Vulnerability and Threat Trends Report 2021

Cybersecurity comes of age

SKYBOX SECURITY

Contents

Introduction

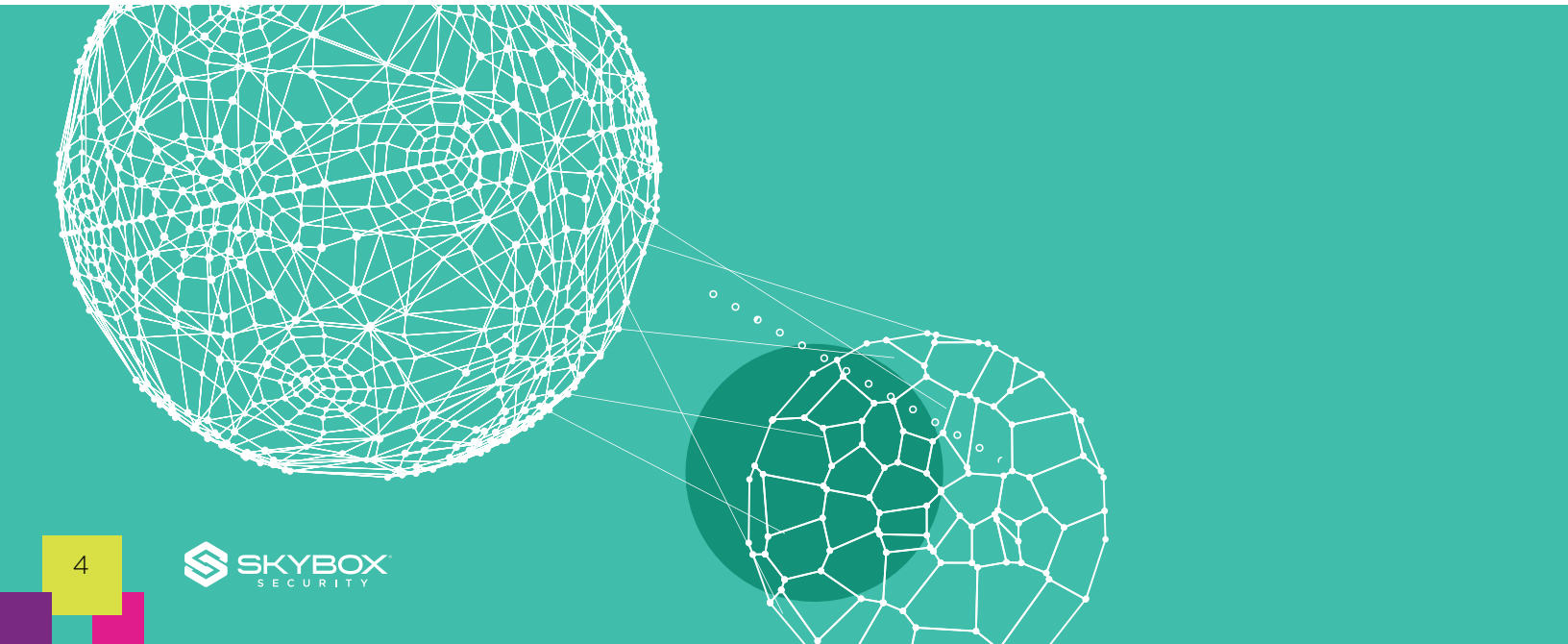
Gidi Cohen, CEO and founder, Skybox Security

The rapid change experienced in 2020 has illuminated a simple truth: What used to work for enterprise security is no longer good enough. Digital transformation has accelerated, organizations have rapidly migrated to the cloud and security has elevated to become a board-level concern. We have seen attack surfaces expand, threat actors grow in sophistication and new vulnerabilities continue to mount. But this change shouldn't be seen as a result of the COVID-19 pandemic. In many ways, it's been a long time coming.

For years, enterprise cybersecurity has been at the cusp of the next stage of its evolution. The problems have mounted: a widening skills gap, increasingly fragmented networks, growing attack surfaces, increasing workloads, visibility and remediation gaps, and ineffective, incomplete scanning. 2020's black swan event put a spotlight on all of these issues. Not only are these problems here to stay, but they are growing worse. Security management practices need to mature. It's time for security to come of age.

This research paper, the seventh edition of the Skybox "Security Vulnerability and Threat Trends" report, puts a fine point on the need for security practices to mature. It reveals 2020 was another record-breaking year for new vulnerabilities and new malware samples have almost doubled. By understanding the vulnerability and threat landscape, we can better anticipate the changes CISOs and their teams will need to make over the coming years.

Yes, cybersecurity needs to mature. Yes, the issues that underpin day-to-day security management can feel overwhelming. But it's also true we are at the beginning of an exciting new era. This is the moment when cybersecurity comes of age to help security teams zero in on what matters and overcome some of their largest and most enduring challenges.



Key findings

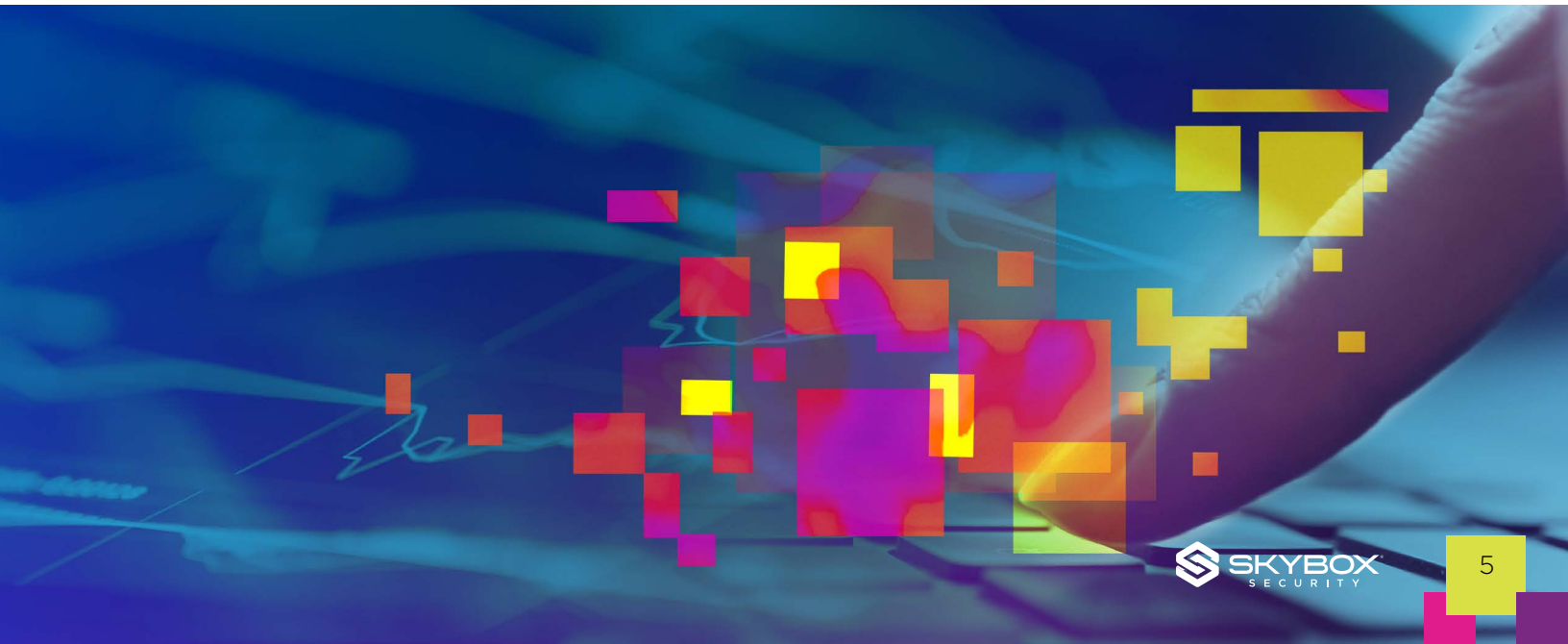
New malware samples nearly doubled, fueled by the pandemic.
New malware samples almost doubled in 2020. There was a 106% increase in new ransomware and 128% growth of new trojans. Threat actors capitalized on new ingress and egress points to networks that were introduced as a result of distributed workforces. Opportunities for successful infiltration have increased and so has the profitability of attacks.

Vulnerability counts hit a new high, further complicating remediation.
Only a fraction of vulnerabilities will ever be exploited. But with 18,341 new flaws reported in 2020, it has become increasingly difficult for security teams to target action where it's needed most.

Lower severity vulnerabilities are being used in chained attacks.
Hackers gain access to critical assets by exploiting the medium- and low-severity vulnerabilities they know are likely to sit unpatched within enterprise environments. By doing so, bad actors can move laterally through the network and enact high-profit and high-impact attacks.

OT environments are under increased threat.
Operational Technology (OT) vulnerabilities increased by 30% year-over-year. Many devices on OT networks are not 'scannable' and are therefore more exposed to risk from IT environments than ever before. New risk is also being introduced through Industrial Internet of Things (IIoT) devices, which saw a 308% increase in new vulnerabilities last year.

Cloud misconfigurations present significant risk.
While misconfigurations remain the biggest risk to cloud security, concern continues to mount about flaws within cloud services. As the popularity of containers increases, so too do their vulnerabilities: there was a 200% increase in new container vulnerabilities between 2016 and 2020.



New malware samples nearly double over 2020

Threat actors have seized on the opportunity of the pandemic. Just one week after the World Health Organization (WHO) coined the term "COVID-19," phishing attacks increased 11-fold and increased in sophistication.[1] Tactics evolved from luring people to share sensitive data with falsified and sensational information about the virus to emulating local government websites and communications. Also, criminals took advantage of the influx of home deliveries by mimicking messages sent by delivery companies.[2]

The rapid development of a distributed workforce opened up a large number of new ingress and egress points to corporate environments. Organizations were also forced to rely more on third-party vendors to support remote workforces, boost productivity and maintain operations. In turn, this created more access points that threat actors could exploit.

The pandemic has energized criminals. This is clear when looking at the volume of new malware samples that have entered the market. The volume of new samples in 2020 was almost double those created in 2019. The types of samples created also illuminate their intent. New ransomware samples increased by 106% year-over-year, and all trojan types experienced 128% growth. These are malware that often work in collusion. Threat actors use trojans to exploit lower severity vulnerabilities. Doing so enables them to gain access to the corporate environment. From there, they can move laterally throughout the network to locate critical assets and deploy ransomware.

Consider the relationship between Emotet, Trickbot and Ryuk: After the Emotet trojan delivers another trojan, called Trickbot, attackers can then move laterally throughout the network to deploy Ryuk ransomware. This method of attack is now as popular as it is dangerous. In October 2020, TrickBot and Ryuk were named alongside the BazarLoader and Conti malware families in a joint advisory from the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Department of Health.[3] Further, data from Kaspersky Labs shows 123,630 of their enterprise users were attacked by trojans between November 2019 and October 2020. This is evidence of just how unrelenting threat actors are in their approach.

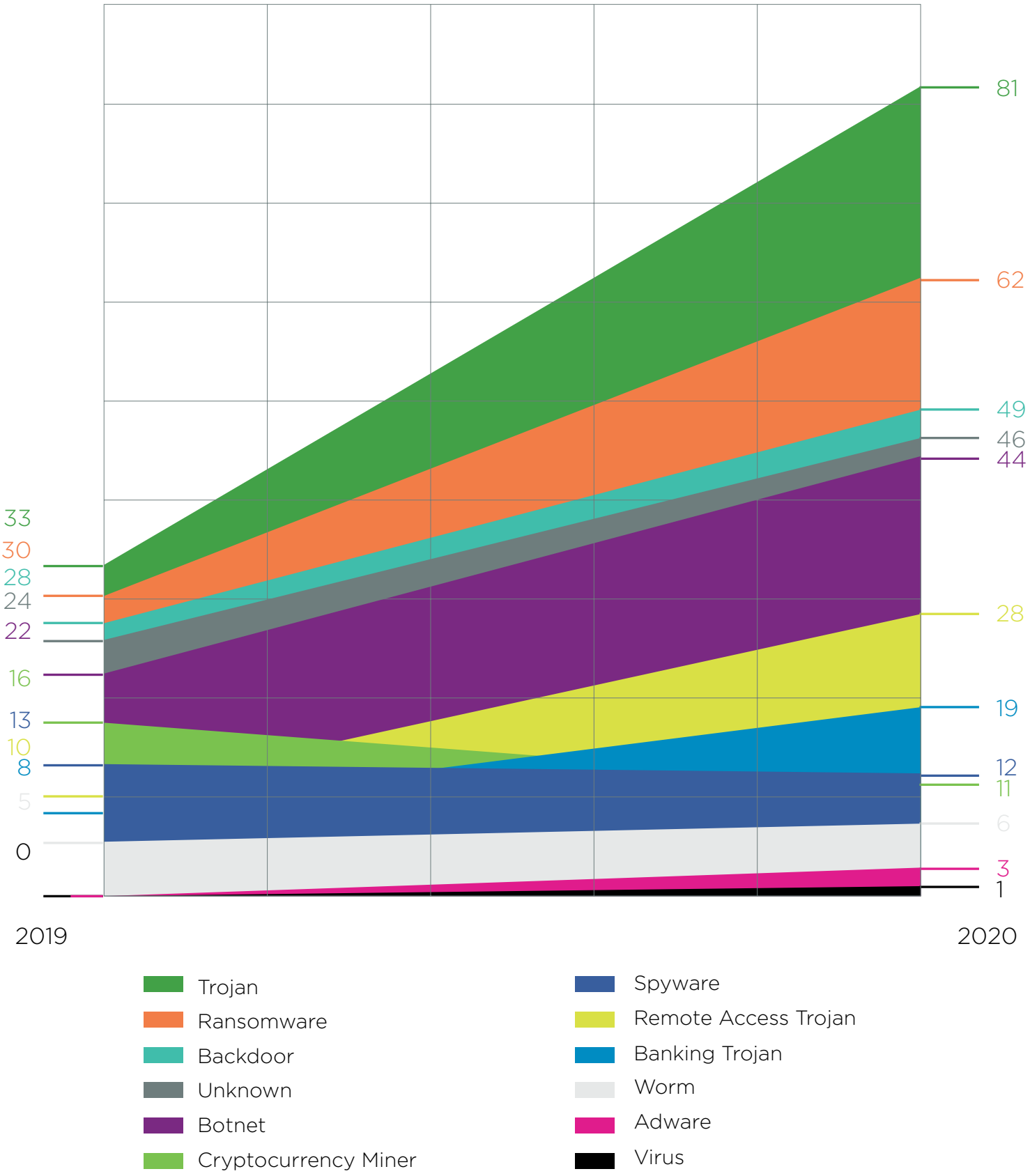
New ransomware samples **increased by 106% year-over-year,** and all trojan types experienced 128% growth.

[1] Exploiting a crisis: How cybercriminals behaved during the outbreak, Microsoft, June 16 2020

[2] Fake deliveries in an age of lockdown, Kaspersky Labs, Kapersky Security Bulletin 2020, Kapersky Labs, November 2020

[3] Ransomware activity targeting the healthcare and public health sector, Cybersecurity and Infrastructure Security Agency, October 2020

New malware samples nearly double in 2020



A profitable new business model: malware as-a-service

One of the most concerning developments is the malware-as-a-service (MaaS) business model. Like the organizations they target, threat actors continuously hone their business models.

Malware-as-a-service (MaaS) facilitates the sale of malware packs that can be bought off-the-shelf on the dark web, just like normal IT software is purchased. Inevitably, this is a model that will gain traction because it drastically lowers the technological bar to carry out attacks. And they work similarly to widely-adopted software-as-a-service (SaaS) products. The malware is nicely packaged and instantly ready for use. The malware creators also take care of the malware's development, maintenance and patching. Although you would still need to know how to deploy the malware, you no longer need to possess the technical skills required to write the exploit itself.

MaaS wouldn't exist if it wasn't lucrative. Cybercriminals can only turn a profit with ransomware when it's used in targeted attacks, whether they be on government agencies, critical infrastructure or large enterprises. Clearly, confidence in the payoff from ransomware attacks has risen. MaaS is a testament to the sophistication of both the malware itself and the exploit tactics threat actors use. In practice, it's now easier than ever for threat actors to carry out attacks. It also means we are likely to see an increase in attacks targeting businesses.

Malware developers and distributers have clearly embraced business innovation. There will always be relative technological parity between the two parties – this isn't a race organizations can hope to win. But they can work to increase the scalability of their security programs in anticipation of further disruption.

"Organizations are so focused on their existing plans and on becoming ISO-certified, they don't realize that they're not taking threat evolution into account. You can't ignore events like Sandworm in 2015 because they happen in different countries. Threat actors don't care where you're located — they follow the money. And, like businesses, they do their own risk management. They don't want to expose themselves. And they are continually evolving their tactics — a failure to recognize and match this agility is harming the progression and potential of security transformation."

Richard Stiennon, author of "Security Yearbook 2020"

Supply chain risk looms large

Concerned with maintaining continuity in 2020, organizations were compelled to increase relationships with third-party vendors while keeping a keen eye on the bottom line. On occasion, this led to firms deciding to work with smaller and less security-conscious vendors. These vendors have yet to fall under threat analysts' scrutiny — the vulnerabilities within their products are mostly unknown, and the threat their exploitation could pose to an organization is equally mysterious.

There have been clear warning signs about the risks within supply chains. In 2019, ASUS fell victim to Operation Shadowhammer when one of its BIOS update utilities coopted to install a backdoor on 660 hardcoded addresses.[4] But it wasn't until the SolarWinds breach came to light that many started to take supply chain risk seriously. Now, we live in the shadow of an attack that infiltrated numerous U.S. government agencies and caused incalculable damage. More must be done to mature enterprise breach prevention capabilities.

Spike in new CVEs in the coming years.

"More organizations are now looking at their downstream supply chains. And, ultimately, everybody wants to save money. Which means that, sometimes, they can choose to go with a lesser vendor. These are vendors who are introducing third-, fourth-, fifth-party risk to large organizations. And with so many new vendors, I believe that we are going to see a spike in new CVEs in the coming years."

Dr. Rebecca Wynn, CISO

Zero Trust plays a starring role

While there is no silver bullet for the insidious nature of supply chain attacks, security teams have become increasingly aware they need to adapt their security and risk management roadmaps to better reflect supply chain attack exposure. Zero Trust plays a starring role in this effort.

Threat actors are known to use generic hosting services, such as Google Cloud Platform and Azure, to obscure their activity.[5] And they are adept at staying under the radar. Whereas it might be natural to trust a VPN to provide security to a network implicitly, the VPN host could be compromised at an earlier point in the supply chain. Therefore, Its traffic should be subject to scrutiny.

To combat this issue, many organizations embrace the concept of Zero Trust and develop frameworks that enable them to verify any connections to their networks before granting access. Yet, achieving Zero Trust is far from straightforward. Developing absolute, hardened no-trust zones requires the tightening up of the entire security architecture. It's a process — one that demands a lot of data, a lot of analysis and insight into all configurations across the entire enterprise environment.

[4] Operation shadowHammer — Compromised ASUS computers, CERT-EU, March 27 2019

[5] Operation chimera — APT operation targets semiconductor vendors, Blackhat, 2020

The best defense is a good offense: intelligence and context

Traditional approaches to security enforcement and incident management lack the sophistication needed to prevent supply chain attacks. To tackle this, we need a new approach focused on breach prevention.

Prevention efforts must start with developing a network model. By aggregating data sets across security, cloud and network technologies, the network model provides security and network teams the ability to analyze network, cloud, IT/OT and security configurations together to proactively gain full context and understanding of the attack surface. It is instrumental to help teams close visibility gaps so they can see and protect all assets and access points.

With a dynamic model of the network and attack surface, it's possible to determine:

+ Where all assets are and how they are connected, configured and secured
+ How hybrid network infrastructure is configured
+ All the complex security controls in place and how these are configured
+ Exploitability of critical assets and applications
+ Interactions between users, elements, endpoints and applications across networks
+ Where the business is exposed to potential cybersecurity attacks
+ Potential risks and the impacts to the business associated with continuous change

Organizations with a network model gain insight into the introduction of new risks, as well as exposures and gaps in compliance. They're able to introduce automation that increases the effectiveness of low-resource security teams. They're able to reduce mean time to respond (MTTR) metrics. They can advance attack simulation capabilities to incorporate deeper attack context and insights to explore all possible attack paths, see all of the devices that could be touched by an attacker, and determine the best course of action to prevent breaches.

A comprehensive model gives you the context that you need

"I love the concept of the network model. Because having that comprehensive model gives you the context that you need. It stops attackers from being successful. And when processes can be automated so security practitioners immediately know what's going to happen — that's invaluable."

Richard Stiennon, author of "Security Yearbook 2020."

Network model defined

A network model is a dynamic representation of the hybrid environment including corporate networks, private cloud, public cloud, and OT. It understands all of the devices, vulnerabilities and configurations within the environment and can be used to run assessments and simulations. With a network model, organizations gain the context that they need to implement automation across a wide range of operational security processes. They are also provided with insight that is used to improve business resilience.

A record-breaking year for new vulnerabilities

Increasing complexities within risk management compound the challenges within the threat landscape. Security practitioners are not only tasked with securing an ever-expanding attack surface, they are now charged with ensuring the success of crucial digital transformation initiatives. And they are expected to continue to support digitization and drive value while improving security posture — all without an increase in headcount.

Pressures to support remote workers, rapidly migrate workloads to the cloud and facilitate critical digital transformation initiatives have forced CISOs to deprioritize critical security tasks. In fact, 43% of security practitioners downgraded their scheduled reporting in 2020.[6] Reduced reporting often leads to fewer new vulnerabilities being detected.

The consideration of known vulnerabilities is important. 1,628 new 2020 vulnerabilities on the NVD database would have actually first come into existence in 2019, if not earlier, and have only recently been published, analyzed and annotated by the NVD. The hundreds, if not thousands, of last year's "unknown" vulnerabilities also need to be taken into account.

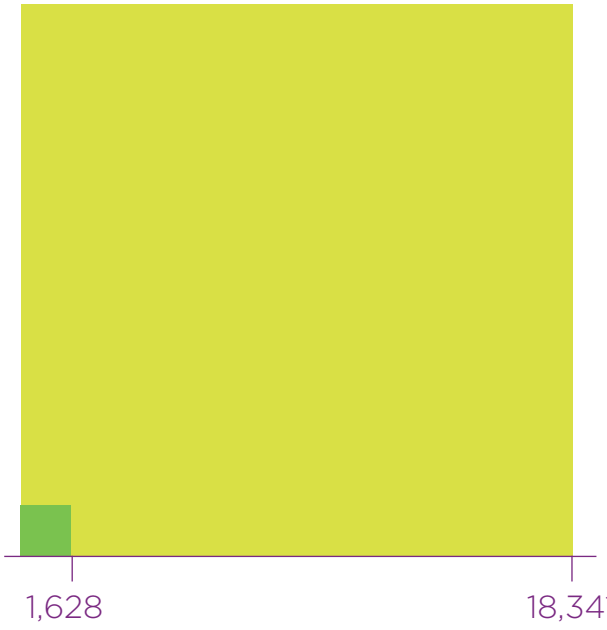
The continued increase in new vulnerability reports is concerning: growth in vulnerabilities is a leading indicator for future attacks. With immature vulnerability management practices, it's impossible for the CISO and their teams to lower their risk profile, let alone have the capacity to support business-wide digitization. High vulnerability counts also complicate prioritization and remediation processes.

43%

of security practitioners downgraded their scheduled reporting in 2020. Reduced reporting often leads to fewer new vulnerabilities being detected.

[6] Cybersecurity in the new normal: securing the distributed workforce and remote operations, Skybox Security, November 2020

New vulnerability reports



Vulnerabilities that entered the NVD database more than a year after first discovery

Total new vulnerabilities

What was once “good enough” will no longer work. Long-held practices rooted in detect-and-respond don’t offer visibility of the entire expansive attack surface. They don’t provide security practitioners with the insight needed to target remediation where it’s needed most. And they cannot safely automate policy changes, which in turn increases opportunities for attacks. This, combined with siloed vulnerability and policy management processes, contributes to systemic risk introduction across the organization.

To deal with the inevitable increase of vulnerabilities, security programs need to mature by incorporating processes that contextualize vulnerabilities based on exposure, exploitability and other factors to keep remediation focused on only the most critical risks.

Hiding in plain sight

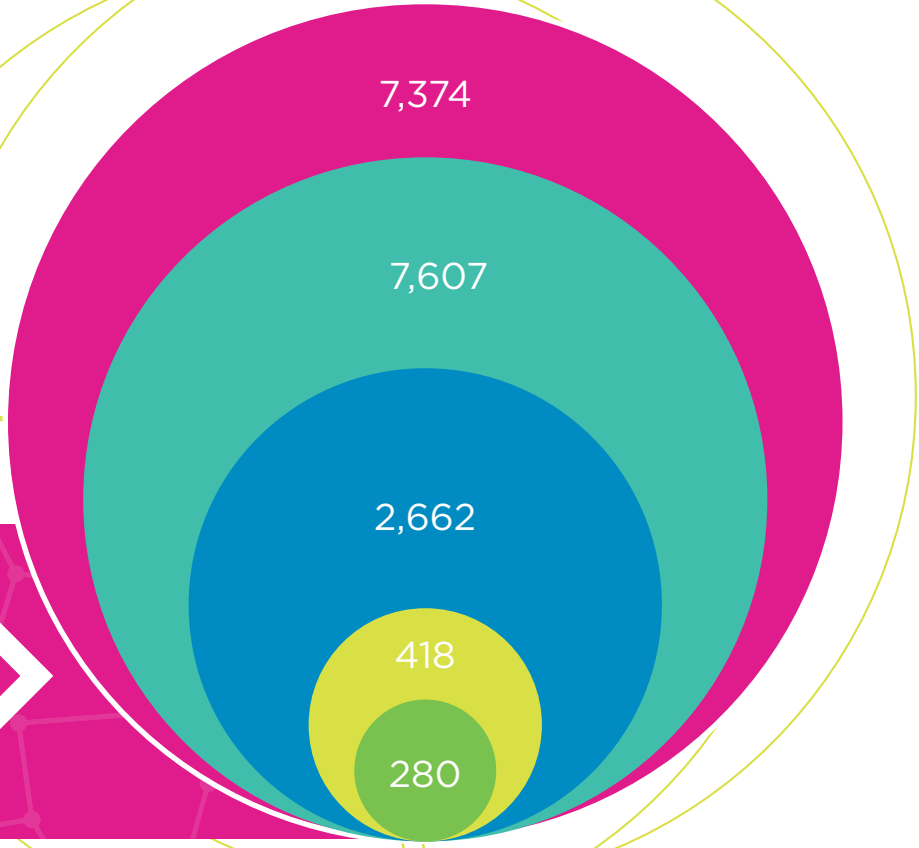
While Common Vulnerability Scoring System (CVSS) is an important aspect of understanding risks a vulnerability poses to an organization, it doesn't offer the full picture. Organizations using traditional remediation practices will immediately focus action on the 15% of critical-severity vulnerabilities, followed by the 42% of high-severity vulnerabilities. This means medium-severity vulnerabilities, which account for 41% of the total share, will sit unpatched for a prolonged time.

Some of the vulnerabilities that have the most pressing need for remediation could hide in plain sight: For example, a CVSS medium-severity vulnerability may be under active exploit in the wild while a critical-severity vulnerability has no exploit developed. In this case, the medium-severity vulnerability would pose a greater risk and is a higher remediation priority — even more so if it's exposed and unprotected by security controls.

Medium severity doesn't equate to medium risk: hackers see these vulnerabilities as an opportunity. They know security teams are distracted by remediating masses of critical- and high-severity vulnerabilities and they are ripe for attack. These vulnerabilities act as a "door opener," allowing attackers to gain lateral movement and deploy malware, such as trojans, to enable the deployment of more disruptive attack methods.

Severity score of all new vulnerabilities

- Critical
- High
- Medium
- Low
- Unknown



Medium severity doesn't equate to medium level risk

SKYBOX SECURITY

Scanning is just one part of the big picture

While vulnerability assessment and remediation are fundamental pillars of a robust security program, the scan-and-patch approach omits crucial elements of the vulnerability management workflow, especially in how remediation priorities are set. Scanners do not have a comprehensive understanding of network topology, therefore they can't identify the organization's actual exposure.

As security leaders work to mature their programs, taking a new approach to scanning is important. Scanners are useful when used as part of a holistic vulnerability management program. Security and IT organizations should also build an offline network model encompassing all network areas to understand connectivity and how risks could impact any part of the environment.

Importantly, data from scanning must be supplemented by data that scanners do not pick up such as CMBD data and network data. Further, threat intelligence and asset exposure data should be incorporated into analysis to better prioritize patches. Flexible remediation practices need to be established for non-patchable areas, such as those within OT environments, to eliminate the possibility of downtime — the model can be leveraged to identify patch alternatives.

I need to understand what the true risk is that I'm carrying.

"I look at data from scanners and say, so what? I need to understand what the true risk is that I'm carrying. I need to know what other controls I have in place, and whether I should put in time and effort to apply a patch. Failing to ask 'so what?' is a critical failure. To make the data useful, I need to know what needs to be patched first and what the order of patches needs to be."

Dr. Rebecca Wynn, CISO

Scanners do not have a comprehensive understanding of network topology, therefore they can't identify the organization's actual exposure.

Cloud misconfigurations present significant risk

The pandemic forced changes that increased the surface area for attack, including a rapid shift to cloud services. "Worldwide end-user spending on public cloud services is forecast to grow 18.4% in 2021 to total $304.9 billion, up from $257.5 billion in 2020, according to Gartner, Inc."[7]

Hybrid and multi-cloud deployments are opening up new cybersecurity challenges. Lack of visibility, misconfigurations and uncertified policies are all becoming more prevalent. Operations teams often underestimate security requirements within different cloud environments, with organizations accidentally introducing new risks as virtual assets are added. Security configuration settings, techniques and tools also vary significantly across various cloud services. This scenario makes it very challenging to incorporate policy changes and certify accuracy, consistency and continuous compliance. In fact, Gartner predicts "through 2023, at least 99% of cloud security failures will be the customers' fault."[8]

To avoid improper configuration, businesses need to enforce strict multi–factor authentication and be stringent with the authorization of managed policies. They need to know where all ingress and egress points are, who has access to them and have the ability to proactively respond to any potential attack vectors like misconfigurations.

Steady vulnerability increases within products also play a significant role in cloud infrastructure. Containers are a good example. Architecture leaders invest in container platform tools to enable improved developer productivity, software agility and reduce technical debt. However, a lack of adequate skills and mature DevOps practices can inhibit operationalizing and succeeding with large-scale production-grade deployment. Comprehensive container security starts in development with an assessment of the risk of the content of the container, along with configuration assessment.

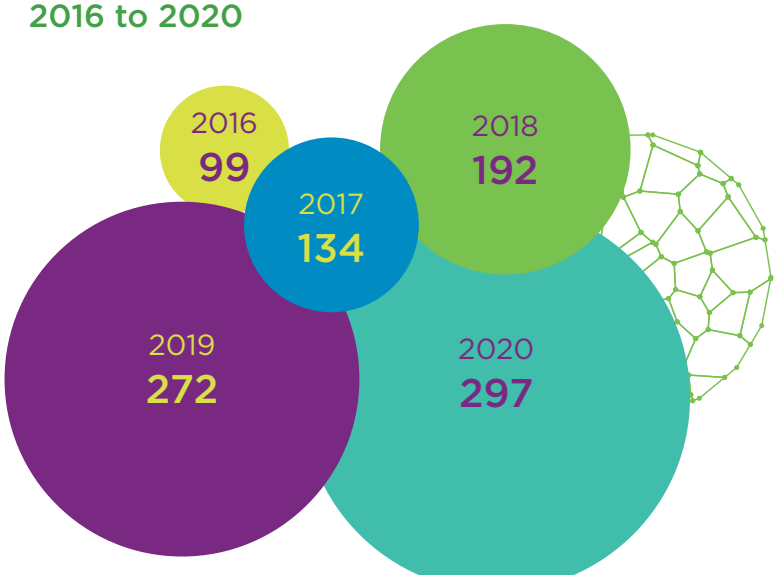
As the popularity of containers increases, so too do their vulnerabilities: Skybox Research Lab discovered a 200% increase in new container vulnerabilities between 2016 and 2020. This could post a significant threat as a container runtime vulnerability can enable container breakout and access to the host system.

To manage cloud security risk and prevent misconfigurations, leading organizations are developing network models. By aggregating data across cloud environments – including gateways, firewalls, routers and containers – network models can analyze paths end-to-end and easily identify violations. They can also be leveraged to automate rule, access and configuration compliance analysis across hybrid networks, giving continuous insight.

Containers defined

A container is software used to package production-ready networks, hardware and other components to embed standards into development and move solutions quickly across environments.

Container vulnerabilities, 2016 to 2020



[7] Gartner Press Release, Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021, November 2020

[8] How to make cloud more secure than your own data center", Gartner, October 2019

SKYBOX SECURITY

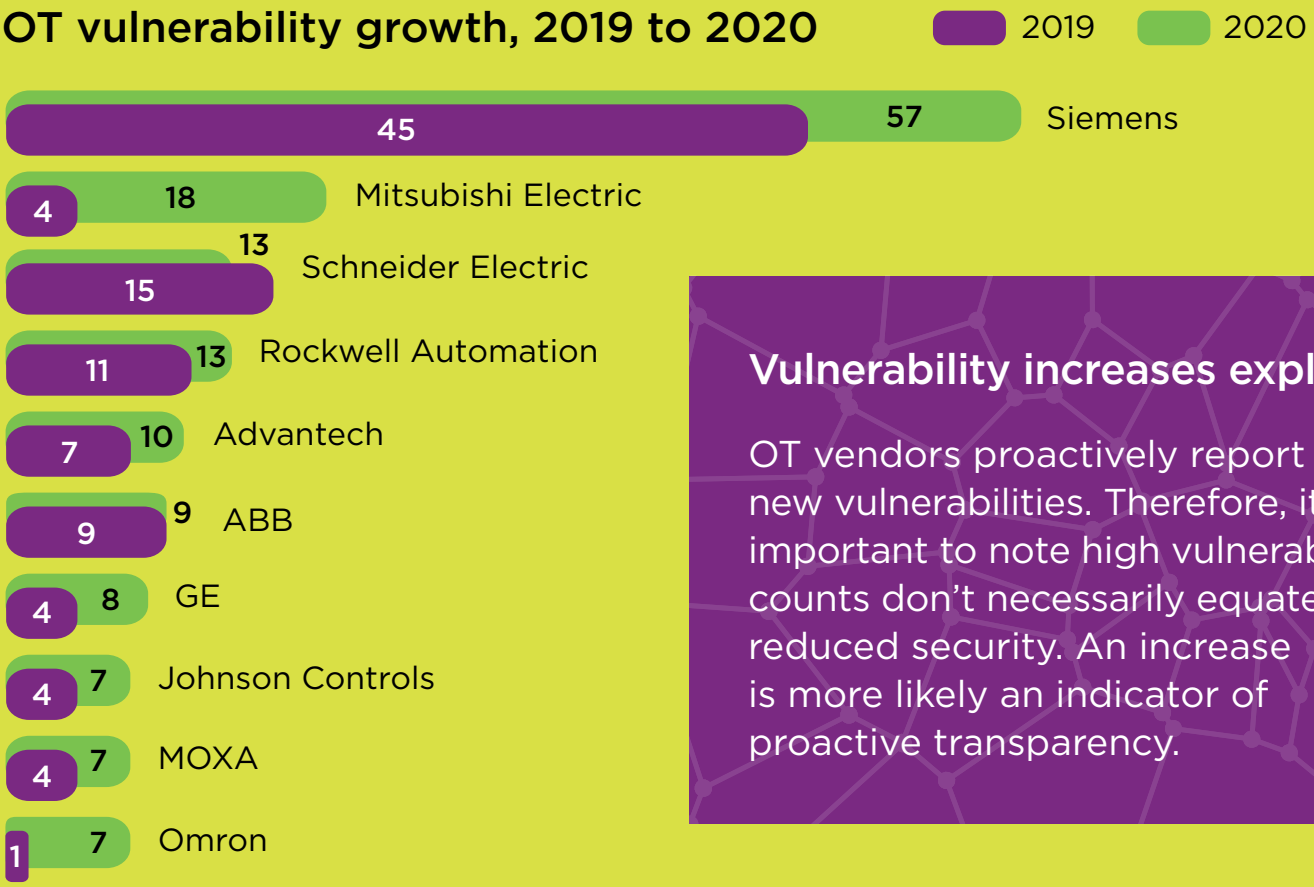
OT networks are under increased threat

Managing OT network security comes with several considerable challenges. These are massive environments that house critical technology that cannot experience downtime, cannot be scanned, run on either proprietary or outdated operating systems, prioritize safety over security, and are difficult to patch. These environments have always been attractive targets for attackers. Skybox Research Lab found Operational Technology (OT) vulnerabilities increased by 30% year-over-year which opens up considerable opportunity for threat actors.

Now that OT environments are no longer insulated from internet-derived risks, threat actors have seized on the opportunity: IBM reported a 2,000% increase in cybersecurity incidents targeting OT in 2019.[9] Further, 53% of manufacturing organizations believe their OT is vulnerable to attack,[10] and 37.8% of Industrial Control System (ICS) computers within the oil and gas industry fell victim to a cyberattack during the first half of 2020.[11] The number of advisories published by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a U.S. government entity considered to be the authority within the OT space, has dramatically increased by 30% to 224 advisories.

The quadrupling of Mitsubishi Electric vulnerabilities is notable. The Japanese corporation was a popular target with attackers in 2020, suffering multiple attacks that may have resulted in critical data being leaked, such as intellectual property associated with a prototype missile.[12]

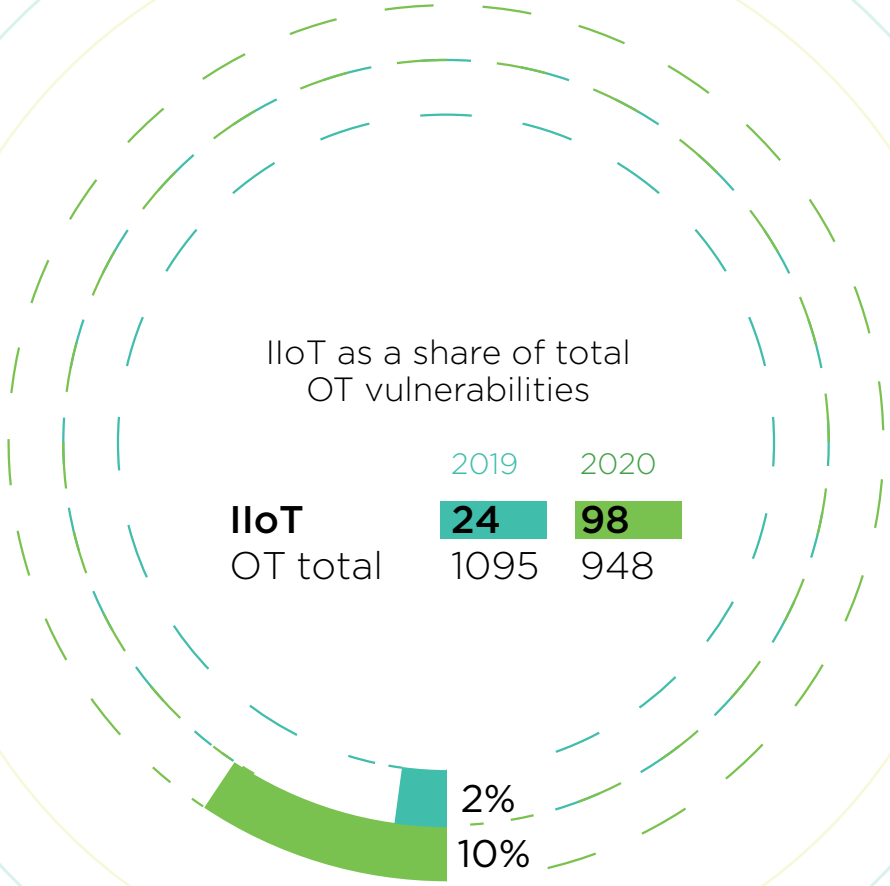
OT vulnerability growth, 2019 to 2020



Vulnerability increases explained

OT vendors proactively report new vulnerabilities. Therefore, it's important to note high vulnerability counts don't necessarily equate to reduced security. An increase is more likely an indicator of proactive transparency.

[9] IBM X-Force threat intelligence index, IBM, 2020
[10] Threat detection and response in manufacturing, Enterprise Strategy Group, October 2020
[11] Threat landscape for industrial automation systems. H1 2020, Kapersky, September 2020
[12] Mitsubishi data breach may have compromised "cutting-edge" missile tech, TEISS, 2020



An exponential increase in IIoT vulnerabilities

There is a pressing need for cybersecurity transformation within the OT space. These are networks that evolve quickly. A key sign of this evolution is the increasing adoption of Industrial Internet of Things (IIoT) technology and the speed with which vulnerabilities grow within these devices. Although IIoT vulnerabilities still only account for 10.3% of all OT vulnerabilities, the number of IIoT flaws grew by 308% over the last year.

The increase in IIoT flaws is concerning because the devices are known for their poor security levels. As IIoT product developers race to release new products ahead of competitors, product cycles are shortened. This has led to security issues being given lower priority.

Default passwords on IIoT devices are often weak and are even frequently posted online for faster device setup. If a customer fails to change to more secure passwords immediately, potential attackers can easily remotely hack IIoT products. Additionally, many IIoT manufacturers do not encourage customers to change default passwords. In some cases, passwords cannot be changed. Even when they can, customers are known to use weak passwords and permissive network communications, which allow the device to communicate with anyone. This is made worse with the revelation that 98% of IIoT device traffic is unencrypted.[13]

[13] 2020 Unit 42 IoT threat report, Palo Alto Networks, 2020

Examples of IIoT security issues are mounting. In June 2020, a series of vulnerabilities were discovered that allowed threat actors to control IIoT devices within oil and gas, manufacturing, nuclear and healthcare industries. These zero-day vulnerabilities affect hundreds of millions of IoT devices and, if exploited, can disrupt critical infrastructure.[14] Further, an IoT Mirai botnet downloader was discovered in July 2020 that can be added to new malware variants to identify points of intrusion.[15]

Vulnerable IIoT devices could be used to hijack critical functionality. For example, ladder logic (a graphical programming language) could be injected into a control device or programmable logic controller. If this low-level code, which is never refreshed, is inserted into a high-priority machine that is rarely, if ever, rebooted, it has a better chance of persisting over time.

The machines in question are usually air-gapped and communicate on proprietary, system-specific protocols, which makes finding a solution to the problem of new threats introduced by IIoT devices to old devices incredibly difficult.

Due to the increasing threat presented by OT and IIoT vulnerabilities, it is necessary to immediately adopt a new approach to vulnerability detection and management. Scans don't cover enough of the environment, and they happen too infrequently. It's not uncommon for applicable OT devices to only be scanned once or twice a year. The paradigm has shifted: Instead of focusing purely on detection and response, leading organizations are developing prescriptive and preventative security strategies.

[14] 19 Zero-Day vulnerabilities amplified by the supply chain, JSOF, June 2020
[15] Mirai Botnet attack IoT devices via CVE-2020-5902, Trend Micro, July 2020

Network device vulnerabilities decrease

Although overall vulnerabilities continue to rise, there was an anomalous 10% year-over-year decrease of flaws within network devices. These devices include firewalls, routers, switches and their operating systems. The reason for this could be deprioritization has led to fewer vulnerabilities being discovered — if this is the case, then we can expect to see a spike in the coming months. Or it could be the code itself is becoming more secure, with fewer innate vulnerabilities — if this is the case, then we might expect to see further declines in 2021 and beyond.

Regardless, a decline in new vulnerabilities isn't a signal that attacks may start to relent. If anything, the move to remote work has made CISOs more aware of the threat network device vulnerabilities pose. For example, scanners usually don't take into account the network security devices that can shield against potential exploits.
This gap has been a boon for malicious actors. Last year, product flaws within leading vendors, including D-Link[16] and Cisco[17], were laid bare. And because many of these new network device vulnerabilities put the network infrastructure itself at risk, network segmentation that has previously been used to circumvent "scan-and-patch" deficiencies is, by itself, not good enough anymore.

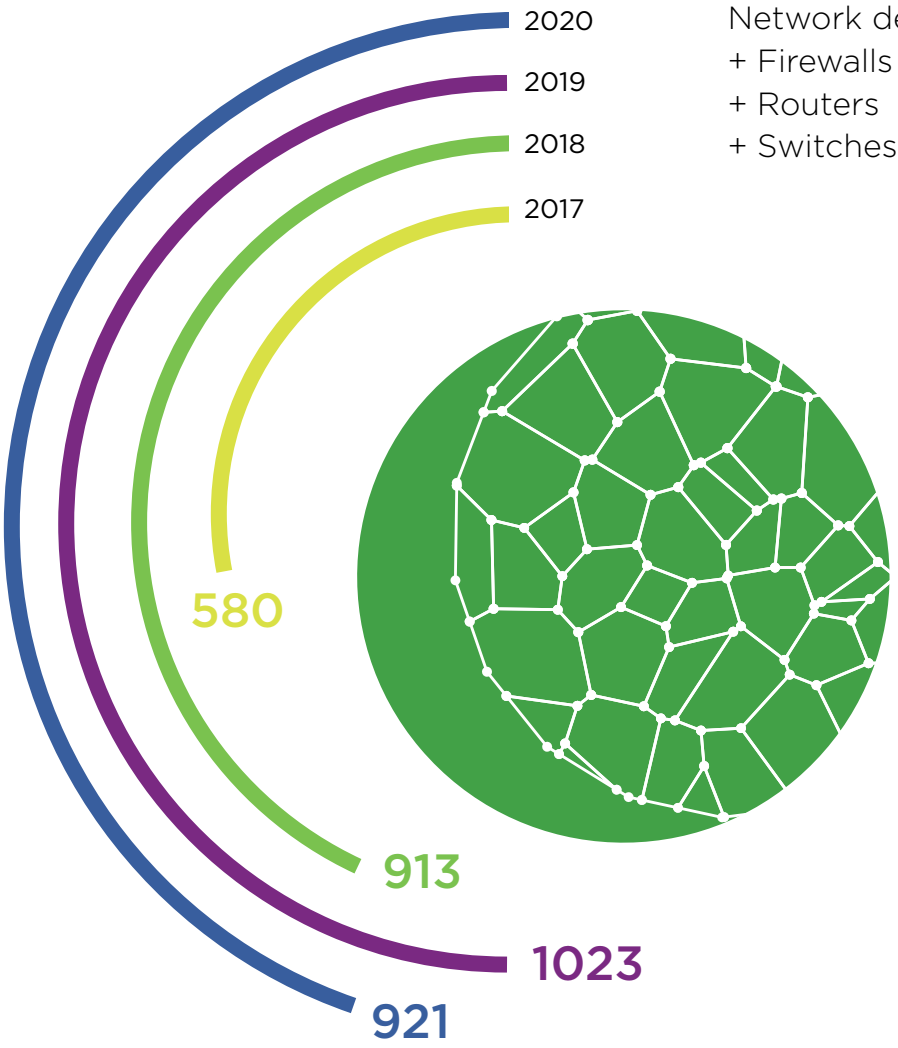
Left unchecked, network segmentation is not enough of a barrier for threat actors. They now have to gain a more holistic view of their networks, thinking not just about their own on-prem devices but about how to mitigate risk associated with MPLS. New upstream and downstream risks emphasize the importance of gaining visibility of all corporate network access points and being able to act quickly to eliminate threats.

Multiprotocol label switching defined

Multiprotocol Label Switching (MPLS) is data forwarding technology that increases the speed and controls the flow of network traffic. With MPLS, data is directed through a path via labels instead of requiring complex lookups in a routing table at every stop.

[16] Multiple D-Link routers found vulnerable to attack, Computer Weekly, December 2020
[17] Cisco warns of attacks targeting high severity router vulnerability, Bleeping Computer, October 2020

New network device vulnerabilities



Network device vulnerabilities include:
+ Firewalls
+ Routers
+ Switches and their operating systems

The broadening interface between home and organizational networks increased network devices' exposure to attacks

How to accelerate your security posture management journey

A new perspective has been embraced by security leaders who have long understood the value of maturing their programs. COVID-19 has created an inflection point for security: 59% of respondents to a recent McKinsey survey revealed innovation that offers inter-connectivity, automation and real-time data had been critical to their crisis responses during the pandemic.[18]

The benefits realized during lockdowns have set a foundation for further transformation. If successful in their efforts, CISOs will be able to address some of their longest-standing challenges — including complexity, talent shortages, expanding attack surfaces, fragmenting networks, visibility and remediation gaps — while improving defenses to tackle increasingly sophisticated threat actors. To achieve these benefits, organizations need agile security that can operate at scale, provides them with insight that enables rapid and targeted resolution of security issues, and continually fortifies security posture.

Addressing this dynamic landscape requires a transformation mindset. Maturing cybersecurity requires an approach that is focused on:

+ Gaining a deep understanding of unique business risk and impacts
+ Optimizing security technologies
+ Conducting precision oriented change management
+ Implementing intelligent automation of intermediate-level tasks
+ Developing prescriptive and holistic vulnerability management practices
+ Optimizing remediation across security, network, cloud, infrastructure, and operations teams

"2020 was an amazing year. People had five-year plans to transform their security programs, and then it all changed within two weeks. This is the only time in history when the main driver of change within the industry hasn't been threat actors. This time, it was a pandemic that caused a difference in the way that we conduct business. Luckily, technology was there to enable change. Now, we're back to traditional, massive breaches as the impetus for change. 2021 is the year cybersecurity is coming of age. It represents a new golden age — not one of being secure, but being able to be secure. We've still got a lot to learn. But now we're being smarter, and more disciplined about it. And we're going to keep moving towards maturity."

Richard Stiennon, author of "Security Yearbook 2020"

[18] COVID-19: An inflection point for Industry 4.0, McKinsey and Company, 2020

01 Gain greater insight

The modern cybersecurity environment has become incredibly diverse. To reduce risk and improve security posture across all network elements, organizations need to operate with a single view of compliance and operational security processes that can be aligned across the entire estate — including on-premises, OT, third-party and cloud networks. Through automating data collection, correlation and analysis, security and IT teams can together leverage a visual, interactive network model to understand risk levels, simulate attacks and remediate where it's needed most. Through attack simulation on a network model, it's possible to see all possible attack paths that can be taken by threat actors. The most exposed flaws are those inadequately protected, which could be accessible to attackers and which have active exploits.

02 Make smarter decisions

A new emphasis must be placed on achieving full context and understanding of the attack surface. This context augments scan data and enables organizations to identify and remediate the risk exposures that pose the greatest threat to the organization. A full life-cycle vulnerability and threat management approach enables organizations to gain complete visibility of all vulnerabilities across their entire attack surfaces, find the best remediation options that reduce the most risk and take appropriate action. Further, this approach increases efficiencies and scale across IT and security teams, frees up talent to support strategic initiatives, and creates value-rich security programs.

03 Remediate based on exposure

Organizations need insight that allows them to stop breaches before they happen. This can only be achieved when they understand how exposed their vulnerabilities are to attack.

By modeling the environment in which a vulnerability occurrence exists, teams can understand the exposure of vulnerabilities to threat origins — a critical component of risk-based vulnerability prioritization. Analyzing exposure takes vulnerability prioritization out of the theoretical realm. It places it in the real world, revealing which vulnerabilities are most likely to be used in an attack.

Exposure analysis is possible when disparate data repositories, such as patch and asset management systems, configuration data, threat intelligence feeds and network security devices are brought together, with data normalized and modeled to infer the presence of vulnerabilities. This sophisticated approach to remediation also requires:

+ Automation to enable rapid closure of security gaps
+ Insight from integrated data to accelerate decision-making
+ Breach and attack simulation capabilities to develop proactive defenses
+ Connected remediation processes to break down silos within the security stack

Exposure defined

Exposure isn't the same as exploitability. Some definitions of exposure refer exclusively to the vulnerability itself, explaining that an exposure is a "software error that allows hackers to break into a system."[19] Essentially, what this really means is the vulnerability is exploitable — whether or not there's an active exploit in the wild.

To fully understand how exposed each vulnerability is, it's important to understand this external threat context. If a vulnerability doesn't have a proof-of-concept exploit or isn't being actively exploited, then it poses a lesser threat. Further, exposure requires an understanding of the context of the vulnerability within the security environment.

[19] Common vulnerabilities and exposures (CVEs), Technopedia

Accelerate your security posture management journey

AD-HOC

+ Reactive and piecemeal
+ Functional and technological silos
+ Blind decisions based on a patchwork of data inputs
+ Sporadic remediation and patching

DEVELOPING

+ Periodic clean up of rules and objects
+ Periodic hardening of configurations
+ Periodic checking and manual recertification of compliance violations
+ Periodic patching to eliminate vulnerabilities

DEFINED

+ Documented policies and process to find and address configuration violations, with limited automation
+ Defined vulnerability management program, with no automation and consistent oversight

MANAGED

+ Informed decisions and consistent visibility based on quality, fresh data and insights
+ Change management automation
+ Vulnerability management automation – discovery, prioritization, remediation
+ Intelligent automation of intermediate level tasks
+ Monitor, report, quantify results of program to make changes as necessary

OPTIMIZING

+ Holistic visibility and analysis of the attack surface of the hybrid enterprise
+ Tight integration with the security and IT management ecosystem (SOC, SIEM/SOAR, ITSM)
+ Common platform and data sets for all teams dealing with security posture management and incident response
+ Contextual, optimized remediation for exposures
+ Context-aware change management

Methodology

The Skybox® Research Lab, the force behind the intelligence used by Skybox's solutions, has provided all information and data in this report without explicit reference. They are a team of security analysts who scour data daily from dozens of security feeds and sources and investigate sites on the dark web. The research lab validates and enhances data through analysis, based on their knowledge of attack trends, cyber events, and the TTP of today's attackers. Their ongoing investigations determine which vulnerabilities are being exploited in the wild and used in distributed crimeware, such as ransomware, malware, exploit kits, and other attacks exploiting client and server-side vulnerabilities. This analysis is incorporated into Skybox Vulnerability and Threat Management solution, which prioritizes the remediation of exposed and actively exploited vulnerabilities.

The Skybox Research Lab tracks tens of thousands of vulnerabilities on more than 8,000 products including:

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

New malware samples

Monitoring new malware samples is a manual process undertaken by the Skybox Research Lab. They continuously scour the dark web, monitor new advisories, and visit websites where exploit codes can be purchased to identify any new malware. This timely and validated intelligence is provided to Skybox customers on a daily basis, alongside information about malware properties. The data on the rise of malware in this report is extrapolated from these daily intelligence feeds.

Vulnerability counts

While the Skybox vulnerability database is updated daily with information from more than 30 different sources. This report is focused on the concentration of new vulnerabilities reported by the National Vulnerability Database (NVD) between January 1, 2020, and December 31, 2020. This report leverages NVD data to avoid counting vulnerabilties more than once. However, many vulnerabilities on the NVD are reported more than one year after first discovery. This lag is acknowledged in the report.

Vulnerability severity scoring

The vulnerability severity rating is based on Skybox Security's risk modeling methodology (CVSS V3 compliant), which takes various parameters into account. Common Vulnerability Scoring System (CVSS) base score ranges on a scale from 0 to 10.

Container vulnerabilities

The Skybox Research Lab collated vulnerability data from container market leaders, including Google Kubernetes and Microsoft Azure, as well as lesser known products from vendors including Cloudera and VMWare. In addition, vulnerabilities within dockers and docker containers were included. During the research process, the team identified and eliminated any replications. All data are derived from public containers and do not incorporate any vulnerabilities that may exist within custom, or otherwise private, containers.

Vulnerabilities within OT and IIoT devices

The report treats advisories issued by the Industrial Control Systems Emergency Response Team (ICS-CERT) as the main authority within the OT space. This distinction has been made because ICS-CERT count differs from CVEs; it's possible to have ICS-CERT advisories without CVEs or to have multiple CVEs within the same advisory. By focusing purely on ICS-CERT advisories, the report provides the clearest possible insight into new risk within OT environments. As such, all OT vulnerability data explicitly reflects new ICS-CERT advisories shared between January 1 2020, and December 31 2020.

To understand IIoT vulnerability increases, vulnerability data within IIoT products were isolated, any replication was removed, and vulnerability counts were collated.

Vulnerabilities within network devices

The Skybox Research Lab collated vulnerabilities within firewalls, routers, switches, and their OSs. Because there is a separate focus on OT and IIoT vulnerabilities within the report, these vulnerabilities were omitted from final network device vulnerability counts. The process used to collect these vulnerabilities started with a wide-reaching query so that all known vulnerabilities related to network devices could be captured. This query was then modified to filter out unrelated vulnerabilities – examples of omitted vulnerabilities include those on cameras and on Industrial Control Systems (ICSs). Finally, the data was further refined through research.

To keep up with the latest vulnerability and threat intelligence, visit **www.vulnerabilitycenter.com**.

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 now focus on the most strategic business initiatives while ensuring enterprises remain protected.

SKYBOX SECURITY