNetwork	176
Spotify	169
GoogleSoftwareUpdate	142
YouTube	129
Chrome 78.0.3904.108	124
nsurlsessiond	123
Chrome 78.0.3904.97	115
Chrome 76.0.3809.132	115



ALERTS

IoT Protect for Enterprise observed 541 alerts during the report timeframe. An alert is triggered when IoT Protect for Enterprise detects specific device behavior that matches criteria set in a user-, system- or anomaly-based policy.

OBSERVED ALERTS



Below are examples of the devices and associated alerts observed during the report timeframe in Acme Corp's network

DEVICES WITH MULTIPLE ALERTS

Name	IP Address	Category	Type	Model	Risk	Alerts
haggertys	192.0.2.45	Computer	Single Board Computer	Raspberry Pi	High	14
android-132q2roiy	192.0.2.10	Handheld	Product Scanner	Zebra TC700H	High	10
Johns-Samsung	192.0.2.56	Handheld	Mobile Phone	Galaxy S8	Medium	10
Jill-iPhone	192.0.2.13	Handheld	Mobile Phone	iPhone 7	High	8
CAMSD01	192.0.2.99	Imaging	IP Cameras	M3044-V	High	7
L989876	192.0.2.98	Medical Support	Medical Workstation	Viewer	Medium	4
sarams-iPhone	192.0.2.22	Handheld	Mobile Phone	iPhone XR	Medium	3
DC01-67hq3	192.0.2.189	Computer	Server	Poweregde R640	Medium	2
1756-EN2T	192.0.2.76	Manufacturing	Plc	1756-EN2T	High	2
burnout	192.0.2.33	Computer	Laptop	MacBook	Medium	2

HIGH RISK UNMANAGED DEVICES

Severity	ID	Title	IP.Address	Name	Type	Model
High	2363	Malicious Domain Access	192.0.2.45	haggertys	Single Board Computer	Raspberry Pi
High	2369	Malicious Domain Access	192.0.2.45	haggertys	Single Board Computer	Raspberry Pi
High	9202	'Urgent 11' Vulnerability Detected	192.0.2.76	1756-EN2T	Plc	1756-EN2T
High	2365	Malicious Domain Access	192.0.2.33	burnout	Laptop	MacBook
High	7287	Threat Detected WannaCry/ DoublePulsar	192.0.2.4	D019i9i	Dektop	ProDesk 600
High	2370	Possible Port Scan in the Network	192.0.2.45	haggertys	Single Board Computer	Raspberry Pi
High	8116	Threat Detected	192.0.2.10	android-132q2roiy	Product Scanner	Zebra TC700H
High	7611	Foreign Domains Access IOT device	192.0.2.99	Axis Device	IP Cameras	M3044-V
High	8116	'Urgent 11' Vulnerability Detected	192.0.2.109	P1345	Printer	Xerox WorkCentre
High	7611	Raspberry Pi Device Detected	192.0.2.45	haggertys	Single Board Computer	Raspberry Pi
High	7211	Telnet Restricted Device	192.0.2.168	SurgeryRoom1	HVACs	Reverse Pressure
Medium	8301	Social Media Usage On Medical Device	192.0.2.99	L989876	Medical Workstation	Viewer
Medium	7245	Unencrypted Credentials Activities	192.0.2.188	app6-dev	Server	Vmware device
Medium	2372	Foreign Domains Access	192.0.2.22	sarams-iPhone	Mobile Phone	iPhone XR
Medium	7266	Unencrypted Credentials Activities	192.0.2.189	DC01-67hq3	Server	Poweredge R640
Medium	7285	Unencrypted Credentials Activities	192.0.2.223	POLY01	VoiPs	Soundstation
Medium	8301	Social Media Usage On Medical Device	192.0.2.178	ULT01FL4	Ultrasounds	LOGIQF
Medium	2372	Foreign Domains Access	192.0.2.23	Joels-MBP	Laptop	MacBook
Low	2371	Network Error	192.0.2.1	BLDG2FL3CONF1	Access Points	AIR-CAP3702I-B- K9

CONTACT US

WORLDWIDE HEADQUARTERS

5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100
Email: info@checkpoint.com

U.S. HEADQUARTERS
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391 | 650-628-2000

UNDER ATTACK?
Contact our Incident Response Team:
emergency-response@checkpoint.com

WWW.CHECKPOINT.COM