

# Vulnerability and threat trends report 2022

Record-breaking vulnerabilities, rising OT security risks, and increasing exploits demand a new approach to vulnerability management



# Contents

- Introduction > ..... 1
- Key findings > ..... 3
- Record-breaking growth in new vulnerabilities > ..... 4
- Attackers and exploits are evolving rapidly > ..... 6
- OT vulnerabilities surge > ..... 8
- De-risk IT-OT convergence > ..... 11
- Network device vulnerabilities climb steadily > ..... 13
- Multistage attacks on the rise > ..... 14
- Malware proliferates, especially cryptomining and ransomware > ..... 15
- Log4Shell spotlights supply chain risks > ..... 18
- Exploitation of new vulnerabilities accelerates > ..... 19
- Advanced risk scoring is essential for today's attack surface management > ..... 20
- Shifting the paradigm: from detect-and-respond to prioritize-and-prevent > ..... 22
- Methodology > ..... 23

# Introduction

Gidi Cohen, CEO and founder, Skybox Security

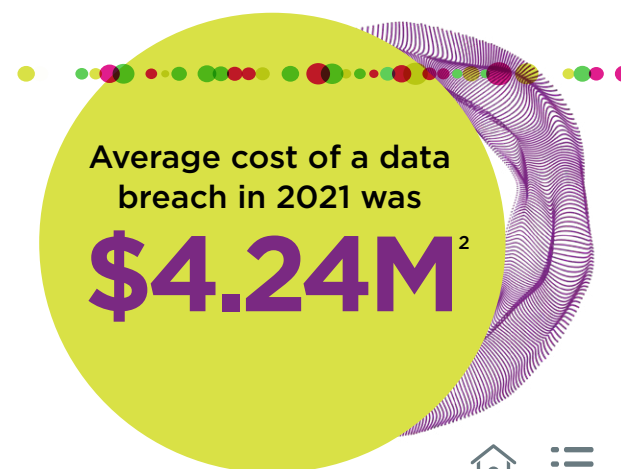
**If the events of 2021 tell us anything about the state of cybersecurity, it's that you can't fight today's battles with yesterday's tools. The rapid evolution of the threat landscape has made past approaches to vulnerability management outmoded, if not downright archaic.**

A phase shift was already well underway when the COVID-19 pandemic kicked it into high gear. It has led to a dramatic expansion of the attack surface, fueled by the headlong migration to the cloud and the explosion of IT and OT (operational technology) assets. Public cloud usage is expected to grow threefold in the next five years. And IDG predicts that there will be over 55 billion connected devices worldwide by 2025, with 75% connected to an IoT platform.<sup>1</sup> Spurred by the pandemic, the pivot to remote work and the hurried rollout of new online services have accelerated these shifts.

At the same time, threats multiplied, and attacks occurred at a cadence and scale never seen before. The security industry was just absorbing the news of the Solar Winds hack when 2021 began; the year

closed with the even more alarming discovery of the Log4Shell vulnerability, potentially impacting hundreds of millions of devices. Between these two bombshells came a procession of increasingly damaging breaches, ranging from ransomware attacks to industrial espionage and sabotage. No sector was safe. Even the critical infrastructure we depend on for energy, water, and food was attacked. The average cost of data breaches hit \$4.24 million, up nearly 10% from 2020.<sup>2</sup>

On top of all this, cybersecurity organizations continue to suffer from significant staffing gaps. In recent surveys, security leaders confided that skills shortages are making it more difficult to meet security needs and respond effectively to incidents.<sup>3,4</sup> The “great resignation” has worsened the talent shortage and led to a loss of institutional knowledge.



<sup>1</sup> Digital Devices Took Over Our Lives In 2020: Here's How To Stay Secure, Forbes, April 15, 2021

<sup>2</sup> 2021 Cost of a Data Breach Report, IBM, July 28, 2021

<sup>3</sup> A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)², 2021

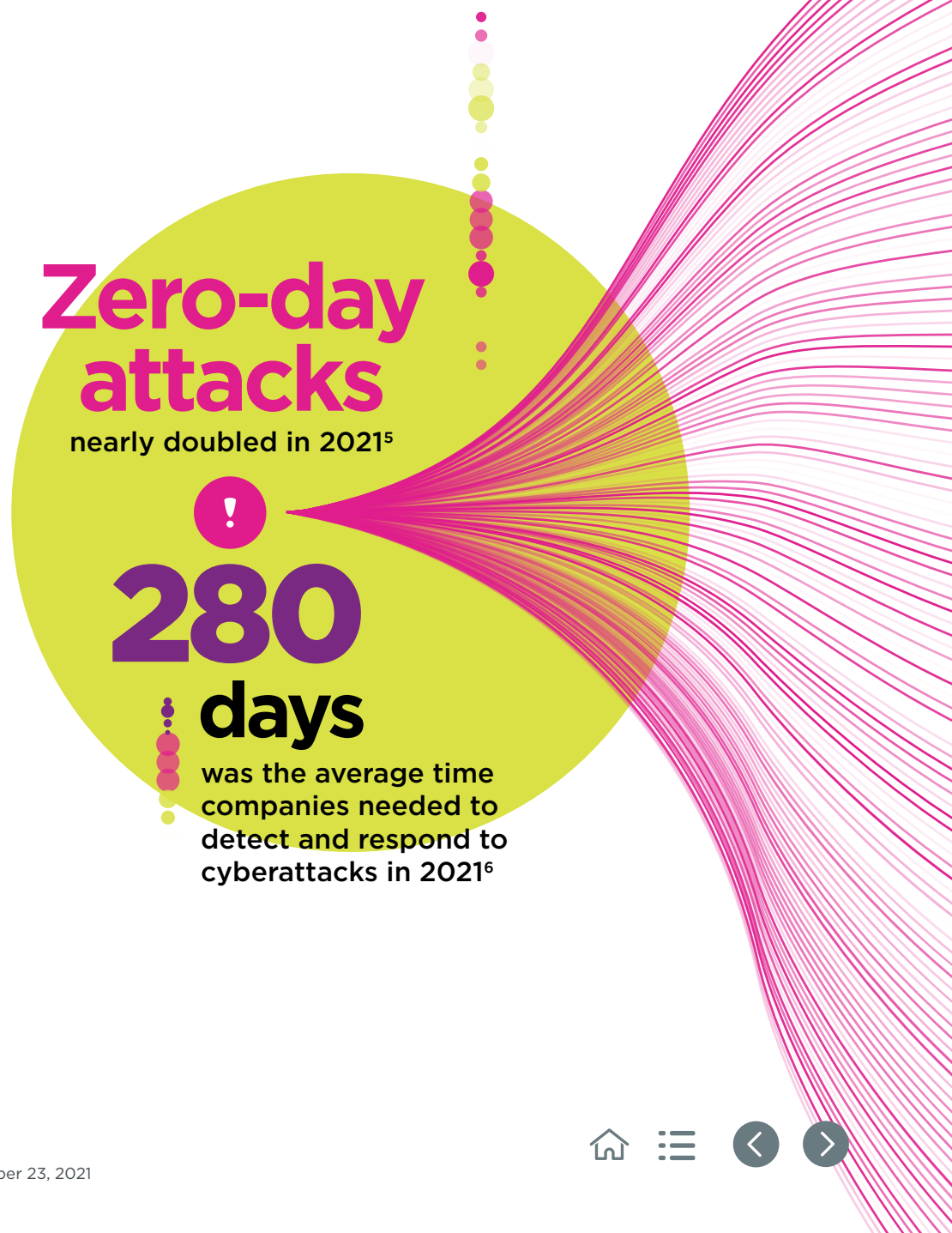
<sup>4</sup> Global Cybersecurity Outlook 2022, World Economic Forum, January 18, 2022



Our own data, analyzed by Skybox Research Lab and detailed in this report, paints a vivid picture of the new reality confronting CISOs and their teams. The findings reveal not only how vulnerabilities — especially in OT — are proliferating at an unprecedented rate, but how threat actors have gotten better and faster at capitalizing on them with a range of new malware and exploits.

As a result, cybersecurity teams are defending a larger, more porous perimeter against a growing array of threats while struggling with greater complexity and tighter resource constraints. Yet many organizations continue to rely on vulnerability management methods that are slow, labor-intensive, piecemeal, and mostly reactive. It's stunning to consider that, even as zero-day attacks nearly doubled in 2021,<sup>5</sup> the average time companies need to detect and respond to cyberattacks stretched to 280 days.<sup>6</sup>

That's unsustainable. As the insights shared in this report make clear, a reset is long overdue. Cybersecurity organizations must move beyond the status quo to a new generation of tools and techniques that flip the script from firefighting to prevention, from manual labor to automated efficiency, and from scattershot, short-term fixes to systematic, comprehensive, and continuous risk reduction.



<sup>5</sup> 2021 has broken the record for zero-day hacking attacks, Technology Review, MIT, September 23, 2021

<sup>6</sup> 2021 Cost of a Data Breach Report, IBM, July 28, 2021



# Key findings



## New vulnerabilities hit an all-time high

There were 20,175 new vulnerabilities published in 2021, up from 18,341 in 2020. That's the most vulnerabilities ever reported in a single year, and it's the biggest year-over-year increase since 2018. The new vulnerabilities add to a huge cumulative total, making it harder than ever for security teams to prioritize and remediate issues.

## OT vulnerabilities nearly double

Vulnerabilities in operational technology jumped 88%, from 690 in 2020 to 1,295 in 2021. At the same time, OT assets are increasingly connected to networks, exposing critical infrastructure and other vital systems to potentially devastating breaches. Attacks on OT systems have risen precipitously, disrupting operations and even jeopardizing health and safety.

## Cryptojacking and ransomware lead new malware production

The malware industry continues to churn out a wide array of malicious software, particularly cryptojacking and ransomware programs, which increased by 75% and 42%, respectively. These programs make it easier for threat actors to mount attacks and turn a quick profit. They demonstrate how nimbly malware developers respond to new market opportunities and economic incentives.

## Threat actors are exploiting weaknesses faster

The number of new vulnerabilities exploited in the wild rose by 24%. That's a sign of just how quickly cybercriminals are now moving to capitalize on new weaknesses, shrinking the window that security teams have to detect and address vulnerabilities before an attack.

# Record-breaking growth in new vulnerabilities

New vulnerabilities hit an all-time high in 2021, surpassing 20,000 for the first time. In all, there were 20,175 CVEs (common vulnerabilities and exposures) published in 2021, 10% higher than in 2020. That’s the biggest jump since 2018. The growth increased in the second half of the year, with 10,723 CVEs published, the most we’ve ever seen in a six-month period.

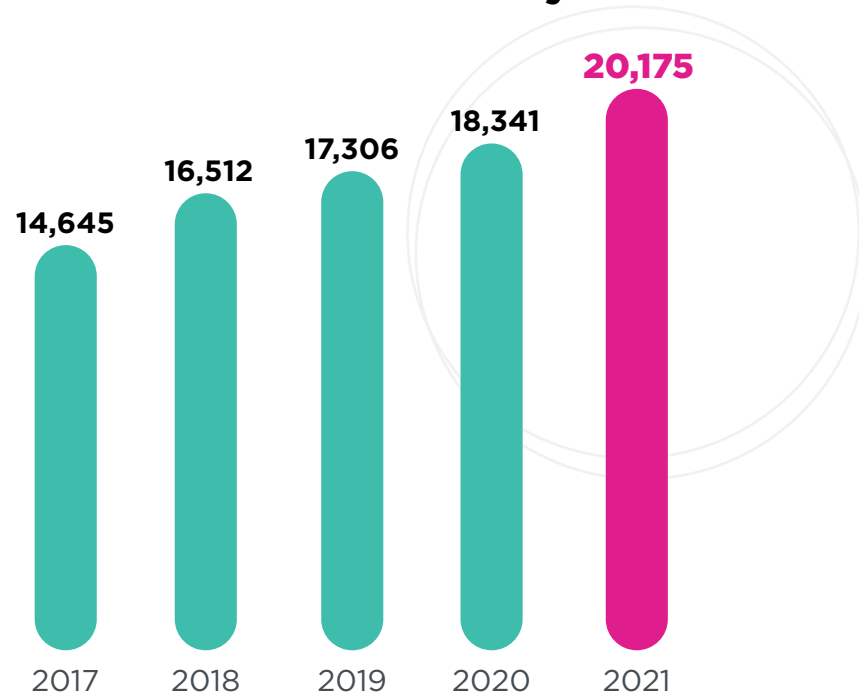
The relentless rise in vulnerabilities has been fueled in large part by the accelerating pace of technological change. Under the mantle of digital transformation and cloud migration, enterprises have been revamping their IT systems at a feverish clip in recent years. This process went into overdrive during the COVID-19 pandemic as companies rushed to support remote workers and stay-at-home customers. The breakneck retooling has introduced new security holes much faster than teams can find and close them. Gartner estimates that “there is a 25-percentage-point increase in the risk of new technologies coinciding with COVID-19-era digital acceleration and the rapid adoption and integration of new technologies, services, and assets.”<sup>7</sup>

As fraught as the situation is on the IT side, things are even more precarious in OT. The number of OT products — especially internet of things (IoT) products — used by enterprises is soaring, and the

associated vulnerabilities are climbing accordingly (see “OT vulnerabilities surge,” on page 8). Further, many formerly air-gapped OT systems are now connected to networks and exposed to external threats without adequate safeguards.

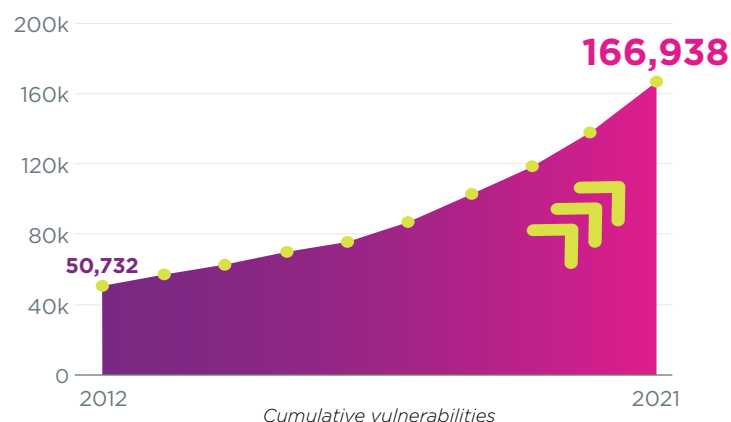


## New vulnerabilities over 5 years



<sup>7</sup> Top 2022 Risks, Gartner, December 10, 2021

## Vulnerabilities have more than tripled over the past ten years



Many new vulnerabilities are also propagating via compromised code libraries and other building blocks — including popular open-source software — used in the software supply chain. Some of these vulnerabilities are inadvertent flaws; others are deliberately implanted by threat actors for use in subsequent exploits, a tactic known as “poisoning.” The vulnerable components are incorporated into a wide array of enterprise software, undetected by developers and customers. The Log4Shell vulnerability, discovered in December 2021 and affecting millions of systems, is an example of how an unintentional flaw in open source software can have catastrophic consequences (see “Log4Shell vulnerability highlights supply chain risks,” on page 18).

New vulnerabilities, worrisome as they may be, are just the tip of the iceberg. The total number of vulnerabilities published over the last 10 years reached 166,938 in 2021 — a three-fold increase over a decade. These cumulative vulnerabilities, piling up year after year, represent an enormous aggregate risk, and they’ve left organizations struggling with a mountain of “cybersecurity debt.”<sup>8</sup> As CISA (the U.S. Cybersecurity and Infrastructure Security Agency) highlights in its list of “Top Routinely Exploited Vulnerabilities,” threat actors are routinely attacking publicly disclosed vulnerabilities from years past.<sup>9</sup>

The sheer volume of accumulated risks — hundreds of thousands or even millions of vulnerability instances within some large organizations — means that security teams can’t possibly isolate and patch all of them. Instead, they need to focus on the exposed vulnerabilities that, if exploited, could cause the most significant business impacts.

**“Malicious cyber actors will most likely continue to use older known vulnerabilities, such as CVE-2017-11882 affecting Microsoft Office, as long as they remain effective and systems remain unpatched.”**

– CISA<sup>10</sup>

<sup>8</sup> The rise of cybersecurity debt, TechCrunch, June 4, 2021

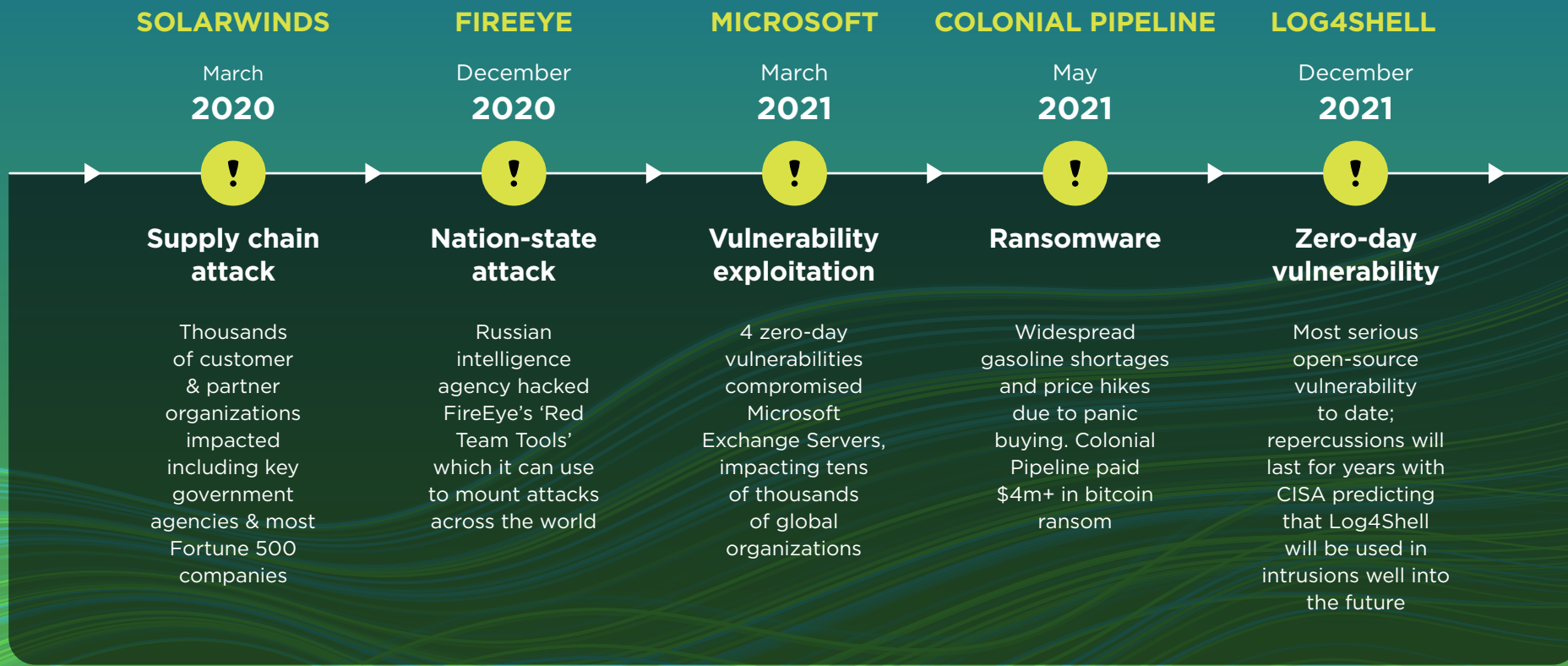
<sup>9-10</sup> Alert (AA21-209A): Top Routinely Exploited Vulnerabilities, CISA, July 28, 2021



# Attackers and exploits are evolving rapidly

Concurrent with the rise in vulnerabilities, we're seeing a rapid evolution of the threat landscape as a whole. Cybercrime has become a vast and thriving industry, with a sprawling ecosystem of specialized goods and services designed to enable and assist threat actors and all varieties of attack, along with an extensive infrastructure to facilitate clandestine communication, collaboration, and financial transactions.

## Rising vulnerabilities, escalating attacks



Cybercriminals have become increasingly diverse. On one side of the spectrum, nation-state actors are using cyber assaults as a weapon against geopolitical rivals. With international tensions flaring in the wake of Russia's invasion of Ukraine, a new era of intensifying state-sponsored attacks may be at hand. Russian hackers have already targeted Ukraine on previous occasions, dating back to 2015, when an attack on the Ukrainian electrical grid cut off power to 230,000 customers. The current conflict has experts contemplating the possibility of full-on cyber warfare.<sup>11</sup> CISA takes the threat of escalating attacks so seriously that it recently issued a rare "shields-up" warning, recommending that "all organizations — regardless of size — adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets."<sup>12</sup>

At the other end of the spectrum, cybercrime is attracting a growing legion of grassroots operators motivated by economic incentives. The quick money to be made from exploits such as cryptojacking and ransomware is tough to resist, especially in parts of the world where pay is low and legitimate career opportunities are few and far between. Easy-to-use exploit kits and malware-as-a-service (MaaS) have made it remarkably simple for non-experts to get into the game and start reaping financial returns.

Innovative tools aren't just making cybercrime more accessible; they also enable a new level of sophistication and stealth. Recent years have seen a steady rise in malware designed to facilitate complex multistage campaigns and hard-to-detect exploits such as fileless attacks (where the malicious code is injected directly into memory, not installed on a hard drive).

Given all the threats and threat actors, it's not surprising that cyberattacks have become more frequent, bigger, and more costly. Prominent examples from the past few years include:

- + **Zero-day attacks** exploiting vulnerabilities in Microsoft Exchange Server, impacting tens of thousands of organizations.
- + **Supply chain attacks** targeting IT software from SolarWinds and Kaseya. The SolarWinds attack affected an estimated 18,000 organizations, while the Kaseya attack impacted roughly 800-1,500 businesses.
- + **Vital infrastructure attacks** including the Colonial Pipeline ransomware attack, which disrupted fuel supplies in the southeastern U.S.

# OT vulnerabilities surge

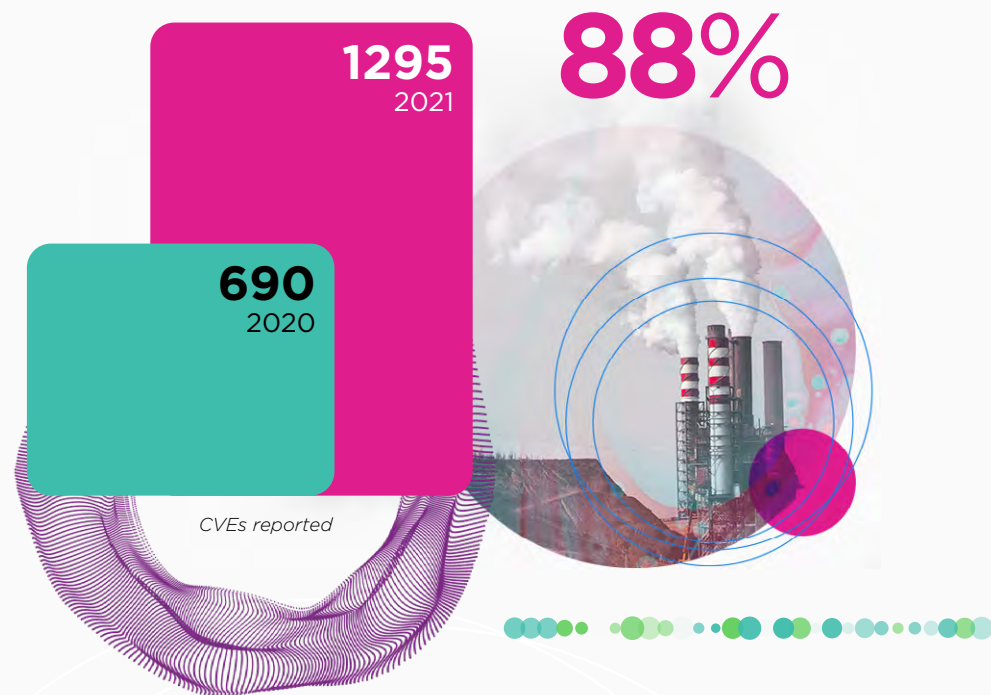
As dramatic as the rise in overall vulnerabilities was in 2021, the vulnerabilities assigned specifically to OT products grew even faster. That number nearly doubled, from 690 in 2020 to 1,295 in 2021. In addition, the number of OT advisories published by CISA jumped 54%.

Siemens, the market leader in OT products, accounted for 40% of the reported vulnerabilities, with 518 CVEs in 2021. This may be in part because of Siemens's broader product line (they have the biggest portfolio of OT products), or perhaps because of the company's greater diligence in uncovering and disclosing vulnerabilities.

The rising tide of OT weaknesses follows years of warnings from security experts, who've long pointed out that OT systems are a ticking time bomb. Designed with weak or non-existent security controls, most OT systems are soft targets for cyberattacks. The only thing protecting them in the past was that they were inaccessible to external threats because they were air-gapped or connected only to isolated internal networks.

That's changed. Many systems are now connected to larger IT networks and the internet itself, often wirelessly. Much of this networking has taken place without any security oversight or planning; devices have been brought online in ad-hoc fashion (to allow remote management, for example — a trend accelerated by the pandemic).

## New OT vulnerabilities increased



## Top 10 OT vendors with the most new vulnerabilities

<b>Siemens</b>   518	<b>Johnson Controls</b>   47
<b>Hitachi</b>   73	<b>Advantech</b>   35
<b>Mitsubishi Electronics</b>   62	<b>Rockwell Automation</b>   33
<b>Delta Electronics</b>   57	<b>Philips</b>   28
<b>Schneider Electric</b>   50	<b>GE</b>   19

*Number of new vulnerabilities in 2021*



The explosion of IoT and industrial IoT (IIoT) products, ranging from sensors to smart appliances to environmental control and industrial automation systems, has greatly exacerbated the problem. In a survey by Forrester, security decision-makers whose organizations were hit by cyberattacks said IoT devices were among the most frequent targets.<sup>13</sup>

The stakes couldn't be higher. OT systems include critical infrastructure (energy, water, transportation, and environmental control systems) and other essential equipment. Attacks on vital assets can inflict serious economic damage and even endanger public health and safety. Threat actors may sabotage or manipulate vulnerable OT systems to cause actual physical harm or to extort ransoms, knowing that many companies will readily pay to avoid disruptions or shutdowns.

As OT and IT networks converge, threat actors are increasingly exploiting vulnerabilities in one environment to reach assets in the other. Many OT attacks begin with an IT breach, followed by lateral movement to access OT equipment. Conversely, intruders may use OT systems as stepping stones to IT networks, where they can deliver malicious payloads, exfiltrate data, launch ransomware attacks, and conduct other exploits. Increasingly, malware is designed to exploit both IT and OT resources.

OT attacks are now occurring with frightening regularity. Examples from 2021 include:

- The attack on a water treatment plant in Oldsmar, Florida, where hackers attempted to poison the water supply with sodium hydroxide (lye).
- The ransomware attack linked to the Russia-based DarkSide cybercrime ring that shut down the Colonial Pipeline, resulting in temporary fuel shortages and panic buying in the southeastern U.S.
- The ransomware attack by another Russia-based organization, REvil, on the world's largest meat processor (JBS), interrupting operations.

Prompted in part by the Colonial Pipeline attack, the federal government has elevated OT to a matter of national security. In July 2021, the White House addressed the gravity of the situation, stating that "the cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation." The Biden administration announced a new joint public-private initiative to bolster critical infrastructure, including the electrical subsector, natural gas pipelines, water and wastewater systems, and the chemical sector.<sup>14</sup>

<sup>13</sup> The State of IoT Security, Forrester, July 9, 2021

<sup>14</sup> National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, The White House, July 2021

That's a positive development, but awareness is still lagging in many organizations. Skybox Security's recent survey of OT security decision-makers revealed that cybersecurity risk is widely underestimated.<sup>15</sup> For example, 56% of all respondents were highly confident that their organization would not experience an OT breach in the next year, yet 83% said they had at least one OT security breach in the prior 36 months. Forty percent of all respondents said that OT is an afterthought compared to other digital initiatives.

Compounding the problem is the fact that many flaws in OT systems are hidden from security teams. That's because most OT systems are hard or impossible to scan. At best, companies scan them infrequently (once or twice a year) because they can't afford to take these mission-critical systems offline or degrade service. Likewise, patching many OT systems is technically impossible or too cumbersome and costly to address all vulnerabilities. As a result, many OT environments are riddled with security holes, with no effective way to assess weaknesses, much less fix them.

A different approach is clearly needed: one that eliminates the blind spots by providing a complete view of the OT and IT attack surface and that also facilitates targeted, effective remediation.

“Attacks on organizations in critical infrastructure sectors have increased dramatically, from less than 10 in 2013 to almost 400 in 2020. **That's a 3,900% increase.**”

- According to Gartner<sup>®16</sup>

<sup>15</sup> Operational technology cybersecurity risk significantly underestimated, Skybox Security, December 6, 2021

<sup>16</sup> 3 Planning Assumptions for Securing Cyber-Physical Systems of Critical Infrastructure, Gartner, February 8, 2022



# De-risk IT-OT convergence

Once upon a time, operations personnel didn't worry about cyberattacks on OT assets because such systems consisted of stand-alone devices with no connection to the outside world. The fact that many or most such OT products lack robust cybersecurity protections was not a concern because they were effectively inaccessible — surrounded by a moat, as it were.

Those days are long gone. Formerly air-gapped OT equipment is now hooked up to IT networks and the internet for purposes of monitoring, control, and automation — with weak or no security controls in place. Many newer IoT products are often networked by default, again with little or no security oversight. As Gartner explains: “Over time, the technologies that underpin critical infrastructure have become more digitized and connected — either to enterprise IT systems and/or to each other — creating cyber-physical systems [CPS]. CPS are composed of both legacy infrastructure (deployed years ago without built-in security) and new assets, which are also deployed full of vulnerabilities.”<sup>17</sup> In other words, the moat is gone, and the drawbridge is down.


Most organizations don't even have visibility into the problem. They have no global view of their attack surface, with its interconnections, entry points, configurations, and policies. It's not just blind spots such as unscannable OT and network devices that prevent such a cohesive view; it's also organizational siloing between IT and OT departments and among their various teams. Often each group has responsibility for a small piece of the puzzle, but no one has the big picture. Without full visibility, it's difficult to detect policy violations, vulnerabilities, misconfigurations, faulty design, or unplanned or unauthorized changes. It's also difficult to recognize and respond to complex attacks; individual teams may see only isolated incidents and fail to recognize that these are part of a larger coordinated campaign.



That's why a modern vulnerability management strategy must begin with a holistic view that models and visualizes the entire attack surface, including IT and OT environments and all of the connections among them. This means going beyond active scanning to include scanless detection techniques. Scanless detection expands coverage by correlating asset information from generic CMDB parsers and patch management repositories with updated vulnerability data from threat intelligence sources. The result is continuous non-intrusive discovery on non-scannable assets (routers, switches, and sensitive OT devices) and fills in the gaps between active scan events on scannable assets.

This collected information can be analyzed in a model of the entire network environment. Teams can use the model to conduct path analysis,

attack simulation, and exposure analysis. In so doing, they can identify and assess risks far more accurately than was previously possible. Improved risk assessment, in turn, enables organizations to prioritize resources and implement the most effective remediations: not just patching (which may be impossible or impractical) but also applying methods that reduce exposures and shrink the attack surface while maintaining uptime. Examples of such measures include segmenting networks or disconnecting OT devices where connections aren't necessary; adjusting configurations; enforcing policies; and applying IPS (intrusion prevention system) signatures. The goal is not just to cut off initial breaches where possible, but also to prevent lateral movement that enables attackers to jump from IT to OT systems and vice versa, or from less critical devices to core systems.



“ The traditional network-centric, point solution security tools originally deployed in critical infrastructure operations are no longer adequate to account for the speed and complexity of the emerging threat environment.”

- According to Gartner<sup>®18</sup>

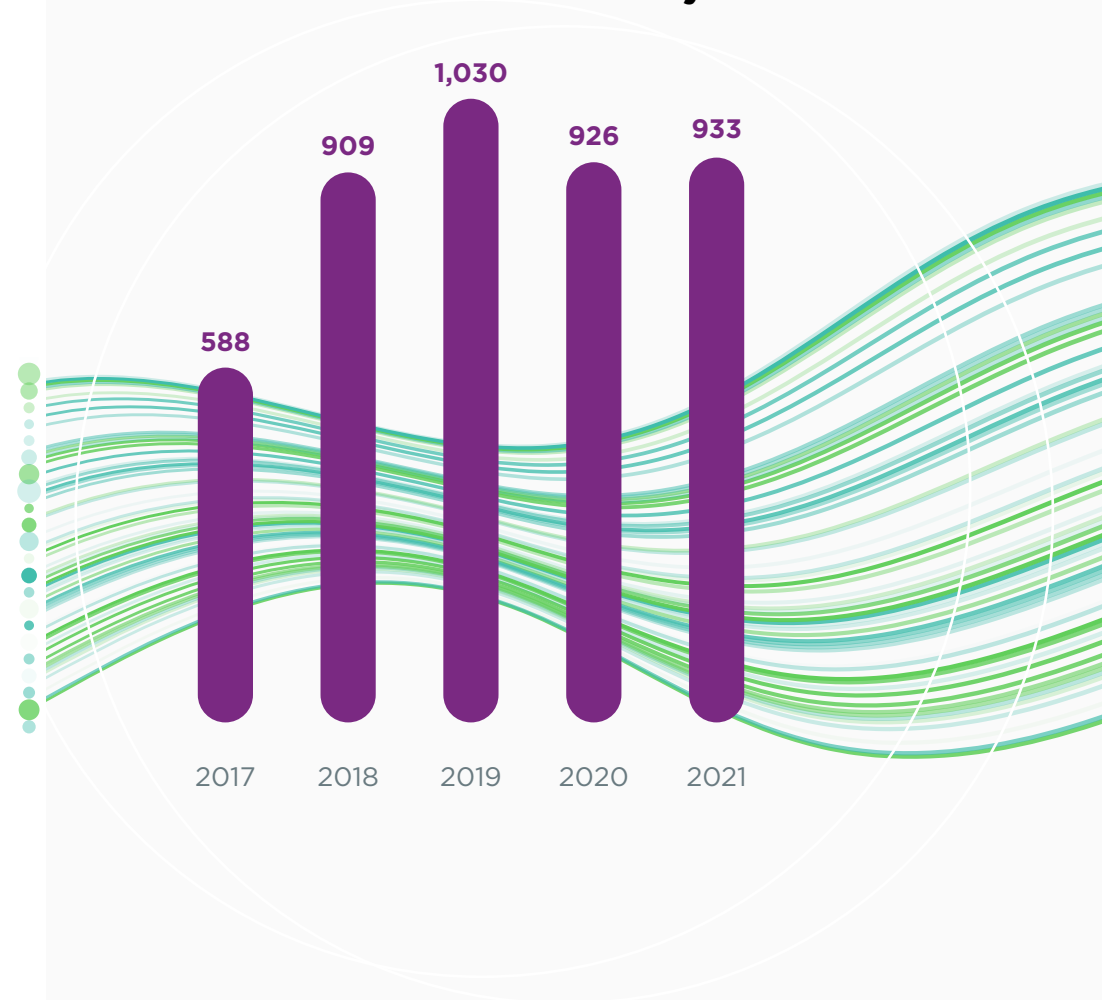
# Network device vulnerabilities climb steadily

We tallied 933 new vulnerabilities in network devices in 2021. The growth in network device vulnerabilities hasn't fluctuated much since 2018, when new vulnerabilities ticked up 35%. In other words, while vulnerabilities continue to grow, the rate of growth at least appears to have stabilized. That may be because network device innovation has slowed, or because vendors are getting better at detecting and eliminating vulnerabilities.

If the latter is the case, it's a step in the right direction, but it shouldn't distract from the large number of cumulative vulnerabilities in network devices and the risks they pose to organizations. The risk is magnified by the fact that, as with OT equipment, many network devices are difficult or impossible to scan.

The rapid deployment of VPNs to support remote workers has contributed to the problem, leading to configuration errors and other security failures that opened the door to breaches. Some network device flaws are widespread, such as a critical vulnerability reported in 2021 in BIG-IP server appliances used by the thousands in some enterprises. Patching them all would be onerous — and wasteful, since only a portion of such devices are exposed. It's therefore critical to apply exposure analysis to triage the problem.

**New vulnerabilities in network devices over 5 years**



# Multistage attacks on the rise

Increasingly, threat actors are employing multistage attacks to circumvent defenses and burrow deeper into organizations. Once restricted to the most sophisticated hackers, these chained attacks can now be carried out even by relative novices, thanks to readily available exploit kits and MaaS that enable inexperienced hackers to execute complicated exploits with no expertise.

Typically multistage attacks begin when a threat actor takes advantage of a stolen credential or common vulnerability to gain initial access to a system such as a user workstation or network device. Once they've gained a beachhead, they can use a series of local exploits to escalate their privileges to administrator status, conduct reconnaissance, and compromise high-value resources such as directories and hard drives containing sensitive information. This allows them to encrypt or exfiltrate critical data as part of ransomware attacks.



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 22-01<sup>19</sup>

Such exploits, which Forrester calls "land and expand vectors,"<sup>20</sup> underscore a major weakness in traditional approaches to vulnerability management. Such approaches often focus on high- and critical-severity vulnerabilities, assuming that lower severity flaws can't do much harm. But in reality, multistage campaigns often exploit less severe vulnerabilities to gain initial ingress, then escalate the attack through lateral movement.

## In this threat landscape, organizations must use tools that:

- 1 Analyze actual exposure, enabling security professionals to detect and close vulnerable entry points (see "Advanced risk scoring is essential for today's attack surface management" on page 20).
- 2 Perform path analysis to identify potential links in a chained attack.
- 3 Recommend effective remediations and policy controls that reduce the "blast radius" even when intruders breach the perimeter.

Such measures may include applying network segmentation, updating IPS signatures, and modifying access policies. These measures can limit lateral movement, prevent unauthorized privilege escalation, and stop intruders in their tracks.

# Malware proliferates, especially cryptomining and ransomware

## NEW PROGRAMS

### Cryptojacking

U  
P **75%**

in 2021

### Ransomware

U  
P **42%**

in 2021

Malware developers were busy creating a variety of new software in 2021.<sup>21</sup> Particularly notable is the increase in cryptojacking and ransomware programs. New cryptojacking programs were up 75% year over year, while ransomware programs increased 42%. Both cases illustrate how the malware industry is getting better at leveraging emerging business opportunities, providing a range of tools and services used by seasoned cybercriminals and inexperienced newbies alike.

Cryptojacking malware highjacks unsuspecting users' computing resources (CPUs and GPUs) for the lucrative activity of cryptocurrency mining. Hackers can use such

exploits to make a quick return with very little effort and up-front investment. As the valuation of cryptocurrency rises, so do the miners' profits. In fact, Bitcoin miners' revenue increased 206% year-over-year, amounting to \$15 billion in revenue.<sup>22</sup> The victims suffer degraded compute performance that can negatively impact productivity but may go unnoticed. Once cryptojacking malware has infected enterprise systems, it can also be repurposed for other types of exploits, such as ransomware attacks. Cryptojacking attacks have snowballed in recent years, quadrupling in 2021.<sup>23</sup>

<sup>21</sup> Skybox Research Lab changed its malware mapping this year to focus only on malicious programs that target known vulnerabilities.

<sup>22</sup> 2022 Digital Asset Outlook Report, Block Research, February 15, 2022

<sup>23</sup> Tales From The Cryptojacking Frontlines, CrowdStrike, October 27, 2021



Like cryptojacking, ransomware can yield a high ROI with a low barrier to entry, thanks to off-the-shelf products and services that do the heavy lifting. In the past, such attacks required a degree of sophistication and resources, but no longer. As one analyst observes: “Gone are the days when every attacker had to write their own ransomware code and run a unique set of activities. RaaS (ransomware-as-a-service) is a pay-for-use malware. It enables attackers to use a platform that provides the necessary ransomware code and operational infrastructure to launch and maintain a ransomware campaign.”<sup>24</sup>


Cybercriminals are launching ransomware attacks at an unprecedented rate with convenient and easy-to-use tools. In a survey by IDC, more than a third of global organizations said they experienced ransomware breaches in 2021.<sup>25</sup>

**According to Forrester, “Ransomware attacks have increased threefold since 2020, with attackers targeting different sectors and verticals in equal measure, and often going after the organizations that they know will be more enticed to pay.”<sup>26</sup>**

Interestingly, we found that new malware is increasingly targeting more recent vulnerabilities (vulnerabilities reported in the last three years). This indicates that malware developers are moving more swiftly to exploit the latest weaknesses. Often this is accomplished by simply tweaking existing malware to perform new exploits. In effect, malware

evolves like viruses, with new variants springing up opportunistically in response to a changing environment.

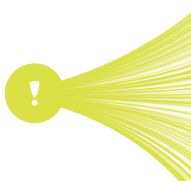
As pragmatic as malware producers are, it makes sense that exploit kits and malware packages include tools targeting the most widespread vulnerabilities. And that’s exactly what our findings show. The table on the next page lists the new vulnerabilities targeted by the largest number of malware programs.



**Notable entries on the list of new vulnerabilities targeted by the largest number of malware programs include:**

- + **Log4Shell:** This recently discovered and nearly ubiquitous vulnerability, first reported in December 2021, already had 15 malware programs targeting it by the year’s end (see “Log4Shell vulnerability highlights supply chain risks,” on page 18).
- + **Microsoft Exchange Server vulnerabilities:** This is another set of widespread flaws impacting many enterprises. Some of these vulnerabilities have been used in multistage attacks.
- + **Pulse Connect Secure vulnerability:** This is an example of a flaw that contributed to the rise in VPN attacks in 2021, underscoring the need for better network device security.

CVE	Name of the vulnerability	No. of malware programs targeting the CVE
CVE-2021-44228	Apache Log4j Critical Remote Code Execution Vulnerability (Log4Shell)	15
CVE-2021-26855	Microsoft Exchange Server Remote SSRF Vulnerability	11
CVE-2021-27065	Microsoft Exchange Server Remote Arbitrary File Write Vulnerability	11
CVE-2021-26857	Microsoft Exchange Server Remote Code Execution Vulnerability	7
CVE-2021-26858	Microsoft Exchange Server Remote Arbitrary File Write Vulnerability	7
CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability	7
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	7
CVE-2021-22893	Pulse Connect Secure Remote Code Execution Vulnerability	7
CVE-2021-26084	Atlassian Confluence Remote Code Execution Vulnerability (Confluenza)	6
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	6



# Log4Shell spotlights supply chain risks

Each year seems to bring news of some new cybersecurity threat that shatters all previous precedents in its scope and potential impact. In 2020, it was the Solar Winds attack. In 2021, it was Log4Shell. First reported in December, Log4Shell is a critical vulnerability in a piece of Java-based open-source logging software known as Log4j, managed by Apache Software Foundation.

The discovery of Log4Shell sent shockwaves through the cybersecurity community, not only because of the criticality of the flaw — which allows any remote attacker to take control of internet-connected devices running the software — but because of its ubiquity. Log4j is used in countless enterprise products and web applications, putting hundreds of millions of devices at risk. “This vulnerability is one of the most serious that I’ve seen in my entire career, if not the most serious,” said Jen Easterly, director of CISA.<sup>27</sup>

Hackers were quick to exploit the vulnerability. According to one source, there were more than a million Log4j-related attacks in the first week after the vulnerability was publicly announced,<sup>28</sup> and as documented by Skybox Research Lab and detailed above, Log4Shell quickly became one of the top targets of new malware.

Log4Shell highlights the growing danger posed by open-source software and the supply chain. Vulnerable or malware-infected components can make their way into widely used software products in ways that are hard to detect and extremely difficult to root out. Such was the case with the Solar Winds hack, and so it is with vulnerable Log4j libraries tucked away in a multitude of enterprise software, with no quick and efficient way to find, much less fix, all of them.

Using traditional, active scanning to find all instances of the vulnerability and then applying patches everywhere is monumentally time-consuming and costly. Fortunately, it’s also unnecessary. Scanless detection can be used to identify affected assets without the cost and performance impacts of active scanning, and exposure analysis can pinpoint the typically small subset of devices that are actually susceptible to attack. Security teams can then apply appropriate mitigation measures such as configuration changes or network segmentation to stem the risks even before patches are applied or in cases where patches aren’t available.

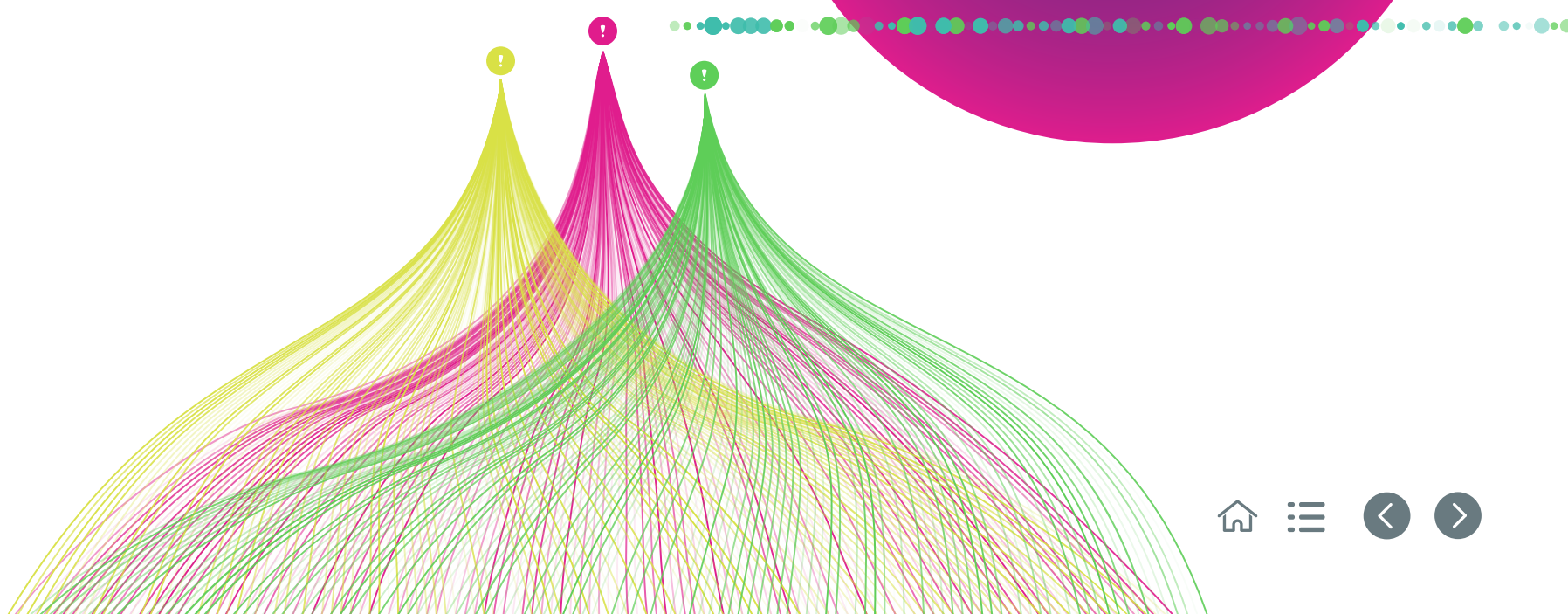


<sup>27</sup> US warns Log4j flaw puts hundreds of millions of devices at risk, ZD Net, December 14, 2021

<sup>28</sup> A deep dive into a real life Log4j exploitation, Check Point, December 14, 2021

# Exploitation of new vulnerabilities accelerates

As new vulnerabilities appeared in 2021, threat actors wasted no time taking advantage of them. One hundred and sixty-eight vulnerabilities that were published in 2021 were promptly exploited within the year — 24% more than the number of vulnerabilities published and subsequently exploited in 2020. In other words, threat actors and malware developers are getting better at weaponizing recent vulnerabilities. This puts security teams in a squeeze, reducing the time between the initial discovery of vulnerabilities and the emergence of active exploits targeting them. That shrinking window means that proactive approaches to vulnerability management are more essential than ever.





# Advanced risk scoring is essential for today's attack surface management

As the attack surface broadens, it's more crucial than ever for security teams to quickly and accurately identify the greatest risks and prioritize remediation efforts accordingly. Conventional approaches that focus primarily on the severity of vulnerabilities as measured by CVSS (the common vulnerability scoring system) miss the mark. No matter how severe a vulnerability is, it may be safe from attack because it's not exposed or because there are no active attempts to exploit it. On the other hand, even a low- or medium-severity vulnerability can constitute a serious risk if it's readily accessible to threat actors and is being actively exploited.

Attackers are increasingly taking advantage of this fact, going after lower-severity vulnerabilities as the first step in sophisticated multistage campaigns. CISA made this point recently, explaining that “the Common Vulnerability Scoring System (CVSS) base score does not account for if the vulnerability is actually being used to attack systems... Known Exploited Vulnerabilities should be the top priority for remediation. Based on a study of historical vulnerability data to 2019, only 4% of the total number of vulnerabilities have been exploited in the wild. Rather than have agencies focus on thousands of vulnerabilities that may never be used in a real-world attack, BOD [Binding Operational Directive] 22-01 shifts the focus to those vulnerabilities that are active threats.”<sup>29</sup>

“Enterprise attack surfaces are expanding. Risks associated with the use of cyber-physical systems and IoT, open-source code, cloud applications, complex digital supply chains, social media and more have brought organizations' exposed surfaces outside of a set of controllable assets. Organizations must look beyond traditional approaches to security monitoring, detection and response to manage a wider set of security exposures.”

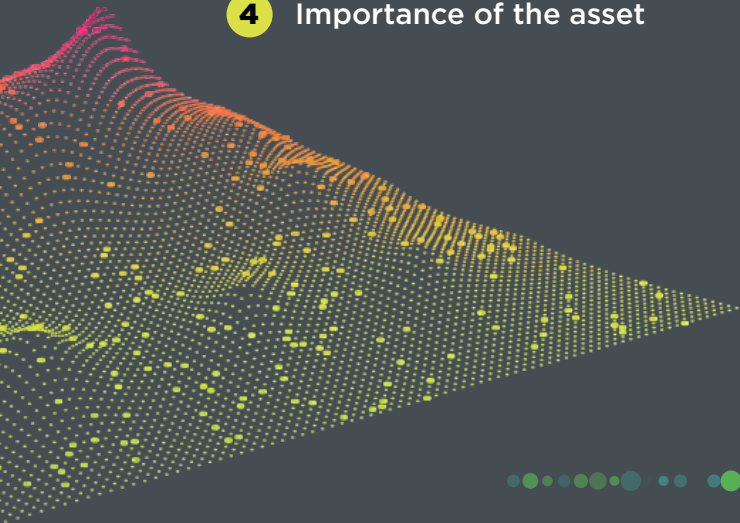
- According to Gartner<sup>30</sup>

Security teams need an objective framework for gauging the actual risk that any given vulnerability poses to their organization. This requires the use of a rigorous scoring system that can be used to prioritize remediation efforts and allocate precious resources where they're most needed. That means calculating risk scores for assets based on four critical variables:

- 1 Measured CVSS severity
- 2 Likelihood of exploitation
- 3 Exposure level based on security controls and configurations in place on the network
- 4 Importance of the asset

Exposure analysis is paramount, yet it's missing from conventional risk scoring approaches. Exposure analysis identifies vulnerabilities and their exploitability potential and correlates this data with an enterprise's unique network configurations and security controls to determine if the system is potentially open to a cyberattack. This process includes path analysis, which maps all the possible paths that packets can take across an enterprise's networks (including complex hybrid networks) — taking account of the policies, security controls, ports, protocols, and applications that affect such movement. Path analysis, in turn, enables attack simulation, which applies advanced algorithms to explore potential attack scenarios and reveal the degree to which various assets might be compromised.

This level of analysis and simulation is only possible when disparate data repositories are normalized and brought together into a multidimensional network model, including patch and asset management systems, vulnerability data, threat intelligence feeds, and cloud and network device configurations.



# Shifting the paradigm: from detect-and-respond to prioritize-and-prevent

The trends described in this report point to an inescapable conclusion: Traditional vulnerability management strategies are wholly out of step with contemporary realities. Approaches centered on scanning and patching are too slow, too scattershot, too laborious, and too costly. They fail to catch many actual threats while squandering valuable resources on false alarms. As a result, security professionals are fighting a rearguard battle against a growing array of threats and adversaries.

It's time to give the advantage back to the defenders. That means turning the tables and changing the dynamic:

- From reactive to proactive
- From siloed to holistic
- From severity-focused to risk-centric
- From manual to automated
- From intermittent to continuous

There's a prescriptive blueprint for doing this. It's called vulnerability lifecycle management, and it has four key parts:

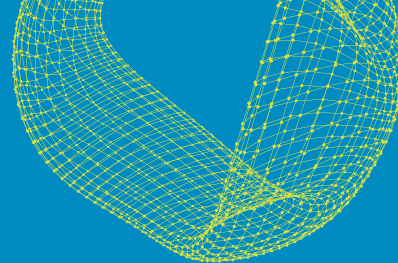
**1. Holistic discovery:** Vulnerability data from all assets (including IT, OT, and cloud) and every corner of the network is aggregated. This requires scanless detection in addition to active scanning. The result is a 360-degree view of the attack surface.

**2. Precise prioritization:** Vulnerability data is incorporated into a network model. This data is then analyzed to reveal exposures. Exposures, severity, exploitability, and asset importance are analyzed together to compute an exact risk score that allows rigorous prioritization.

**3. Targeted mitigation and remediation:** Automated tools identify and recommend effective, practical measures to address and reduce risks. These measures go well beyond patching and include configuration changes, network segmentation, and more. This enables organizations to prevent or limit attacks (including zero-day attacks) even when patches are impractical or unavailable.

**4. Ongoing oversight:** Automated tools assist security personnel in implementing and maintaining remediation. The tools automatically generate tickets, track performance versus SLAs (service-level agreements), keep teams apprised of changes requiring updates, and ensure that issues are promptly addressed.

The lifecycle approach transforms vulnerability management from a sporadic, patchwork process to a continuous and comprehensive one. Most importantly, it enables organizations to move from reaction to prevention — no longer stuck responding to threats after the fact but prepared for whatever may come.



# 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. The Skybox Research Lab has been at the forefront in 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 **130,000 vulnerabilities** in roughly **14,000 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



Most of the statistics and findings in this report are based specifically on the intelligence in the Skybox database. In a few cases, we've used other sources such as the National Vulnerability Database (NVD) instead, 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 2021 if they were published in the NVD during that period.

## OT vulnerabilities

When counting OT vulnerabilities, we consult CISA, the most authoritative source of OT vulnerability data. The OT vulnerabilities in this report are based on new vulnerabilities shared by CISA in 2021.

## New malware

To identify new malware, our security analysts continuously monitor new cybersecurity advisories and other sources. The data on the rise of 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.

## Exploits in the wild

When counting new exploits in the wild, we've focused specifically on exploits targeted at new vulnerabilities, drawing on the intelligence collected in the Skybox database.



## 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.

Interested in speaking with an expert to help solve your greatest security challenges?

**Contact us.**  
**[skyboxsecurity.com](https://skyboxsecurity.com)**