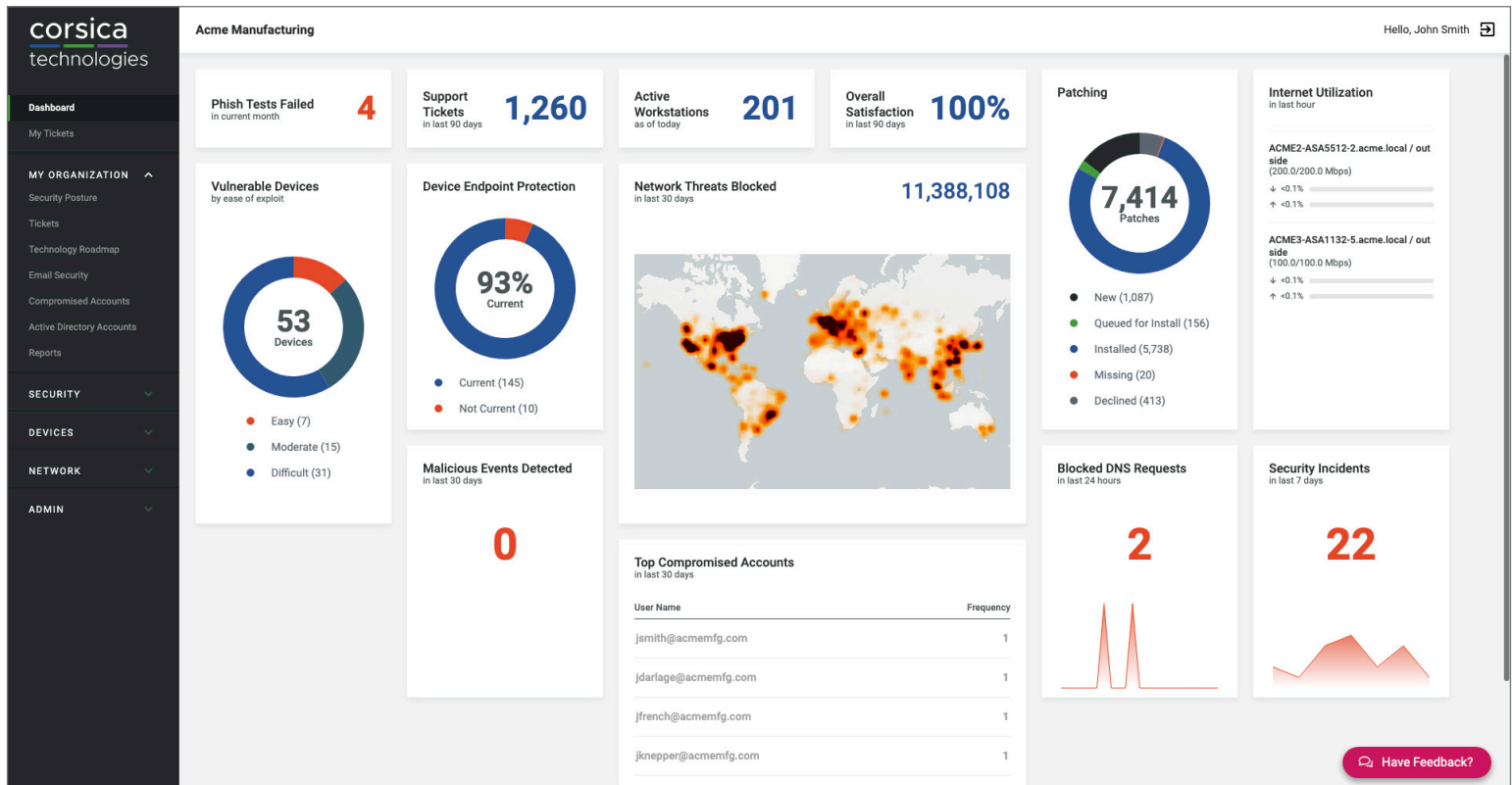


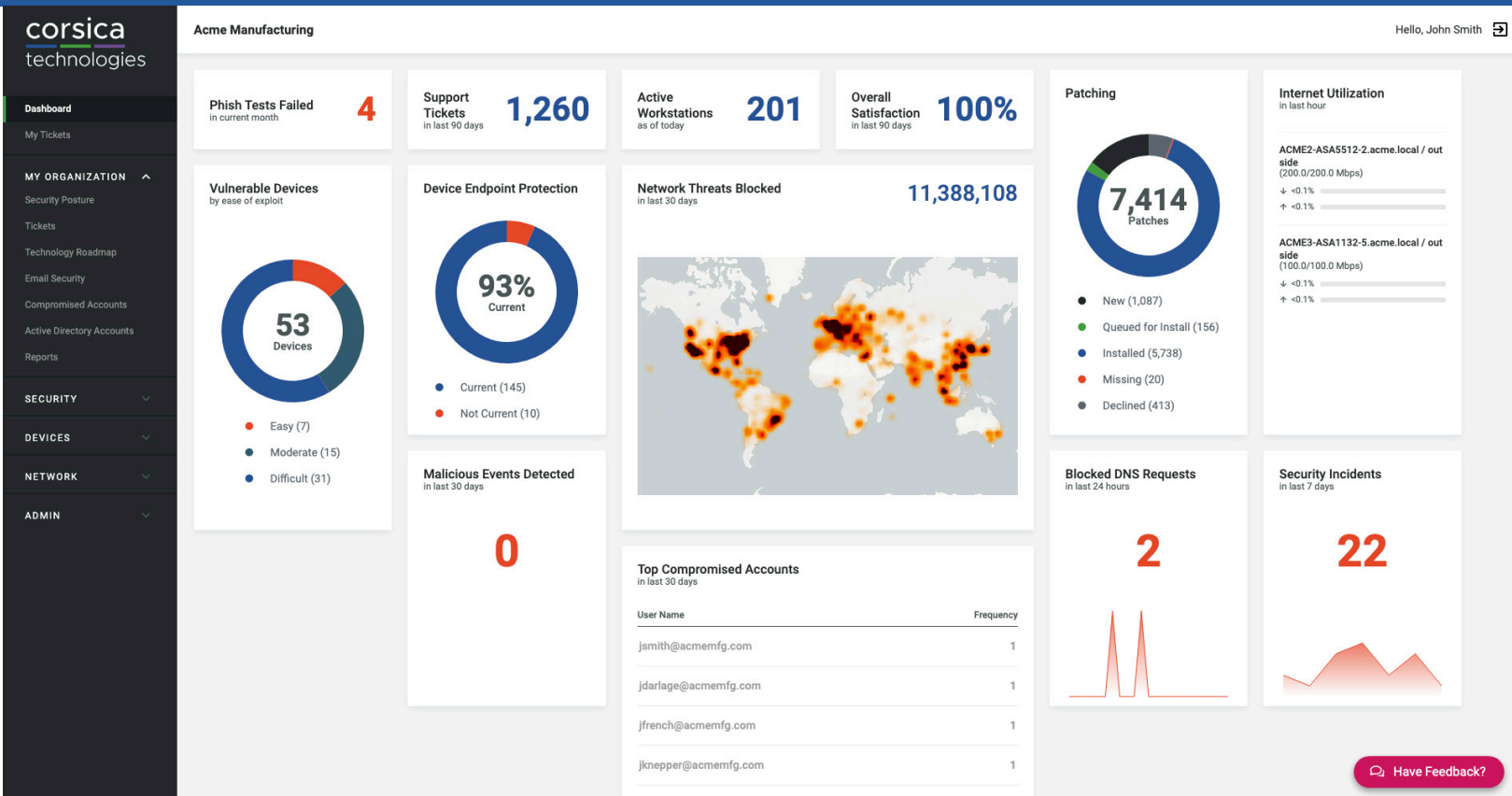
Client Portal Overview



Transparency. Accountability. Reliability. See your IT and cybersecurity in action.

When you partner with a technology provider you should expect more visibility, not less. The Corsica Technologies portal gives you access to your organization's cybersecurity and technology in real-time. Get visibility into your device endpoint protection, employees' behavior, support tickets, and more.

Main Dashboard



A snapshot of your organization's cybersecurity and IT health is available 24/7/365, right from your fingertips.

Features:

- Executive overview
- Gain insight into device patching and endpoint protection
- View email security information
- Quickly manage support tickets

Organizational Ticket Overview

corsica

technologies

Acme Manufacturing

Dashboard

My Tickets

MY ORGANIZATION

Security Posture

Tickets

Technology Roadmap

Email Security

Compromised Accounts

Active Directory Accounts

Reports

SECURITY

DEVICES

NETWORK

ADMIN

Tickets

Last updated 8/12/21 at 7:24 AM

Open (42)

Closed (2412)

Tickets Opened

in last 90 days at All Sites

2398

Site

All Sites

Showing 42 of 42 tickets

Search

Filter

Ticket #	Title	Status	Priority	Category	Type	Contact	Assigned To	Owned By	Created	Last Activity
812887	10.10.51.15 Failed Logon to Nonexistent Account admin	Scheduled	Standard	Alert	Alien Vault	Barry Allen		Corsica	08/12/2021	about 5 hours ago
810310	FW: Crowdstrike New Detection	Scheduled	Standard	Alert		Trey Williamson	Nicholas Martin	Corsica	08/10/2021	about 15 hours ago
812175	[Phish Alert] Beniversal Update: Thanks for giving us an A!	New	Low	Incident	Phishing	Pam Thomas		Corsica	08/11/2021	about 18 hours ago
812094	[Phish Alert] USCS LaVergne Appointment Desk	New	Low	Incident	Phishing	Candice Valencia		Corsica	08/11/2021	about 19 hours ago
812015	[Phish Alert] Hello Clinton, check out our new nitrile gloves, Bonjour Clinton découvrez nos nouve	New	Low	Incident	Phishing	Clinton Freed		Corsica	08/11/2021	about 20 hours ago
811988	[Phish Alert] RE: Warehouse Management Executives	New	Low	Incident	Phishing			Corsica	08/11/2021	about 20 hours ago
811723	[Phish Alert] RE: AWS - Strategic Playbook	New	Low	Incident	Phishing			Corsica	08/11/2021	about 22 hours ago
284291	Twice Weekly Meeting with Acme Team	Scheduled	Planned	Request		Joey Marx	Fred Bilton	Corsica	01/25/2021	1 day ago
810837	[Phish Alert] Access needs...	New	Low	Incident	Phishing	Eric Eifert		Corsica	08/10/2021	1 day ago
810815	[Phish Alert] A \$100 Amazon Card for Automotive and Transportation Contact	New	Low	Incident	Phishing	Emerson Roberts		Corsica	08/10/2021	1 day ago

Easily access your organization's service tickets. Want to view the specifics of a particular ticket? Just click on a ticket to pull up all the details and communication history.

Features:

- Review open support tickets
- Quickly check the communication history for a ticket
- Add notes and attachments to tickets

Technology Roadmap

- Dashboard
- My Tickets
- MY ORGANIZATION**
- Security Posture
- Tickets
- Technology Roadmap**
- Email Security
- Compromised Accounts
- Active Directory Accounts
- Reports
- SECURITY**
- DEVICES**
- NETWORK**
- ADMIN**

Acme Manufacturing

Technology Roadmap

[To Do \(6\)](#)
[Done \(3\)](#)
[Archived \(0\)](#)

New Roadmap Item

Showing 6 of 6 roadmap items

Importance	Project	Category	Status	Next Step Assigned to	Budget	Anticipated Start ↑
● Recommended	WAN Redesign	Applications	Approval Needed	Thomas Cartwright	<div><div style="width: 25%;"></div></div>	August 2019
● Recommended	Windows Server 2008 End of Life	Data Center	Approval Needed	Thomas Cartwright	<div><div style="width: 25%;"></div></div>	December 2020
● Recommended	Windows 7 End of Life	Endpoints	Approval Needed	Thomas Cartwright	<div><div style="width: 25%;"></div></div>	December 2020
● Recommended	Mobile Device Management (MDM)	Security	Approval Needed	Thomas Cartwright	<div><div style="width: 25%;"></div></div>	January 2021
● Recommended	Security Awareness Training and Testing	Security	Approval Needed	Thomas Cartwright	<div><div style="width: 25%;"></div></div>	January 2021
● Recommended	Disaster Revcovery (DR) Planning	Disaster Recovery	Approval Needed	Thomas Cartwright	<div><div style="width: 25%;"></div></div>	July 2021

Download PDF

Be better prepared with a list of important upcoming projects, including what to expect when it comes to budget.

Features:

- View recommended technology initiatives
- Plan for current and long-term projects
- Align budgets with goals
- Understand the timing of budget items
- Include your hardware, software, and all IT-related projects

Gain full transparency into how your employees fare against email phishing tests, identifying risky behavior before it's too late.

- Understand which employees repeatedly fail phishing tests
- See how aware your users are in today's threat landscape
- Gauge which employees need additional cybersecurity training
- View how many tests your employees have received

Compromised Account Report

corsica

technologies

Dashboard

My Tickets

MY ORGANIZATION

Security Posture

Tickets

Technology Roadmap

Email Security

Compromised Accounts

Active Directory Accounts

Reports

SECURITY

DEVICES

NETWORK

ADMIN

Acme Manufacturing

Hello, John Smith

Choose a start date

8/12/2020

Choose an end date

8/12/2021

Compromised Accounts

Last updated 8/11/21 at 10:01 PM

Review Status

190

Accounts

New (0)

In Progress (0)

Completed (190)

Top Compromises by Website

Source	Frequency
adapt.io - Nov, 2018	57
gonitro.com	11
houzz.com - May 2018	8
parkmobile.io	7
drivesure.com	5
homechef.com	5

Top Compromised Accounts

User Name	Frequency
gchapman@acmemfg.com	10
dstreich@acmemfg.com	9
astreicher@acmemfg.com	8
rfrench@acmemfg.com	7
twolf@acmemfg.com	6
tchapman@acmemfg.com	6

Showing 190 of 190 compromised accounts

Search

Filter

User Name

Type

Source

Website

Date Occurred

Date Found

Status

rfrench@acmemfg.com	Not Disclosed	Id Theft Forum		8/5/2021	8/6/2021	Completed
dwilliamson@acmemfg.com	Data Breach	Id Theft Forum		7/13/2021	7/16/2021	Completed
dstreich@acmemfg.com	Data Breach	Id Theft Forum		7/13/2021	7/16/2021	Completed
gchapman@acmemfg.com	Data Breach	Id Theft Forum		7/13/2021	7/16/2021	Completed
twolf@acmemfg.com	Data Breach	Id Theft Forum		7/13/2021	7/16/2021	Completed
astreicher@acmemfg.com	Data Breach	Id Theft Forum		7/13/2021	7/16/2021	Completed

Stay on top of where and when your employees' credentials are exposed online.

Features:

- Identify when and where threats are occurring
- View which accounts have been compromised
- Review resolution status

Devices Overview

corsica

technologies

Dashboard

My Tickets

MY ORGANIZATION

SECURITY

DEVICES

Devices Overview

Patching

Endpoint Protection

Vulnerabilities

Vulnerabilities (Basic)

DNS Activity

Malware Activity

Server Utilization

NETWORK

ADMIN

Acme Manufacturing

Devices Overview

Last updated 8/12/21 at 7:47 AM

Total Devices

currently active at All Sites

673

Site

All Sites

Workstations (524)

Servers (149)

Network Devices (0)

Other (0)

Showing 524 of 524 workstations

Search Workstations

Filter

Name/Hostname	IP Address(es)	OS	Device Model	Last Login	Last User
dfeipel	172.20.9.1	Microsoft Windows 10 Pro	Latitude 5591	6/15/2021	dfeipel
ACME-ADP	10.12.45.145	Microsoft Windows 10 Pro	Surface Pro 4	6/30/2021	ADP
ACME-ASUEVER	10.12.50.165	Microsoft Windows 10 Pro	Latitude 5501	8/4/2021	asuever
ACME-BDRV	10.12.50.59	Microsoft Windows 10 Pro	OptiPlex 5060	8/10/2021	cheichel
ACME-BDRV2	10.12.50.73	Microsoft Windows 10 Pro	OptiPlex 5080	8/11/2021	cmason
ACME-CLRK1	10.12.50.57	Microsoft Windows 10 Pro	OptiPlex 5060	8/11/2021	mwallace
ACME-CLRK2	10.12.50.56	Microsoft Windows 10 Pro	OptiPlex 5060	8/11/2021	msmith
ACME-CLRK3	10.12.50.58	Microsoft Windows 10 Pro	OptiPlex 5060	8/11/2021	andock
ACME-DD18	10.12.50.53	Microsoft Windows 10 Pro	OptiPlex 5060	8/4/2021	andock
ACME-DD35	10.12.50.54	Microsoft Windows 10 Pro	OptiPlex 5060	8/11/2021	dkise
ACME-DREYHER	10.12.50.166	Microsoft Windows 10 Pro	Latitude 5520	8/3/2021	dreyher
ACME-DSNODDY	10.12.250.21	Microsoft Windows 10 Pro	Latitude 5491	7/29/2021	dsnoddy
ACME-FRICK	10.12.31.50	Microsoft Windows 10 Pro for Workstations	Precision 5820 Tower	7/12/2021	Frick
ACME-ERNTDSK	10.12.50.65	Microsoft Windows 10 Pro	OptiPlex 5050	8/11/2021	djohnson

View device details across your organization, including workstations, servers and network devices.

Features:

- Review device details, activity and health information
- View device inventory, warranty and lifecycle

Server Utilization Report

corsica

technologies

Dashboard

My Tickets

MY ORGANIZATION

SECURITY

DEVICES

Devices Overview

Patching

Endpoint Protection

Vulnerabilities

Vulnerabilities (Basic)

AVS Activity

Malware Activity

Server Utilization

NETWORK

ADMIN

Acme Manufacturing

Hello, John Smith

Server Utilization

Last updated 8/12/21 at 7:48 AM

Processor

Disk

Physical Memory

Virtual Memory

Processor Utilization

amudb

ajodb

afrdb

aexacq_dvr

aMURP

Average Processor Utilization per Device

last 30 days

Search

Name	Processor(s)	Cores	Sockets	Avg. Utilized %
aexacq_dvr	AMD EPYC 7261 8-Core Processor	8	1	62.6%
amudb	Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz	4	1	32.8%
afrdb	Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz	8	1	29.5%
aMURP	Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz	4	1	27.3%
avfr10	Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz	8	1	24.7%

View the performance of your servers all in one place.

Features:

- Gain insight into the workload and activity on your servers
- See processor, disk and memory utilization

Endpoint Protection

corsica

technologies

Dashboard

My Tickets

MY ORGANIZATION

SECURITY

DEVICES

Devices Overview

Patching

Endpoint Protection

Vulnerabilities

Vulnerabilities (Basic)

DNS Activity

Malware Activity

Server Utilization

NETWORK

ADMIN

Acme Manufacturing

Hello, John Smith

Endpoint Protection

Last updated 8/12/21 at 7:47 AM

There are 10 devices that are not current. [View devices](#)

Devices Current

as of date selected

93%

As of Today

Showing 155 of 155 devices

Search

Filter

Device Name	Category	OS	Version	Last Seen	Status
ACME-10223	Workstation	Microsoft Windows 10 Enterprise	6.24.13806.0	6/30/2021	Not Current
ACME-SD-ET	Workstation	Microsoft Windows 10 Pro	6.24.13806.0	6/30/2021	Not Current
ACME-NHCLG3K	Workstation	Microsoft Windows 10 Pro	6.24.13806.0	7/01/2021	Not Current
ACME-EXP-EW2	Workstation	Microsoft Windows 10 Enterprise	6.24.13806.0	7/01/2021	Not Current
ACME-0BV25RS	Workstation	Microsoft Windows 10 Enterprise	6.24.13806.0	7/06/2021	Not Current
ACME-HN66QH2	Workstation	Microsoft Windows 10 Enterprise	6.24.13806.0	7/06/2021	Not Current
ACME-10450	Workstation	Microsoft Windows 10 Pro	6.24.13806.0	7/07/2021	Not Current
ACME-BI	Server	Microsoft Windows Server 2016 Standard	6.24.13806.0	7/09/2021	Not Current
ACME-EXCHANGE	Server	Microsoft Windows Server 2016 Standard	6.24.13806.0	7/09/2021	Not Current
ACME-20660	Workstation	Microsoft Windows 10 Pro	6.25.13909.0	7/13/2021	Current
ACME-S1240DESKTOP	Workstation	Microsoft Windows 10 Enterprise	6.25.13909.0	7/16/2021	Current
ACME-N3NHU0F	Workstation	Microsoft Windows 10 Enterprise	6.25.13909.0	7/16/2021	Current
ACME-682ANRS	Workstation	Microsoft Windows 10 Pro	6.25.13909.0	7/16/2021	Current
jsmith-vm	Workstation	Microsoft Windows 10 Pro	6.25.13909.0	7/17/2021	Current
ACMFNVWKS03	Workstation	Microsoft Windows 10 Pro	6.25.13909.0	7/21/2021	Current

Understand your company’s device endpoint protection status and identify any devices that are out of date.

Features:

- View device endpoint protection statuses
- Quickly identify devices that need attention
- View monthly snapshots

Corsica Technologies © 2021. All Rights Reserved.

v3 082021

Security Incidents

corsica

technologies

Dashboard

My Tickets

MY ORGANIZATION

SECURITY

Incidents

DEVICES

NETWORK

ADMIN

Acme Manufacturing

Hello, John Smith

Security Incidents

Last updated 8/12/21 at 4:03 AM

Activity Period

Last 7 Days

Incidents

for selected activity period

22

Date	Incidents
8/6/21	2
8/7/21	1
8/8/21	4
8/9/21	5
8/10/21	2
8/11/21	4
8/12/21	1

Top Incidents by Category

Uncategorized	11
Credential Access	10
Persistence	3
Impact	0
Exfiltration	0

Showing 22 of 22 security incidents

Search

Filter

Rule Name	Attack Type	Category	Target Device	Time	Ticket #	Ticket Status
Failed Logon to Nonexistent Account	Brute Force	Credential Access	acme-file22.acme.local	8/12/21 3:06am	812945	Resolved
Dropbox		Uncategorized	172.29.35.203	8/11/21 2:42pm	812349	Resolved
Critical IPS Event		Uncategorized	10.101.100.116	8/11/21 3:45am	811454	Resolved
Critical IPS Event		Uncategorized	10.101.100.116	8/11/21 3:43am	811454	Resolved
Failed Logon to Nonexistent Account	Brute Force	Credential Access	acme-file21.acme.local	8/11/21 3:06am	811434	Resolved
AWS IAM Credentials	Account Manipulation	Credential Access, Persistence	iam.amazonaws.com	8/10/21 3:15am	810075	Resolved
Failed Logon to Nonexistent Account	Brute Force	Credential Access	acme-file18.acme.local	8/10/21 3:06am	810051	Resolved
Critical IPS Event		Uncategorized	10.101.100.116	8/9/21 10:27pm	809952	Resolved
EBS Snapshot		Uncategorized	ec2.amazonaws.com	8/9/21 3:45pm	809610	Resolved

View security incident activity in real-time as the Corsica Technologies team identifies and remediates threats against your network and devices.

Features:

- View security incident activity over time
- Gain visibility into resolution statuses and associated tickets
- View incidents by category and attack type

Device Vulnerabilities

corsica

technologies

Dashboard

My Tickets

MY ORGANIZATION

SECURITY

DEVICES

Devices Overview

Patching

Endpoint Protection

Vulnerabilities

Vulnerabilities (Basic)

DNS Activity

Malware Activity

Server Utilization

NETWORK

ADMIN

Acme Manufacturing

Hello, John Smith

Vulnerabilities

Last updated 8/11/21 at 11:02 AM

Vulnerable Devices

by ease of exploit

53

Devices

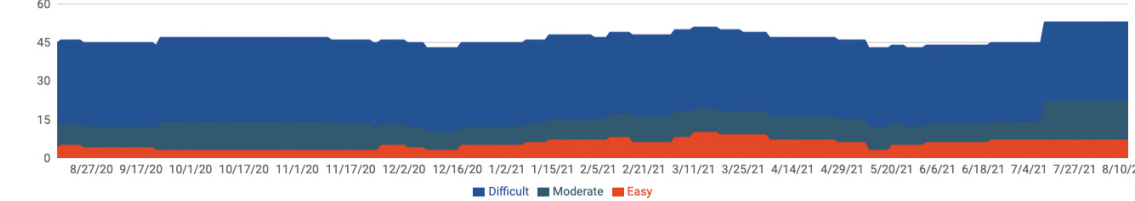
Easy (7)

Moderate (15)

Difficult (31)

Vulnerable Device History

by ease of exploit



Showing 174 of 174 vulnerabilities

Filter

Search

Device Name	IP Address	OS	Malware Vulnerable	Published Exploits	Vulnerabilities	Risk Score ↓	Last Scan
ACME-EXP-TP0D	172.29.100.15/32	Windows 8.1 Enterprise Edition			447	136,116	8/5/2021
ACME-BRIDGE	172.29.224.130/32	Windows Server 2016 Standard Edition			355	93,746	8/5/2021
ACME-ADMINAC	172.29.35.55/32	Windows 10 Enterprise Edition			85	28,263	6/17/2021
ACME-TECHS-SS	172.29.0.103/32	Windows 10 Professional Edition			62	21,311	8/5/2021
ACME-SDWDSP-01	172.29.0.136/32	Windows 10 Enterprise Edition			79	18,561	8/5/2021
ACME-DC01.acme.local	172.29.96.75/32	Windows Server 2016 Standard Edition			65	14,907	8/5/2021
ACME-DC02.acme.local	172.29.96.92/32	Windows Server 2016 Datacenter			64	14,169	8/5/2021

Track device vulnerabilities and risk profile over time.

Features:

- View all devices with identified vulnerabilities, ranked by ease of exploit
- Get additional details on vulnerabilities and published exploits
- Track changes in risk profile over time