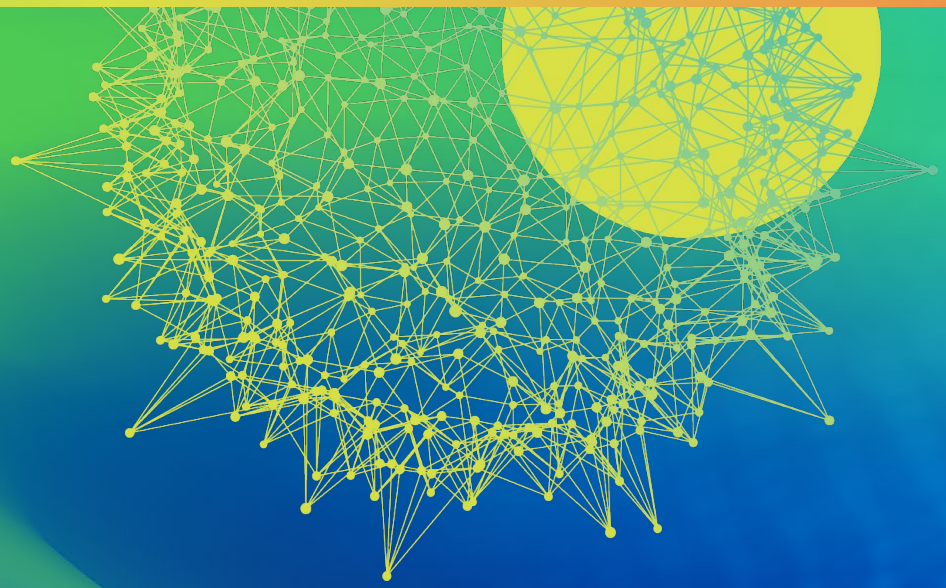


SKYBOX SECURITY

# Vulnerability and threat trends report 2023

Record-breaking year for vulnerabilities and exploits driving the need for improved exposure management.

# Contents

# Introduction

**Mordecai Rosen, CEO, Skybox Security**

**The latest edition of the World Economic Forum's annual *Global Risks Report* marks a sobering milestone: for the first time in the report's history, "widespread cybercrime and cyber insecurity" now ranks among the top ten threats facing humanity, alongside perennial worries like natural disasters, war, and economic instability.**[1]

It's a recognition—belated, some would say—that the wall between the virtual and physical worlds has fallen. In today's era of pervasive digitization and hyperconnectivity, cyberattacks can have far-reaching consequences that touch every aspect of our lives. From financial networks and critical infrastructure to healthcare systems and government, every sector faces massive risks. The advent of generative AI will only add to the perils.

Our findings in this year's *Skybox Vulnerability and Threat Trends Report*, detailed below, make the urgency of the situation abundantly clear. Vulnerabilities have skyrocketed, eclipsing all previous records. Attacks are increasing in velocity and impact. Threat actors are targeting more sensitive assets and inflicting more damage. They are better organized—backed increasingly by large crime rings and nation-states—and are employing more sophisticated tools and tactics, such as a growing assortment of backdoor malware and advanced persistent threat (APT) attacks.

While the threat landscape expands at a head-spinning rate, cybersecurity teams are being stretched thin by talent shortages, budget constraints, and a host of new regulatory requirements. For once, the phrase "perfect storm" is more than a cliché.

The writing is on the wall. Traditional reactive approaches to cybersecurity—waiting until vulnerabilities are reported and then scrambling to scan and patch every instance—are more outmoded by the day. There are far too many vulnerabilities, it takes too long to find them and close them, and many are unpatchable in any case. Understaffed cybersecurity organizations can't keep up.

> **"Fortunately, a new class of solution has emerged…It's known as continuous exposure management."**

In place of brute force, CISOs and their teams need precision guidance: a way to accurately identify and prioritize the most pressing business risks, anticipate impacts, and mitigate them proactively while offloading teams and making optimal use of scarce resources. Fortunately, a new class of solution has emerged in recent years that's designed to do just that. It's known as continuous exposure management, and we'll take a closer look at its capabilities and benefits in the final section of this report.

[1] *The Global Risks Report 2023*, World Economic Forum, January 11, 2023.

# Key findings

## New vulnerabilities are soaring

The National Vulnerability Database (NVD) added 25,096 new vulnerabilities in 2022. That's the largest number of vulnerabilities ever published in a single year, and it's a 25% jump from the 20,196 new vulnerabilities reported in 2021. In other words, vulnerabilities aren't just rising; they're rising faster.

## Cumulative vulnerabilities are nearing 200,000

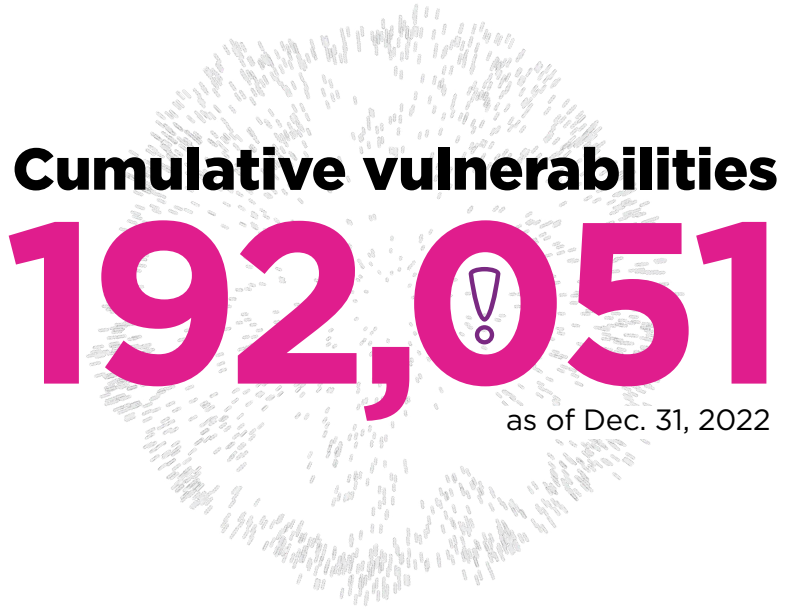
By the end of 2022, the total number of vulnerabilities cataloged in the NVD hit 192,051, and the count will soon surpass 200,000. That's 200,000 unique vulnerabilities (aka CVEs: critical vulnerabilities and exposures). The number of vulnerability instances out in the world is, of course, far greater; some large enterprises have millions of them.

## Most new vulnerabilities are medium and high severity

We found that 80% of vulnerabilities reported in 2022 were medium or high severity. Only 16% were deemed critical, but that's hardly reassuring. Severity does not equal risk, which depends on a variety of factors. Many threat actors specifically target less severe weaknesses, exploiting these vulnerabilities to land (gain ingress to a system) and expand (move laterally and escalate attacks).

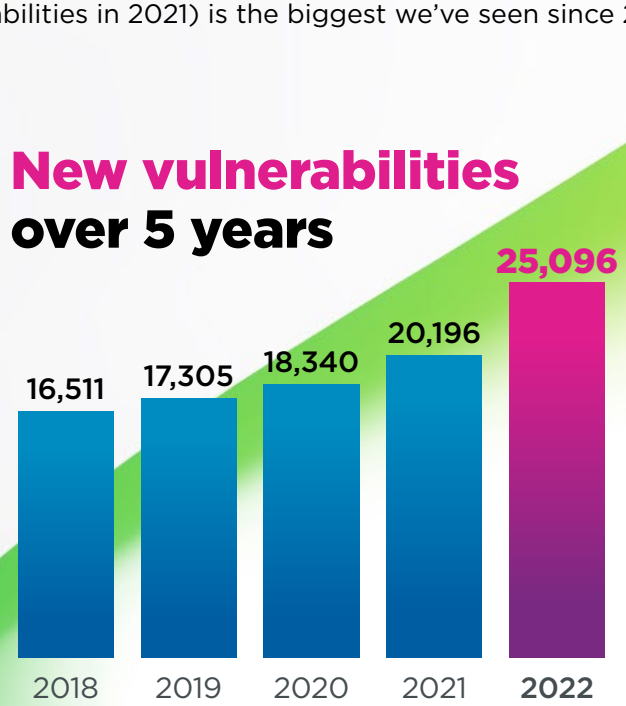
## Backdoor is the fastest-growing malware category

Backdoor malware was the fastest-growing type of malware we tracked in 2022, outpacing categories such as cryptojacking and ransomware, which topped the malware charts in last year's Skybox report. Backdoors enable hackers to bypass normal authentication and gain unauthorized access to systems. The surge in backdoor malware is one of several signs pointing to an increase in advanced persistent threats (APTs). APTs are complex, multi-stage attacks in which intruders enter a system surreptitiously and linger for extended periods, during which they may install malware, steal information, conduct espionage, disrupt operations, and more. APTs are typically the work of highly skilled and well-resourced groups such as cybercrime organizations and nation-states. The uptick in APTs reflects the growing sophistication and ambitions of threat actors.



# New vulnerabilities: another record year

The 25,096 new vulnerabilities published in 2022 set an all-time record for a single year. That's up from the 20,196[2] new vulnerabilities logged in 2021, itself a record at the time. The 25% year-over-year rise (new vulnerabilities in 2022 versus new vulnerabilities in 2021) is the biggest we've seen since 2017.




The surge in new vulnerabilities stems from a number of factors. On the positive side, software and hardware vendors—compelled by tighter regulations and policies—may be getting better at recognizing and disclosing existing security bugs in their products. On the other hand, new bugs are being introduced into products at a faster rate, as rapid technological change leads to more mistakes in product development. Accelerating digital transformation and cloud migration (driven in part by the COVID-19 pandemic and shift to remote work), rushed development schedules, inadequate validation, and greater software complexity are all creating more opportunities for error.

At the same time, the growing interdependencies and interconnections among systems are opening new entry points and enabling new modes of attack. As technology and vectors evolve, vulnerabilities are cropping up in areas that were formerly thought safe. For example, one of the "new" security flaws reported in 2022 was an integer overflow in 22-year-old SQLite database library software. The bug wasn't considered exploitable in the 32-bit computing era when the software was written but became vulnerable as 64-bit architectures proliferated.[3]

The blizzard of new vulnerabilities comes on top of a mountain of previously-reported issues. By the end of 2022, the total number of unique CVEs identified in the NVD hit 192,051. The tally is likely to exceed 200,000 by mid-2023. These vulnerabilities can persist in organizations for years, ripe for exploitation and targeted by an ever-expanding arsenal of malware. Large enterprises can have hundreds of thousands or even millions of total vulnerability instances, spread across far-flung attack surfaces encompassing IT and OT environments, on-premises systems, public and private cloud services, and remote endpoints. All of this has made traditional, blanket approaches to vulnerability management—aka "scan and patch everything"—increasingly futile.

[2] This 2021 figure is slightly higher than the one we quoted in last year's *Skybox Vulnerability and Threat Trends Report*, due to subsequent revisions of the NVD.
[3] *22-Year-Old Vulnerability Reported in Widely Used SQLite Database Library*, Hacker News, October 25, 2022.

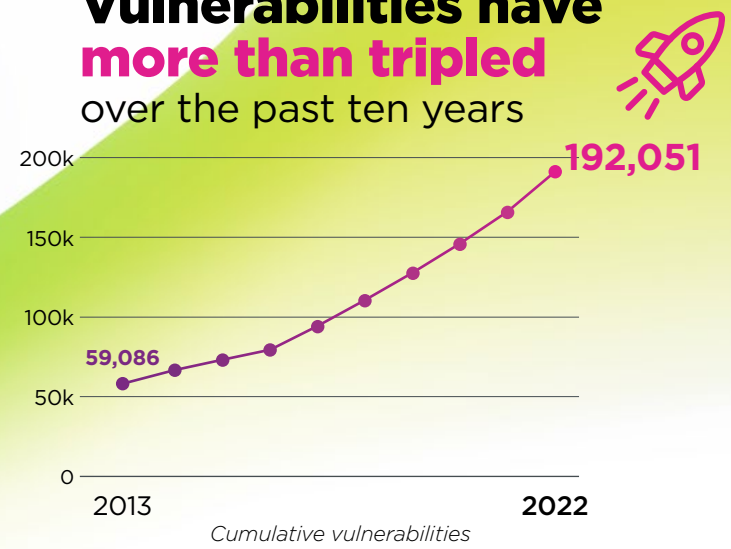
# The threat landscape is evolving rapidly

As vulnerabilities multiply inside organizations, threats are intensifying externally. Cybercrime is a trillion-dollar-plus industry, fed by a thriving ecosystem of vendors, tools, and services catering to a wide range of threat actors, from novices to major crime organizations.[4] As the World Economic Forum states (WEF), "Lower barriers to entry for cyber threat actors, more aggressive attack methods, a dearth of cybersecurity professionals and patchwork governance mechanisms are all aggravating the risk."[5]

The range of cybercrime targets and tactics has expanded dramatically, and cyberattacks hit an all-time high in 2022, taking a mounting toll on businesses, governments, and institutions worldwide.[6] Particular areas of concern include:

## Supply chain attacks

By compromising a single widely used product or software component from a trusted vendor, supply chain attackers can infect many organizations at once in ways that are very hard to detect and repel. That's what happened in the infamous Solar Winds attack reported in late 2020, which is believed to have impacted thousands of organizations. In a large-scale study of data breaches, IBM found that a whopping 19% "occurred because of a compromise at a business partner."[7] Some analysts expect supply chain attacks to rise sharply in the next few years, impacting nearly half of all businesses by 2025.[8]




## Attacks on network devices

2022 saw a wave of incidents that exploited vulnerabilities in firewalls from companies including Fortinet and Sophos, as well as attacks on other network technology such as load balancers and traffic managers.[9] [10] As with OT attacks, many attacks on network devices exploit old, unpatched vulnerabilities, which are still widespread because of the difficulty of scanning and patching active network devices.

## OT and critical infrastructure attacks

Operational technology, used to monitor and control physical systems in sectors such as energy, public utilities, manufacturing, building automation, transportation systems, and healthcare, is an increasingly frequent target for a wide range of threat actors, from ransom-seeking cybercriminals to hostile nation-states. It's gotten so bad that, per the WEF, "Attacks on critical infrastructure have become the new normal."[11]

[4] *Cybercriminals Raking in $1.5 Trillion Every Year*, TechRepublic, March 12, 2020.
[5] *The Global Risks Report 2022*, World Economic Forum, January 11, 2022.
[6] *Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks*, Dark Reading, January 5, 2023.
[7] *Cost of a Data Breach Report*, IBM, July 2022.
[8] *The Next Generation of Supply Chain Attacks Is Here to Stay,* Dark Reading, November 18, 2022.
[9] *Hackers Exploited Zero-Day Vulnerability In Sophos Firewall—Patch Released*, The Hacker News, September 24, 2022.
[10] *CISA adds Fortinet CVE to vulnerability catalog after attacks escalate*, Cybersecurity Dive, October 12, 2022.
[11] *A Boiling Cauldron: Cybersecurity Trends, Threats, And Predictions For 2023*, Forbes, November 23, 2022.

## Ransomware attacks

After several years of breakneck growth, the volume of ransomware attacks may have slowed in 2022, according to some sources.[12] [13] Nonetheless, many of the year's most costly cyberattacks involved ransomware, and the constant threat of ransomware is one of the factors pushing up the price of cyber insurance.[14]

## New methods and tools

Threat actors continue to up their game with a variety of cunning new tactics, techniques, and procedures (TTPs):

- Advanced persistent threats (APTs), used by nation-state actors and organized cybercriminals, are on the rise.[15] [16]
- Malware developers are taking malicious programs originally written in older languages like C and C++ and rewriting or recompiling them in newer languages such as Rust and Nim, making them less detectable by anti-virus software, firewalls, and endpoint detection and response (EDR) solutions.[17]
- Malware-as-a-service and cybercrime-as-a-service are booming.
- Malware is becoming more versatile, with individual packages designed to perform a wider variety of exploits.
- Malware is also getting more destructive. For example, Fortinet reports a big jump in "wiper malware": malicious programs designed to destroy data.[18]

> **"Amid the rising frequency and severity of ransomware claims, cyber insurance pricing in the United States rose by 96% in the third quarter of 2021, marking the most significant increase since 2015 and a 204% year- over-year increase"**
>
> **– WEF[19]**

## State-sponsored operations

Rising geopolitical tensions are fueling a new level of nation-state cyber activity. The Russia-Ukraine war is the biggest flashpoint, giving rise to thousands of exploits and attacks, such as repeated assaults on the Ukrainian power grid.[20] [21] Some of the cyber offensives have been orchestrated directly by nation-state actors, others by state-aligned entities—such as "hacktivists" supporting Russia or Ukraine, or private Russia-based interests turning to cybercrime to circumvent Western economic sanctions. Beyond the Russia-Ukraine war, China, Iran, and North Korea have all stepped up their malicious cyber operations in recent years.[22]

## Existential stakes

Cybercriminals are going after bigger targets and causing greater harm than ever before, threatening not only individual organizations, but whole economies, governments, and society at large.[23] Escalating attacks on vital infrastructure and services (power, water, food, communications, transportation, healthcare) are imperiling public health and safety. A devastating wave of ransomware attacks launched against the government of Costa Rica in late 2022 led to a nationwide state of emergency.[24] Attacks on hospitals are reportedly surging.[25] The Russia-Ukraine conflict has ignited an era of "hybrid war," with hostilities taking place simultaneously on physical and virtual fronts. Some analysts foresee cyber warfare tactics being adapted and used by commercial cybercriminals in the future.[26]

[12] *Ransomware attacks decreased 61% in 2022*, Security Magazine, January 11, 2023.
[13] *The Latest 2023 Ransomware Statistics*, AAG IT Support, March 3, 2023.
[14] *The 13 Costliest Cyberattacks of 2022: Looking Back*, Security Intelligence, December 29, 2022.
[15] *2022 Data Breach Investigations Report*, Verizon, May 24, 2022.
[16] *Where Advanced Cyberattackers Are Heading Next: Disruptive Hits*, New Tech, Dark Reading, December 02, 2022.
[17] *Why are ransomware gangs pivoting to Rust?*, IT Pro, July 7, 2022.
[18] *Key Findings from the 1H 2022 FortiGuard Labs Threat Report*, Fortinet, February 22, 2023.
[19] *The Global Risks Report 2022*, World Economic Forum, January 11, 2022.
[20] *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*, Google Threat Analysis Group and Mandiant, February 2023.
[21] *A Boiling Cauldron: Cybersecurity Trends, Threats, And Predictions For 2023*, Forbes, November 23, 2022.
[22] See CISA reports on China, Iran, and North Korea
[23] *Shadowboxing and geopolitics on the dark web*, Politico, December 11, 2022.
[24] *Costa Rica State of Emergency Declared After Ransomware Attacks*, Security Intelligence, November 16, 2022.
[25] *The mounting death toll of cyberattacks*, Politico, December 28, 2022.
[26] *The Top 23 Security Predictions for 2023*, GovTech, December 23, 2022.

# Advanced risk scoring is essential

Faced with a multitude of vulnerabilities and threats, security teams need better ways to cut through the noise and prioritize the most urgent issues. Conventional risk scoring tools that focus primarily on severity can swamp security teams with false alarms, sending them chasing after huge numbers of vulnerabilities that may not represent significant risk.

Advanced risk assessment solutions, by contrast, help security teams zero in on the issues that really matter and stop wasting time on the ones that don't. This requires weighing a number of factors: not just severity but exploitability, exposure, asset importance, and, ideally, business impact (i.e., cyber risk quantification, described below). In so doing, advanced multidimensional risk measurement can winnow the list of actionable vulnerabilities by orders of magnitude (from hundreds of thousands to a few hundred, for example, or from thousands to dozens), enabling teams to effectively allocate limited resources where they're needed most.

## Risk is multi-dimensional

**RISK = Severity + Exploitability + Exposure + Impact**

Advanced scoring solutions weigh four key factors to measure the risk of vulnerabilities.

> **"Some of the most widespread and devastating attacks have included multiple vulnerabilities rated 'high,' 'medium,' or even 'low.' This methodology, known as 'chaining,' uses lower score vulnerabilities to first gain a foothold, then exploit additional vulnerabilities to escalate privilege on an incremental basis."**
>
> **– CISA Directive 22-0119**

# The growing importance of cyber risk quantification

The ability to gauge the potential business impacts of cybersecurity issues is known as cyber risk quantification (CRQ), and it's an important feature of today's most powerful risk assessment solutions. It enables organizations to estimate the tangible harm that might be done if a particular vulnerability is compromised, and conversely, the potential benefits if the vulnerability is closed or mitigated. CRQ takes the guesswork out of prioritization. Companies can accurately rank relative business risks, and focus their efforts on maximum risk reduction.

CRQ means looking beyond simple guesstimates of asset importance to understand the potential consequences of a successful attack: the impacts on company operations, finances, personnel, customers, and partners. CRQ replaces abstract measures of risk with concrete terms that company management and boards understand, and it helps security teams justify budgets and demonstrate the effectiveness of vulnerability management programs. CRQ is quickly becoming a must-have feature, with additional impetus from regulatory agencies such as the SEC, which is proposing new rules for cyber risk accounting and disclosure for publicly-held companies.[27]

> **"Boards want to see ROI for cyber and expect security leaders to show what they are doing with the precious budget that they are entrusted with. Tech execs are pushing this pressure onto security leaders, demanding more-reasoned business cases — and increasingly, the use of cyber risk quantification — to show annualized loss expectancy reduction seen from cyber investment."**
>
> **– Forrester[28]**

[27] *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, U.S. Securities and Exchange Commission, March 9, 2022.
[28] *Optimize Your Security Tech Stack*, Forrester Research, August 17, 2022.

# Network device vulnerabilities pose unique risks

Network devices have become an area of major concern in recent years. Vulnerabilities are rife in network products such as firewalls, traffic managers, virtual private networks (VPNs), routers, and load balancers. Large enterprises have many such systems, and any particular vulnerability may be repeated in hundreds or thousands of instances. Some of these weaknesses enable bad actors to bypass normal protections such as those provided by firewalls and gain wider access to company networks and the systems connected to them. A growing assortment of malware is designed to exploit these vulnerabilities, and attacks on network devices are on the rise.

Adding to the problem, many network devices are difficult or impractical to scan and patch, because companies can't afford to take the systems offline or degrade service. It's therefore essential that security teams leverage additional tools that can pinpoint security weaknesses without active scanning, and mitigate risks when patching isn't feasible.

> **"[Network] devices are ideal targets for malicious cyber actors because most or all organizational and customer traffic must pass through them. An attacker with presence on an organization's gateway router can monitor, modify, and deny traffic to and from the organization. An attacker with presence on an organization's internal routing and switching infrastructure can monitor, modify, and deny traffic to and from key hosts inside the network and leverage trust relationships to conduct lateral movement to other hosts."**
>
> – CISA: ***Securing Network Infrastructure Devices***

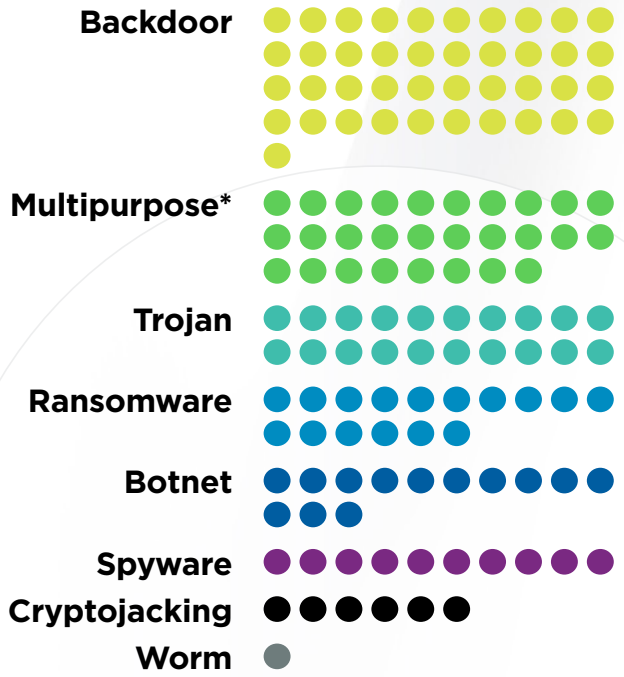
# New malware: backdoor is up, cryptojacking is down

In the previous two editions of this report, we described how cryptojacking software had become the fastest-growing malware type among the categories we track. Crytptojacking programs hijack computing power to mine new cryptocurrency, which was a lucrative activity during the crypto boom of recent years. But cryptomining became less profitable last year as crypto values plummeted. We found that the number of new cryptojacking programs declined accordingly. Cryptojacking now sits near the bottom of our 2022 malware growth rankings.

Similarly, new ransomware programs, which were the second-fastest growing malware category in 2021, leveled off in 2022. This tracks with third-party data suggesting a dip in ransomware attacks during the year—perhaps due to the increasing refusal of victimized companies to pay ransoms.[29]

By contrast, production of new backdoor malware took off in 2022, outpacing every other category in our rankings. This is consistent with observations from a number of third-party researchers. IBM's X-Force security service, for instance, found that incidents involving backdoor malware surged in 2022, replacing ransomware as the top action on objective.[30]

## New malware (2022) programs exploiting known vulnerabilities




*Multipurpose malware consists of programs that can perform a variety of exploits. They might offer, say, ransomware along with cryptojacking and backdoor capabilities. By creating programs that exploit multiple vulnerabilities, malware providers serve a wider range of customers with a single product. These versatile programs are like Swiss Army knives, used for a range of objectives.

[29] *Ransomware attacks decreased 61% in 2022*, Security Magazine, January 11, 2023.
[30] *X-Force Threat Intelligence Index 2023,* IBM Security, February 24, 2023.

Threat actors use backdoors to bypass authentication and infiltrate systems and networks undetected. Backdoors are a major facet of many APT campaigns: sustained attacks in which intruders may spend weeks, months, or even years conducting reconnaissance, collecting information, and planning next moves before striking at opportune moments. APTs are characteristic of large, well-organized threat groups—nation-states and cybercrime rings—and the jump in backdoor malware adds to a growing body of evidence that cybercriminals are becoming more resourceful, capable, and strategic. The changes we've seen in malware production also illustrate just how nimble and market-savvy malware developers are these days, quickly adjusting their product mix to capitalize on the latest cybercrime trends.

## Top ten vulnerabilities targeted by new malware

| | | |
|---|---|---|
| 1 | CVE-2021-44228 | Critical Remote Code Execution Vulnerability in Log4j (Log4Shell) |
| 2 | CVE-2022-26134 | Atlassian Confluence Remote Code Execution Vulnerability |
| 3 | CVE-2022-30190 | Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability ("Follina") |
| 4 | CVE-2022-1388 | F5 BigIP Remote Code Execution, DoS and Information Disclosure Vulnerability |
| 5 | CVE-2022-22954 | VMware Products Remote Code Execution Vulnerability |
| 6 | CVE-2022-25075 | TOTOLINK A3000RU Remote Command Injection Vulnerability in "Main" function |
| 7 | CVE-2022-22947 | Spring Cloud Gateway Remote Code Execution Vulnerability |
| 8 | CVE-2022-22960 | VMware Products Local Privilege Escalation Vulnerability |
| 9 | CVE-2021-45105 | Apache Log4j2 Remote DoS Vulnerability |
| 10 | CVE-2021-4034 | Polkit Local Privilege Elevation Vulnerability in pkexec |

To better understand the wave of malware that debuted in 2022, we looked more closely at the specific vulnerabilities the programs are designed to exploit. The table above shows the top ten CVEs exploited by new malware, ranked by the number of malware programs targeting them. Several important trends jump out:

## Log4Shell isn't going away

The Log4Shell vulnerability was far and away the most popular target of the new malware we tracked in 2022. First reported in 2021, Log4Shell is a flaw in open-source Log4J logging software. The ubiquity of Log4J (used in hundreds of millions of systems), the nature of the bug (allowing attackers to take control of internet-connected devices), and its easy exploitability make Log4Shell one of the most serious vulnerabilities ever found. Within a month of its discovery, millions of attack sessions were observed.[31] It was even used by Iran-affiliated state-sponsored actors to attack a U.S. Federal government agency.[32] While Log4Shell is no longer making so many headlines, the wave of new malware targeting it indicates that it's still high on threat actors' hit lists. And though the initial blitz of Log4Shell assaults abated somewhat in mid-2022, attacks ticked back up toward the end of the year.[33] Beyond Log4Shell, a number of new malware programs target another Log4J bug: the Apache Log4j2 Remote DoS Vulnerability, number nine on our list of the most targeted vulnerabilities.

## Development environments are fertile hunting grounds

After Log4Shell, the second most-targeted CVE on our list is a vulnerability in Atlassian Confluence Server—collaboration software widely used by software engineers.[34] This highlights another important threat trend of recent years: attackers' growing recognition of software development and DevOps environments as vulnerable high-value targets. Last year's widely publicized attack on LastPass, a service used by millions of people to secure and manage their passwords, was an example.[35] Attackers initially gained access to a development environment and later used information thus obtained to successfully penetrate a production instance and exfiltrate user account data. In other cases, hackers have infiltrated development environments to harvest and sell sensitive information and embed malicious code in software products (the first step in a supply chain attack).[36]

## Network devices are prime targets

Another group of new malware programs allows threat actors to take control of widely used network devices and software such as VMware identity managers and F5 network controllers. Compromising these critical network assets can enable hackers to carry out a wide range of exploits and campaigns. It's therefore critical to identify and mitigate network risks in ways that go beyond scanning and patching, which aren't always feasible in network devices.

More generally, virtually all of the malware on our top ten list is aimed at some form of remote access and intrusion. That's yet another sign of the increasingly sophisticated and insidious tactics—such as APT exploits—being employed by a growing number of threat actors.

[31] *Top CVEs to Patch: Insights from the 2022 Unit 42 Network Threat Trends Research Report,* Palo Alto Networks, July 21, 2022
[32] *CISA Alert: Iran-Backed Actors Hit Federal Agency in Log4Shell Attack,* GovTech, November 16, 2022.
[33] *Log4Shell a year on,* Kapersky Labs, December 8, 2022.
[34] *Zero-Day Exploitation of Atlassian Confluence,* Volexity, June 2, 2022.
[35] *What we know about the LastPass breach (so far),* Security Dive, January 5, 2023.
[36] *7 Tips for Securing The Software Development Environment,* Dark Reading, August 24, 2021.

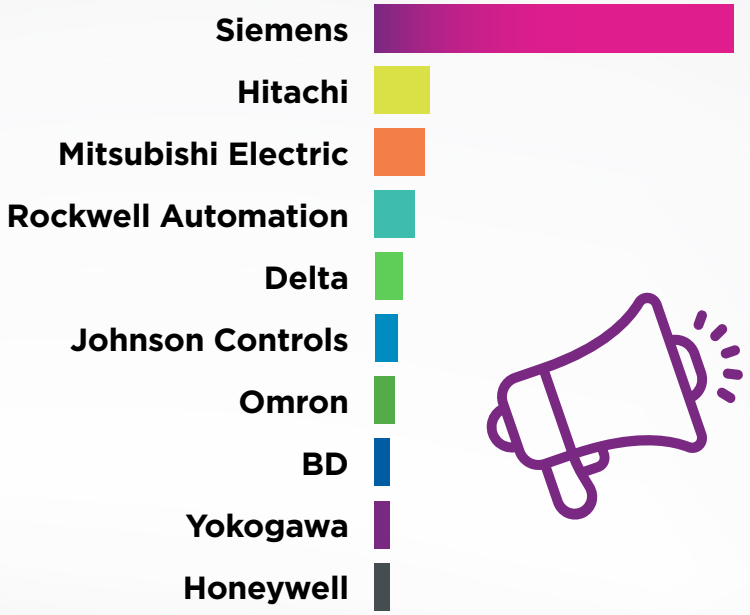
# OT continues to be a major weak spot

CISA (the U.S. Cybersecurity And Infrastructure Agency) issued 385 OT advisories in 2022, up from 379 in 2021. OT has become an area of acute concern in recent years, because many of these systems are weakly defended or not defended at all, and because OT assets control critical infrastructure and other vital systems in energy, manufacturing, utilities, healthcare, and other industries.

A growing number of formerly air-gapped OT systems are being exposed to attack as they're wired up to company networks and the internet for purposes of remote and automated management. Many of these systems lack robust security protections and are hard or impossible to scan and patch. They're sitting ducks for malicious exploits ranging from sabotage to extortion, and OT attacks are now commonplace. As OT and IT networks converge, threat actors are increasingly exploiting vulnerabilities in one environment to reach assets in the other. As in the case of network devices, organizations need more effective ways of detecting and addressing OT security flaws, using techniques that go beyond scanning and patching.

The chart on the right shows the ten OT vendors with the largest number of CISA advisories. Siemens leads the list by a wide margin. This may be in part because of Siemens's broader product portfolio (it's the leading OT vendor), or perhaps because the company is more diligent in uncovering and disclosing vulnerabilities.

## Top ten OT vendors with the most CISA advisories



# Top ten products with the most vulnerabilities

| | | |
|---|---|---|
| 1 | **RedHat** | Enterprise Linux |
| 2 | **Google** | Android |
| 3 | **Microsoft** | Windows |
| 4 | **RedHat** | Enterprise Linux Server |
| 5 | **Apple** | MacOS X |
| 6 | **Google** | Chrome |
| 7 | **Microsoft** | Edge Chromium |
| 8 | **Linux** | Linux Kernel |
| 9 | **Apple** | iOS |
| 10 | **Juniper Networks** | JUNOS |

The list on the left shows the ten products with the largest number of new vulnerabilities reported in 2022, per the NVD. This is mostly unsurprising: larger, more complex software tends to have more vulnerabilities, and these are among the largest, most complex software products on the market. It's notable that while most of the products on this list are normally identified with consumer systems, a number of them (the Linux products and Windows, for example) are also widely used on servers. That's a reminder of how important it is to implement and maintain proper configurations and controls such as firewall policies and network segmentation that keep servers from being exposed to attack, given the large number of vulnerabilities and the time it takes to patch them.

# Cybersecurity is facing a complexity crisis

All of the trends described above have contributed to a meteoric rise in cybersecurity complexity. The number and variety of vulnerabilities have shot up. Attack surfaces have exploded. Threat actors are more numerous, more skilled, more organized, and better equipped. They're taking aim at bigger targets and doing more damage. They're also moving faster: the time from vulnerability discovery to exploitation is shrinking to mere hours in some cases.[37] Compliance burdens are growing, too, owing to a raft of new requirements from government regulators, standards-setting bodies, and company policies.

As workloads snowball, cybersecurity teams are hamstrung by limited budgets and chronic talent shortages. The WEF estimates that there is a 3-million-person gap in cyber professionals worldwide, and 62% of organizations in a recent survey reported insufficient cybersecurity staffing.[38] [39]

Traditional tools and methods—labor-intensive, piecemeal, reactive, and scattershot—are adding to the pain. They fail to detect many security weaknesses while bombarding teams with false positives, providing no way to prioritize and allocate resources effectively. "Solution fatigue" is endemic. As Forrester explains: "Tech execs have a security tech sprawl problem that is hobbling operations. For many years, security leaders have tried solving unique or niche security challenges by purchasing best-of-breed security technologies. This leaves organizations with an unwieldy number of security solutions and the large budget to go with it."[40]

"Complexity," as PwC observes, "has driven cyber risks and costs to dangerous new heights."[41] Organizations that continue to rely on cumbersome conventional approaches are falling further and further behind. Fortunately, a new generation of solutions can radically reduce cybersecurity complexity and harness new efficiencies. We'll look at key capabilities in the next section.

**In its annual Cost of A Data Breach Report, IBM identified three key factors that added significantly to the cost of a breach: cloud migration, compliance failures, and security system complexity.[42]**

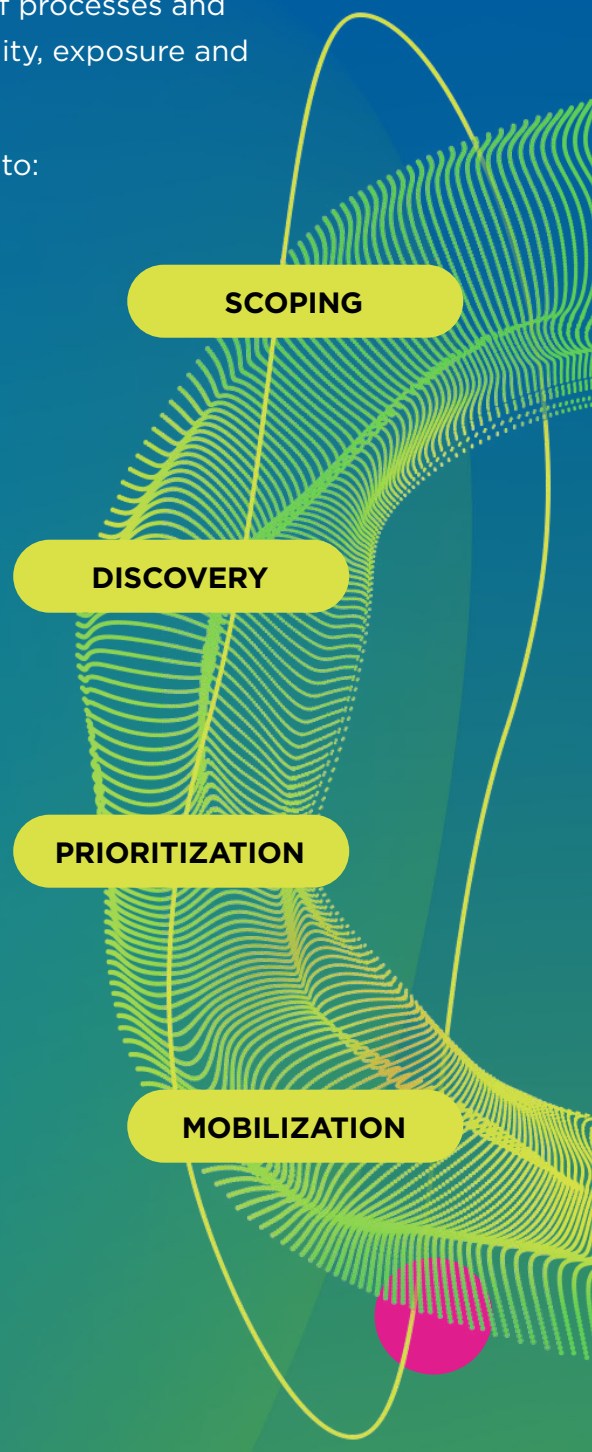
[37] *Attackers Move Quickly to Exploit High-Profile Zero Days: Insights From the 2022 Unit 42 Incident Response Report*, Palo Alto Networks, July 26, 2022.
[38] *The Global Risks Report 2022,* World Economic Forum, January 11, 2022.
[39] *34 Cybersecurity Statistics to Lose Sleep Over in 2023*, TechTarget, January 26, 2023.
[40] *Optimize Your Security Tech Stack*, Forrester Research, August 17, 2022.
[41] *Simplifying cybersecurity,* PwC, February 17, 2021.
[42] *Cost of a Data Breach Report,* IBM, July 2022.

# How continuous exposure management re-levels the playing field

There's no sugar-coating the fact that ongoing vulnerability and threat trends have made cybersecurity more difficult—and cybercrime easier. Status-quo security tools aren't helping; if anything, they're compounding the complexity. The good news is that a new approach, known as continuous exposure management, offers dramatic improvements in performance, efficiency, and risk reduction. Gartner® refers to this as continuous threat exposure management (CTEM), described as "a set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exposure and exploitability of an enterprise's digital and physical assets."[43]

To make the most of this modern, risk-based paradigm, look for solutions that help you to:

- **Take a holistic approach.** Consolidate your cybersecurity functions and eliminate the disconnects and vendor fatigue that plague point solutions. Manage vulnerabilities, compliance challenges, network risks, and policy configuration management with a seamless interoperating platform.
- **Maintain 360-degree visibility.** Understand your entire attack surface including on-premises and cloud assets, IT and OT environments, hybrid networks, devices, and applications. Bring together all relevant asset data including properties (ownership, location), connectivity, and security policies in a single unified view.
- **Discover and detect the full range of exposures.** Leverage not only active scanning but also scanless detection and threat intelligence. Continuously verify compliance while detecting misconfigurations and gaps in security controls that leave assets exposed.
- **Assess risks and prioritize.** Using multidimensional risk scoring as described above and techniques such as exposure and access analysis, passive attack simulation, and network modeling, advanced solutions provide the fine-grained risk prioritization that companies need to optimally allocate resources and make the most of their remediation efforts.
- **Choose the appropriate remediation.** Today's best solutions recommend remediations and enforce policies and best practices such as network segmentation, which can limit damage even where patching isn't possible.
- **Automate the response and validate success.** Best-in-class solutions automate prioritization based on risk quantification, initiate remediation using automated workflows, validate corrective action, and report the results.
- **Partner with experts.** Cybersecurity is a team game, requiring a wide array of competencies and a high degree of coordination and cooperation among various players. It's imperative to choose vendors based not only on their technology and products, but also their real-world experience, their problem-solving skills, and their ability to leverage learnings from their customers and ecosystem.




When combined, these capabilities enable a proactive, integrated, sustainable approach to vulnerability and security policy management. Continuous exposure management makes cybersecurity much more rigorous, pragmatic, and cost-effective, and it enables resource-constrained teams to avoid overload and focus on the risks that truly matter to their business. It's quickly become a cornerstone of mature cybersecurity strategy and a key to robust cyber resilience.

Get out of firefighting mode, get ahead of emerging threats, and empower your teams. Continuous exposure management can help you safeguard your organization by pre-emptively identifying and mitigating your biggest cyber risks.

**Talk to our experts today and we'll show you how.**

**skyboxsecurity.com/contact-sales**

[43] Implement a Continuous Threat Exposure Management (CTEM) Program, Gartner, July 21, 2022.

# Methodology

All of the findings in this report, unless otherwise noted, are based on data from Skybox Research Lab, the threat intelligence division of Skybox. Skybox Research Lab has been at the forefront of analyzing the latest cyber vulnerabilities and threats for over a decade. The lab delivers comprehensive, actionable, and timely threat intelligence that powers Skybox's vulnerability and threat management solution and enables our customers to discover, prioritize, and remediate risks.

Our team of security analysts continuously monitors dozens of security sources, tracking and analyzing tens of thousands of vulnerabilities on thousands of products, along with the latest data on exploits and malware taking advantage of these vulnerabilities. Drawing on this research, the team identifies the vulnerabilities most likely to impact our customers' networks and assets. These vulnerabilities are combined with critical contextual information on whether and how the vulnerability has been exploited, the prevalence of the vulnerability, the malware that exploits it, the damage it can inflict, and optimal approaches to remediation. All of this information is incorporated in a proprietary database used in our product and by Skybox customers.

The Skybox database has information on more than **150,000 vulnerabilities** in over **15,000 products**, including:

+ Server and desktop operating systems
+ Business and desktop applications
+ Networking and security technologies
+ Developer tools
+ Internet and mobile applications
+ IIoT devices
+ Industrial control system (ICS) and supervisory control and data acquisition (SCADA) devices

Many of the statistics and findings in this report are based specifically on the intelligence in the Skybox database. In some cases, we've used other sources such as the National Vulnerability Database (NVD), as explained below.

## Overall vulnerabilities

Overall vulnerability counts are based on new vulnerabilities reported in the NVD. The age of vulnerabilities is based on the publication date in the NVD. For example, vulnerabilities are counted as "new" in 2022 if they were published in the NVD during that period.

## OT advisories

OT advisories are collected from the Cybersecurity and Infrastructure Security Agency (CISA), the cybersecurity arm of the United States Department of Homeland Security (DHS).

## New malware

To identify new malware, our security analysts continuously monitor new cybersecurity advisories and other sources. The data on new malware in this report is extrapolated from these daily intelligence feeds. In this report, we focus specifically on malware that exploits known vulnerabilities.

## Vulnerability severity

The vulnerability severity rating used in this report is part of our risk modeling methodology (CVSS V3 compliant), which takes a variety of parameters into account. The CVSS base score ranges from 0 to 10.

## Network device vulnerabilities

To track network device vulnerabilities, we've specifically looked at vulnerabilities in firewalls, routers, switches, network appliances, and their operating systems. We've deliberately excluded other OT systems such as cameras and industrial control systems, since those are covered separately in the OT section of this report.

## About Skybox

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of dynamically changing attack surfaces. At Skybox, we don't just serve up data and information. We provide the intelligence and context to make informed decisions, taking the guesswork out of securely enabling enterprises at scale and speed.

Our security posture management platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization. The vendor-agnostic platform intelligently optimizes security policies, actions, and change processes across all corporate networks and cloud environments. With Skybox, security teams can focus on the most strategic business initiatives while ensuring enterprises remain protected.

**www.skyboxsecurity.com**



SKYBOX SECURITY