Device Security Threat Report

2025

paloalto NETWORKS | STRATA™

Table of Contents

Executive Summary

There's no doubt about it: We live in a device-oriented world. Consider how many devices you have in your own home—spanning cellphones and televisions to routers and your work laptop. Now, considering your organization, multiply that number by tens of thousands. Many organizations don't know how many devices are on their network or realize the significant risks that they pose.

Threats continuously evolve, making a proactive security program essential, by combining continuous external threat monitoring with robust internal capabilities for timely detection and response. Adversaries readily exploit knowledge gaps, including blind spots in asset inventories, unknown risks, deprecated protocols, default credentials, unmanaged applications, and overlooked dependencies.

Dangers of Unmanaged IT and IoT Devices

In this report, we dive into unprecedented statistics involving the danger of unmanaged IT, managed, and IoT devices, and provide short anecdotes on how enterprises can start thinking about solving them. Devices aren't inherently bad. They provide incredible value, speed, and convenience that connect us with the outside world. Ultimately, our goal is to surface the importance of holistically protecting these important devices, especially with the onset of AI-powered attacks.

To defend effectively, organizations must understand their environments better than any attacker ever could—across every device, every system, and every asset in the network. It is not enough to protect the crown jewels. An effective security posture must also account for what's vulnerable, untracked, and most likely to be compromised so security teams can proactively apply the necessary security controls and mitigations. Failure to do so directly translates to increased business risk, including potential operational downtime, financial losses from breaches, and damage to the organization's reputation. Adversaries thrive on gaps in knowledge: blind spots in asset inventories, unknown risks, deprecated protocols, usage of default credentials, usage of unmanaged applications, and overlooked dependencies.

Visibility as Your Strongest Defense

Actionable intelligence is the cornerstone of any modern cybersecurity strategy. This report digs into this concept by exploring the importance of how increased contextualized visibility enhances risk posture, prioritization, and mitigation, all essential in more effectively defending an enterprise network. While visibility serves as the foundational element of defense, it alone is insufficient. True visibility requires deep insights into device attributes, vulnerabilities, and interactions, not merely a count of existing devices. Such comprehensive, contextualized visibility is crucial for a strong security posture, enabling enhanced risk assessment, patching prioritization, and policy enforcement. It empowers organizations to fully understand their attack surface, pinpoint and prioritize risks, and apply precise security policies.

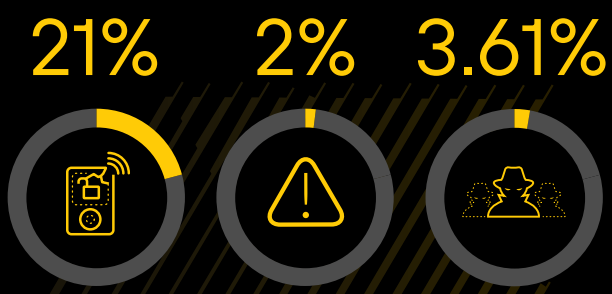
In this report, Palo Alto Networks researchers analyzed the telemetry data of a dataset that contained more than **27 million devices**, of which almost 23 million (84%) were IT devices and just over 4 million (16%) were IoT devices. In all, these devices belonged to 1,803 enterprise networks customers. This analysis highlights that, while visibility is the foundation, assessing deep contextual information—including vulnerabilities, security hygiene posture, communication patterns, and business criticality—is crucial for organizations to maintain a strong security posture.

To defend effectively in today's dynamic threat landscape, see how organizations must move beyond simple awareness to achieve a profound understanding of their entire environment.

Key Findings

Widespread vulnerabilities in IoT devices

Approximately 21% of all IoT devices have at least one known vulnerability. More critically, 2% of IoT devices are susceptible to Known and Exploited Vulnerabilities (KEV), meaning they're already being actively abused in the wild. Another 3.61% are affected by vulnerabilities with publicly available exploits (proof of concept [PoC] available), significantly lowering the technical barrier for attackers.

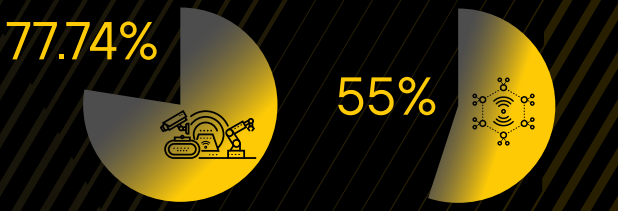


High-risk traffic from high-risk IoT devices

A substantial 48.2% of all observed connections from IoT to internal IT devices originate from high-risk IoT devices.

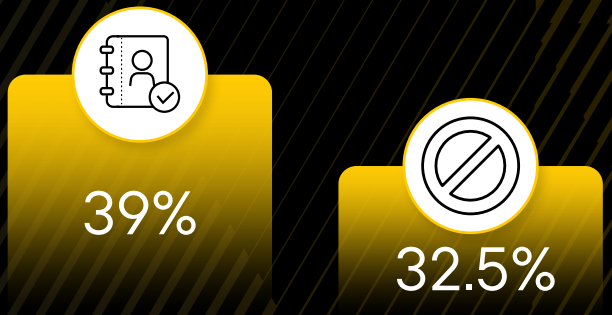
Flat networks increase risk

A majority of networks (77.74%) exhibit a low concentration of similar devices (mixed networks), with subnets containing a nearly even mix of IT and IoT assets (a 55% ratio).



Significant gaps in endpoint security coverage

Nearly 39% of IT devices registered in Active Directory (AD) lack an active endpoint detection and response (EDR) or extended detection and response (XDR) agent. Furthermore, 32.5% of devices in corporate networks are unmanaged, including, for example, IoT devices or bring your own devices (BYODs) that are incompatible with traditional agents. This expands the attack surface because they might not adhere to corporate security policies.



Top exploitation attempts

SSH authentication brute-force remains the most prevalent attack, with over 3.48 billion attempts recorded, underscoring the persistent threat of credential-based attacks. Apache Log4j remote code execution (RCE) also shows a substantial 2.7 billion attempts, highlighting the continued exploitation of critical software flaws.

For IoT devices specifically, routers RCE vulnerabilities are a major concern, with over 15.4 million occurrences observed.

3.48B+
SSH AUTHENTICATION BRUTE-FORCE ATTACK ATTEMPTS

2.7B
APACHE LOG4J REMOTE CODE EXECUTION ATTEMPTS

15.4M+
ROUTERS RCE VULNERABILITIES

Most vulnerable device types

Devices with the highest number of distinct known vulnerabilities (Common Vulnerabilities and Exposures [CVEs]) include video conference and video streaming devices, network equipment, personal computers, and IT servers.

The Network Is the First Act of Defense

Understanding the network is the first act of defense, because visibility forms the foundation of any effective security strategy. An organization cannot protect its assets if they're unknown or seen, nor can it secure them without understanding their specific risks.

Our analysis of network environments highlights several critical layers of visibility that are often overlooked. The initial challenge is establishing a complete asset inventory. While traditional IT systems make up the majority at 84% of devices, 16% consist of IoT devices, which frequently fall outside of standard management and security programs.

Our analysis also shows that an average organization's network hosts approximately 34,075 connected devices, comprising roughly 80 distinct device types. The scale of this device population makes manual monitoring impractical and necessitates security solutions that can operate effectively across tens of thousands of endpoints. More importantly, the diversity of these assets, which span traditional IT, IoT, and BYOD categories, introduces significant complexity. Each device type has a unique operating system, management capability, and risk profile, rendering a single, uniform security policy ineffective.

IT Device Categories

The vast number and variety of IT devices connecting to enterprise networks create a massive and complex attack surface. Every endpoint, from a corporate-owned laptop to a personal mobile phone, is a potential entry point for cyberthreats. To effectively manage this expanding risk, security teams must first understand the landscape. This section breaks down the most prevalent categories of IT devices found on modern networks and highlights the unique security challenges they introduce.

Personal Computers

Personal computers, including both company-owned devices and personally owned BYODs, are the most prevalent IT device category, accounting for approximately 71.1% of IT devices. They can be compromised via phishing or other social engineering attacks, as well as with malware, like ransomware and Trojans.

Mobile Devices

These devices, such as smartphones and tablets, account for approximately 24.3% of IT devices. A significant security concern arises from these devices, because many are unmanaged or BYOD and might not be subject to corporate security policies and controls. Combined, unmanaged devices and BYOD highlight the continued importance of end-user devices in the overall IT landscape of an enterprise network.

Organizations must implement robust endpoint security that extends beyond traditional corporate-issued devices. They must address risks like phishing, social engineering, and malware, as well as ensure consistent policy adherence. A single successful phishing attack or malware infection on one of these devices can directly lead to a company-wide data breach or ransomware event. Therefore, the strategic priority must be a defense-in-depth approach for endpoints.

Virtual Machines

This notable category underscores the widespread adoption and critical role of virtualization technologies in modern IT environments. The frequent lack of enforced or verified security policies for virtual machines operating on personal computers creates a significant risk.

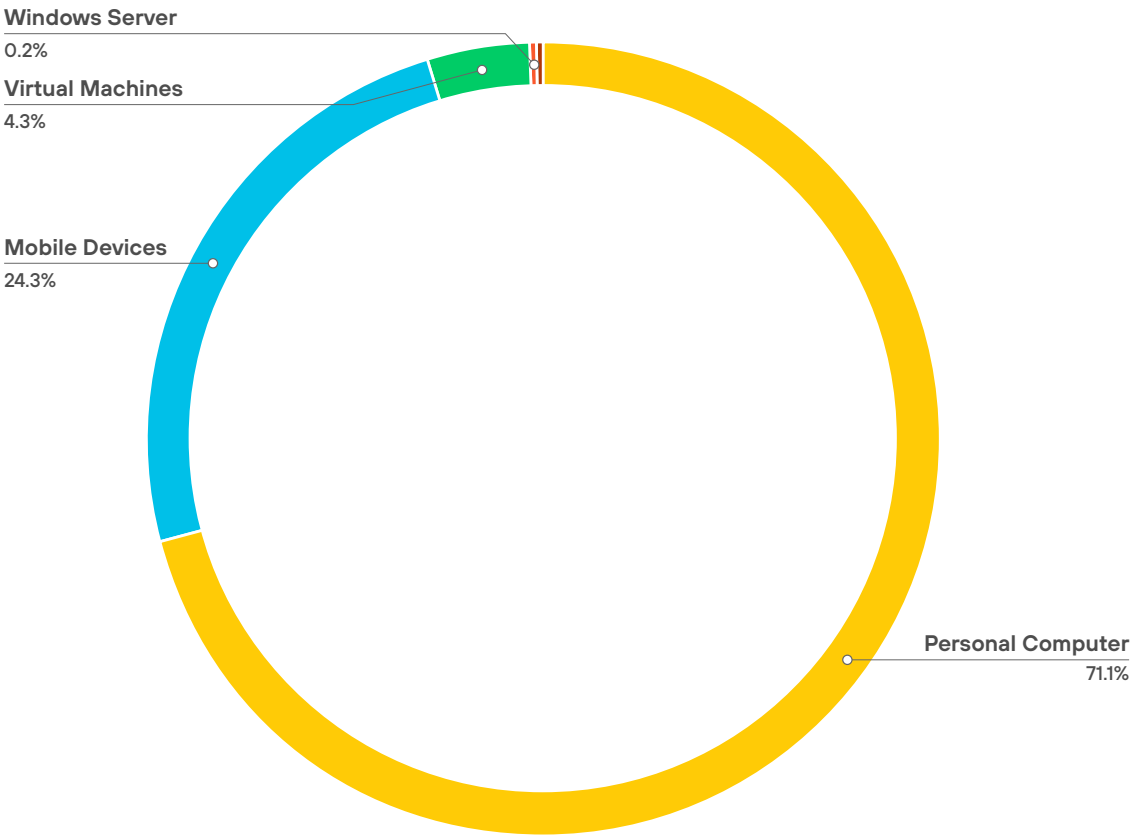


Figure 1. Top IT device categories

Key IoT Device Categories Excluding Network Devices

The security implications of the IoT device landscape are significant. IP cameras, for instance, are known for being vulnerable and serve as a common entry point for attackers. These devices are prime targets for being co-opted into massive botnets, the primary type of malware that affects IoT devices.

The following categories are within the IoT landscape of enterprise networks.

Consumer Electronics

Consumer electronics, such as virtual assistants, is the dominant category and represents 26.5% of all devices. It also highlights a significant presence of general consumer devices, accounting for almost one-third of the total device count.

IP Cameras and Video Gaming

IP cameras, which represent 15.9% of devices, are present in almost every organization. Video gaming (13.7%) is commonly found in, for example, corporate break rooms, hospital pediatric wards, and resorts. Both are substantial categories that, collectively, make up over a quarter of the devices and indicate a strong focus on entertainment and smart-home technologies.

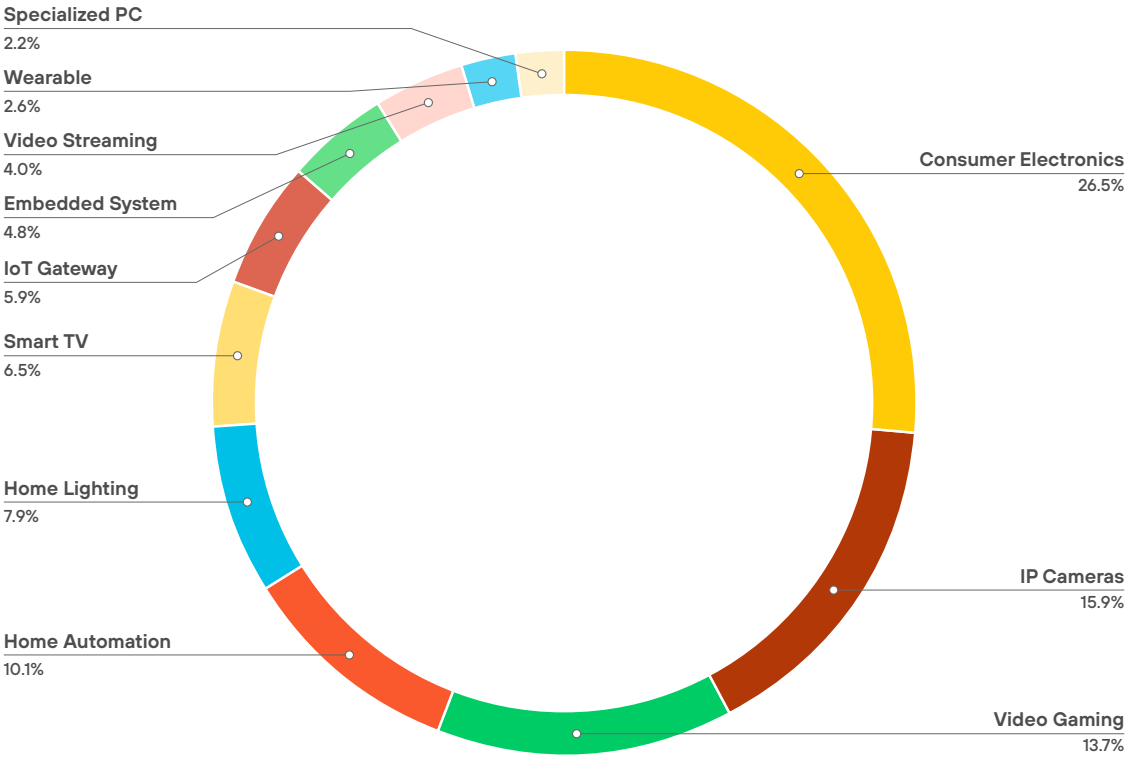


Figure 2. Distribution of the top IoT device categories

IoT Device Count Over the Past Year

Figure 3 illustrates the growth trajectory of the IoT device population from a dataset of 90 paid customers with the most presence of IoT devices from May 2024 through May 2025.

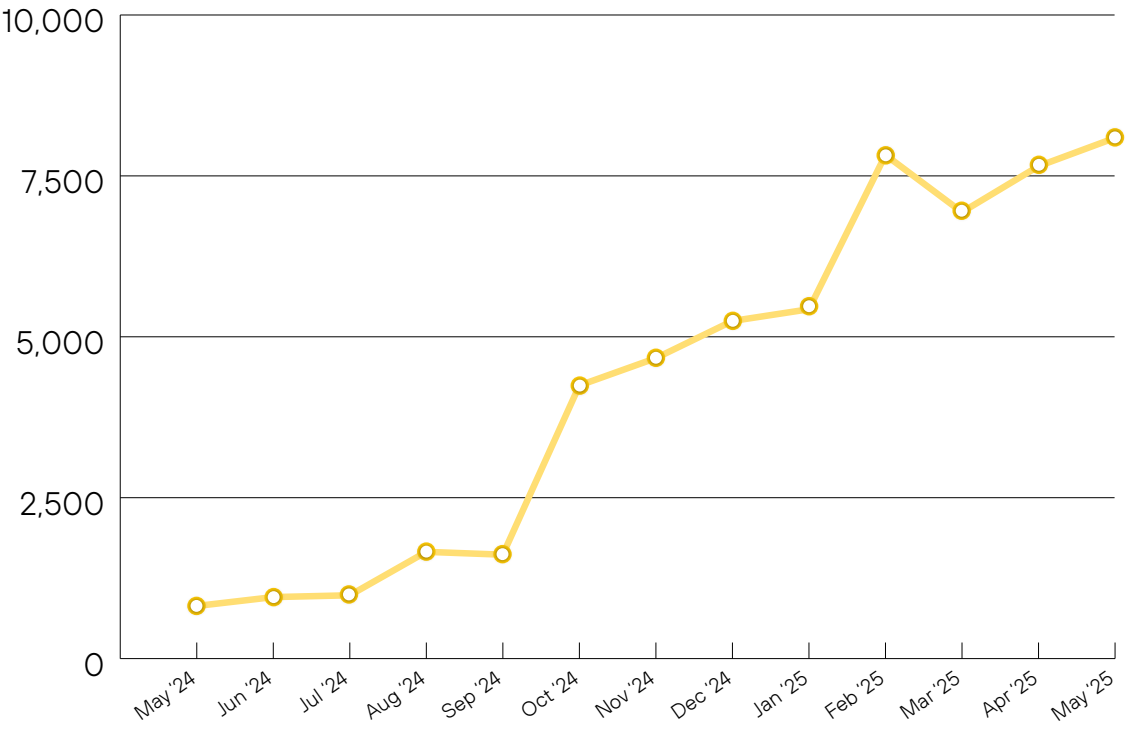


Figure 3. Growth of IoT devices over time

A key finding from the data is the acceleration in device growth observed through early 2025. Despite initial fluctuations, the overall data reflects a clear and consistent upward trend in the device population over the entire period. This growing trajectory became more pronounced after the start of this year, confirming the continued phase of rapid and sustained adoption of IoT devices in enterprise networks.

During this time, the following top categories had the most growth, shown in order of most growth to least growth:

1. Video audio conference
2. Physical security
3. Network security equipment
4. Smart building systems
5. Digital signage
6. IoT gateway
7. Energy management
8. VoIP communications equipment
9. Smart plugs or outlets
10. Smart TV or IPTV

The rapid growth of IoT devices requires organizations to scale their security strategies accordingly. Without doing so, the attack surface will continue to expand, creating more blind spots as unmanaged or poorly secured IoT assets become part of the enterprise network.

Visibility and Risk Assessments Yield Faster Identification and Mitigation

Combining comprehensive visibility with robust risk assessment, classification, context, and control directly results in better and faster threat identification and mitigation. A direct outcome of achieving comprehensive network visibility is the ability to conduct markedly better and faster risk assessments.

An assessment becomes "better" when it's context-aware. Instead of identifying a vulnerability, full visibility enables a security team to evaluate that vulnerability based on the affected asset's business criticality, network exposure, threat landscape, and the presence of any compensating controls. This way, teams can prioritize genuine threats over low-impact findings.

When asset inventory, vulnerability and threat data, and network topology are unified, security analysts can almost instantly identify and triage complex risk conditions that would otherwise take days to piece together. This combination of speed and accuracy enables security programs to shift from a reactive to proactive posture so they can remediate the most critical risks before they're exploited.

Devices Running on Unsupported Operating Systems

Devices that run on unsupported operating systems pose a persistent risk to organizations. Some of them are associated with end-of-life (EoL) devices, which no longer receive vendor support, including critical security updates or troubleshooting assistance. While some of these devices might continue to function, they increasingly become vulnerable to known exploits and misconfigurations over time. Others stop operating entirely, turning into electronic waste if not properly decommissioned.

In some cases, attackers with physical access to the disposed device can retrieve sensitive data from discarded or neglected devices that weren't securely wiped. For IT and security teams, managing the full lifecycle of assets, from procurement through secure retirement, is essential for both minimizing risk and optimizing operational efficiency, as well as reducing long-term costs and environmental impact.

Our data shows that, even within a managed infrastructure, critical risks can persist. Approximately 7.87% of all Windows systems,[1] including Windows servers,[2] as well as a notable 26.4% of Linux systems are running unsupported versions (EoL versions) that no longer receive security patches.[3] These figures demonstrate that, without a comprehensive and multilayered view of inventory, exposure, and lifecycle state, an organization's defensive posture will remain fundamentally incomplete. The continued use of EoL systems exposes an organization to unpatchable vulnerabilities, creating a permanent and easily exploitable entry point for attackers. This increases the risk of a costly data breach and can lead to audit failures and noncompliance with regulatory requirements. A strategic decision to prioritize and fund a hardware and software refresh cycle is crucial to mitigate this persistent threat.

7.87%

of Windows systems, including Windows servers from our dataset, are running an EoL version of the Windows operating system

26.4%

of Linux Systems from our dataset are running an EoL version of the Linux Kernel

1. "Microsoft Windows," endoflife.date, updated August 10, 2025.
2. "Microsoft Windows Server," endoflife.date, updated August 10, 2025.
3. "Linux Kernel," endoflife.date, updated October 1, 2025.

Some threat actors are known to target EoL devices as part of their operations. One example is Volt Typhoon, a group linked to the Chinese government that focuses on gaining long-term access to critical infrastructure networks. Their tactics include exploiting unpatched vulnerabilities in routers, firewalls, and IoT systems that have reached EoL status. These devices often remain deployed in industrial or enterprise environments despite lacking support or updates. Because they're no longer maintained, they can serve as ideal entry points or staging areas for lateral movement, persistence, or command and control. This reinforces the importance of full asset lifecycle management and timely decommissioning of unsupported systems.

Exploitation Attempts Across IT and IoT Devices

From our Advanced Threat Prevention solution telemetry, it's possible to observe the top exploit attempts.

Figure 4 shows significant trends in different types of exploitation attempts. It highlights the most frequently targeted services, of which the most notable are:

- **SSH user authentication brute-force attempt** stands out as the most prevalent attack, with over 3.48 billion recorded attempts. This underscores the persistent threat of credential-based attacks.
- **Apache Log4j RCE vulnerability** follows closely, showing a substantial 2.7 billion attempts, demonstrating the continued exploitation of this critical software vulnerability.
- **HTTP directory traversal request attempt** also represents a major concern, with over 1.57 billion attempts.

The attacks against Zyxel products are the only ones making it the most attempted IoT attack from our dataset, specifically the vulnerabilities identified with the CVE-2023-28771 and CVE-2020-9054.

These figures collectively emphasize the critical need for organizations to implement robust security protocols. The protocols must be focused on strong authentication mechanisms, timely patching of known vulnerabilities like Log4j, and a comprehensive defense against common web-based attacks to prevent the most frequently attempted breaches.

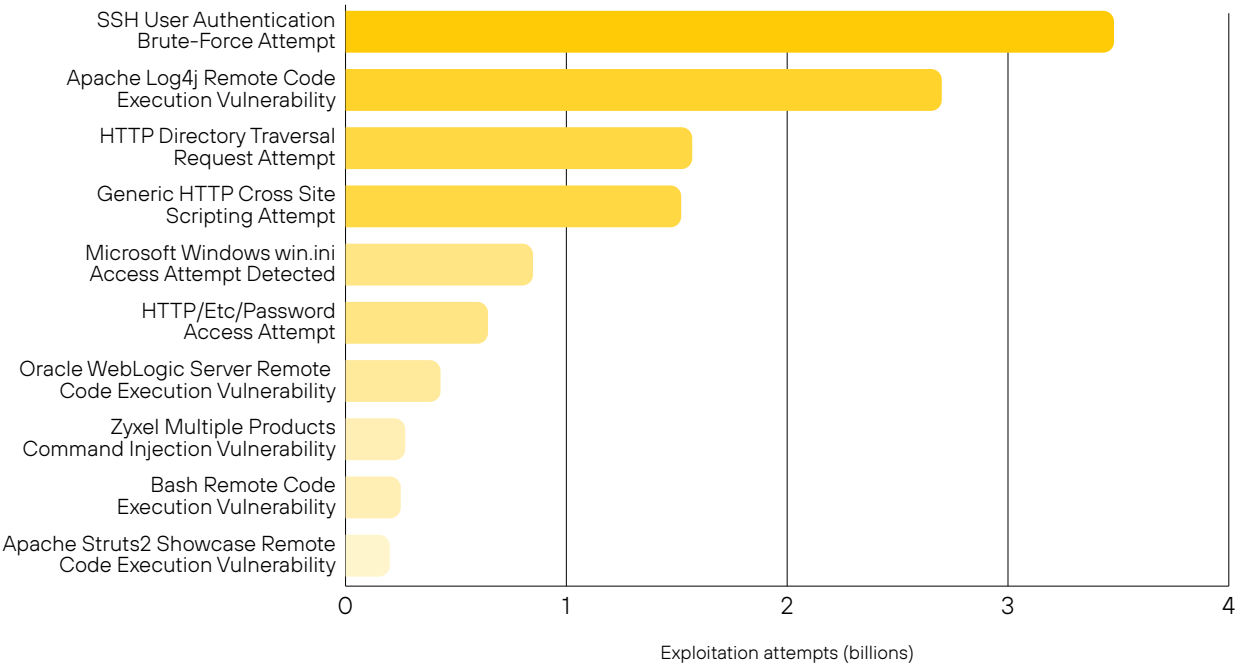


Figure 4. Top exploitation attempts by attack type

Prevalent Exploitation Attempts in IoT Devices

Excluding Zyxel devices, the top exploitation attempts for IoT devices include:

- **D-Link routers RCE vulnerabilities (CVE-2020-25506 and CVE-2016-11021)** stand out as the most prevalent (after exploitation attempts against Zyxel devices), with over 15.4 million recorded occurrences.
- **Netgear ProSAFE Plus unauthenticated RCE vulnerability (CVE-2020-26919)** follows with approximately 7.66 million. Close behind is **Micro Focus Operations Bridge Reporter RCE vulnerability (CVE-2021-22502)** with 7.61 million counts. These figures underscore the critical importance of addressing remote code execution vulnerabilities, particularly in consumer network devices.
- **MVPower DVR TV RCE vulnerability (CVE-2016-20016)**, for example, show high counts at around 1.23 million. The data highlights a significant concern with video surveillance equipment vulnerabilities.
- **CVE-2023-26801**, a command injection vulnerability affecting certain **LB-LINK BL-AC1900** routers, has shown the highest growth rate in exploitation attempts since its disclosure.

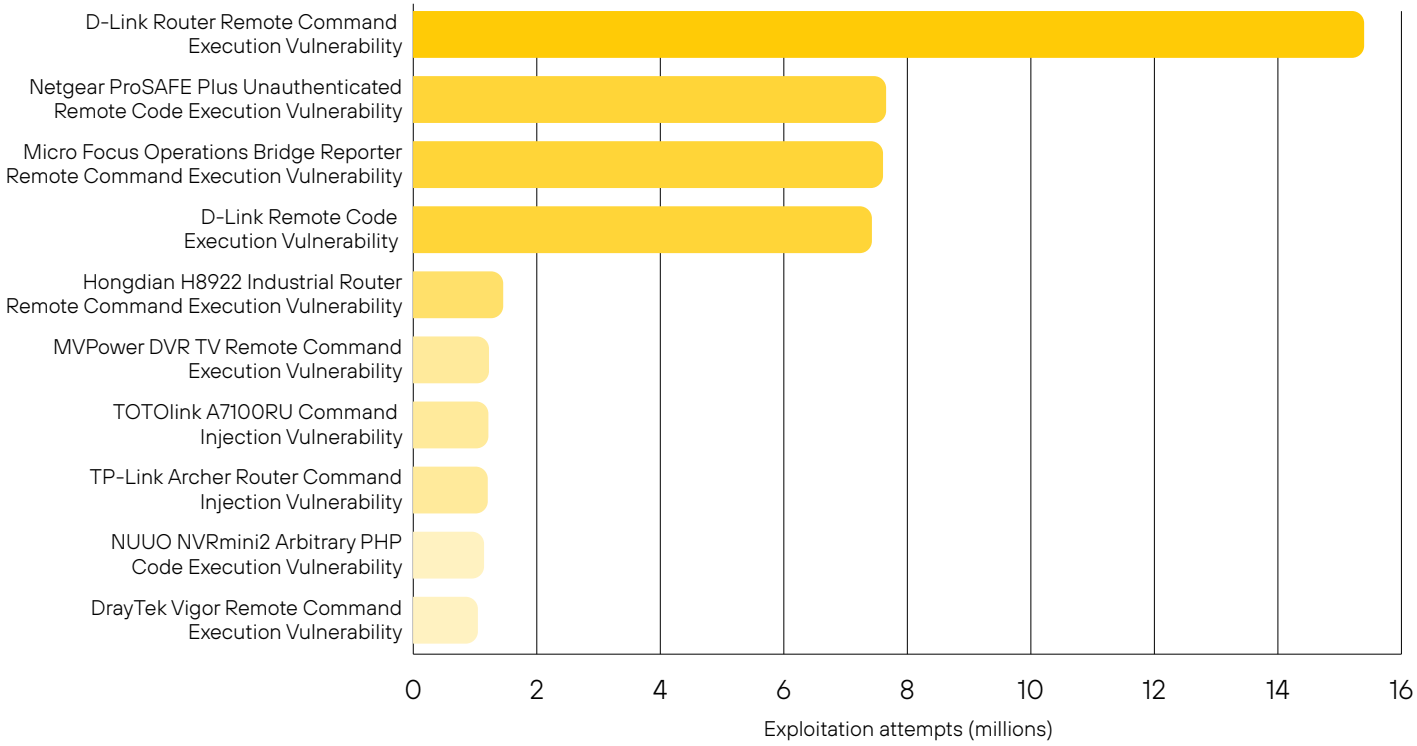


Figure 5. Prevalent exploitation attempts of IoT devices

A large number of these devices are unsupported and no longer receive security patches, making their vulnerabilities a critical point of risk. Mitigating them requires contextual device visibility and stronger security controls to prevent widespread exploitation. Overall, the telemetry highlights how IoT environments remain a prime target. A major number of devices are exposed to vulnerabilities that are both known and, in many cases, actively exploited and weaponized. This underscores the need for better visibility, firmware hygiene, and targeted mitigation efforts across the IoT landscape.

Additionally, around 21.29% of the IoT devices in our dataset have at least one known vulnerability, whether a public exploit or PoC is available. While these weaknesses aren't currently identified as being used in attacks, their widespread presence indicates a broad potential for future exploitation, especially as more vulnerabilities are discovered and weaponized over time.

Even more concerning, around 2% of IoT devices in our dataset are susceptible to KEV, meaning they're tied to ongoing campaigns and are already being abused in the wild. This reflects real-world exploitation observed across different environments.

Looking at vulnerabilities with a publicly available exploit but with no observed exploitation yet, 3.61% of IoT devices are affected by vulnerabilities with publicly available exploits. These significantly reduce the technical barrier for attackers, enabling automated exploitation and integration into commodity malware.

Finally, 0.49% of IoT devices are vulnerable to issues known for their use in malware or found in exploit toolkits. This suggests that a considerable portion of the IoT footprint is already being leveraged or remains at high risk of future targeting.

Table 1. Vulnerable Devices by Exploit Availability

Category	Percentage	Number of Devices
Weaponized	0.49%	21,567
Exploited in the wild	1.96%	85,371
PoC available	3.61%	157,242
No exploit available	20.18%	880,232
No associated vulnerabilities	78.71%	3,432,791

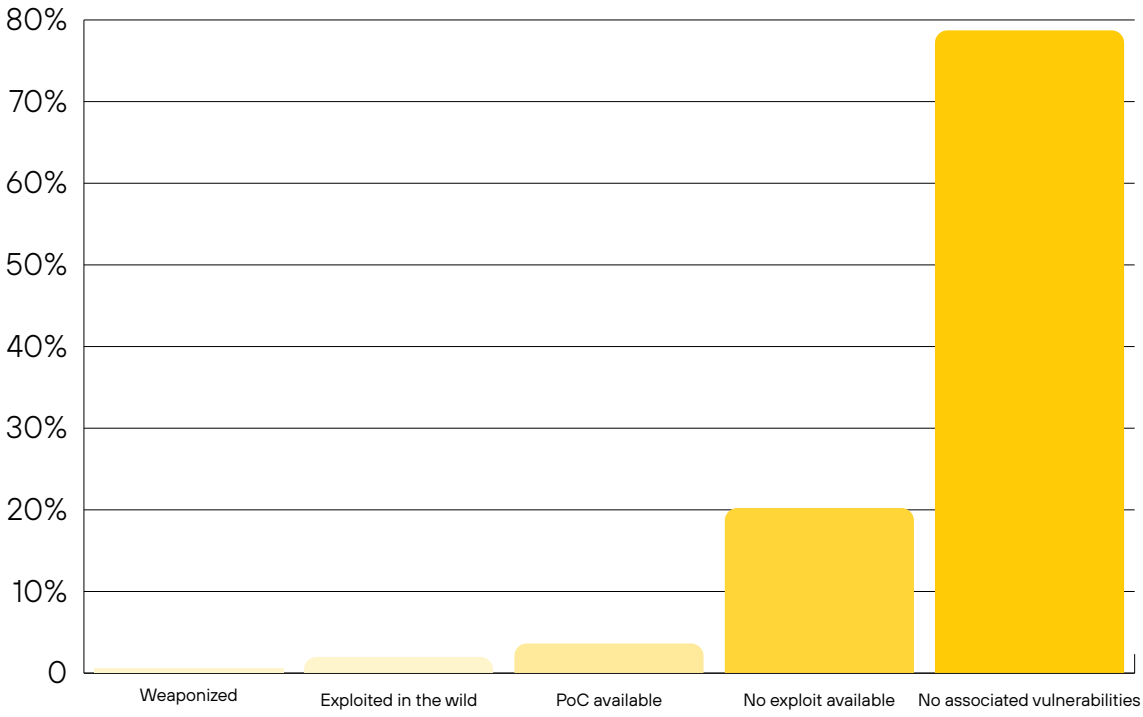


Figure 6. Vulnerable devices by exploit availability

Effective vulnerability management requires knowing which flaws to fix first. For instance, information showing that a vulnerability has a publicly available exploit (PoC) or is already being used in active attacks enables teams to distinguish a theoretical weakness from an immediate danger. This intelligence enables security teams to focus their resources on patching the vulnerabilities that pose a genuine and urgent threat to the organization, rather than just relying on static severity scores.

Most Vulnerable Device Types

Figure 7 lists the device types associated with the highest number of distinct known vulnerabilities (CVEs) observed in our dataset. This ranking reflects the disclosed security vulnerabilities affecting each device type, regardless of exploit availability or prevalence in the environment. While some of these systems are widely used in enterprise networks, such as personal computers, servers, and network equipment, others represent categories that are often part of collaboration tools or consumer IoT devices.

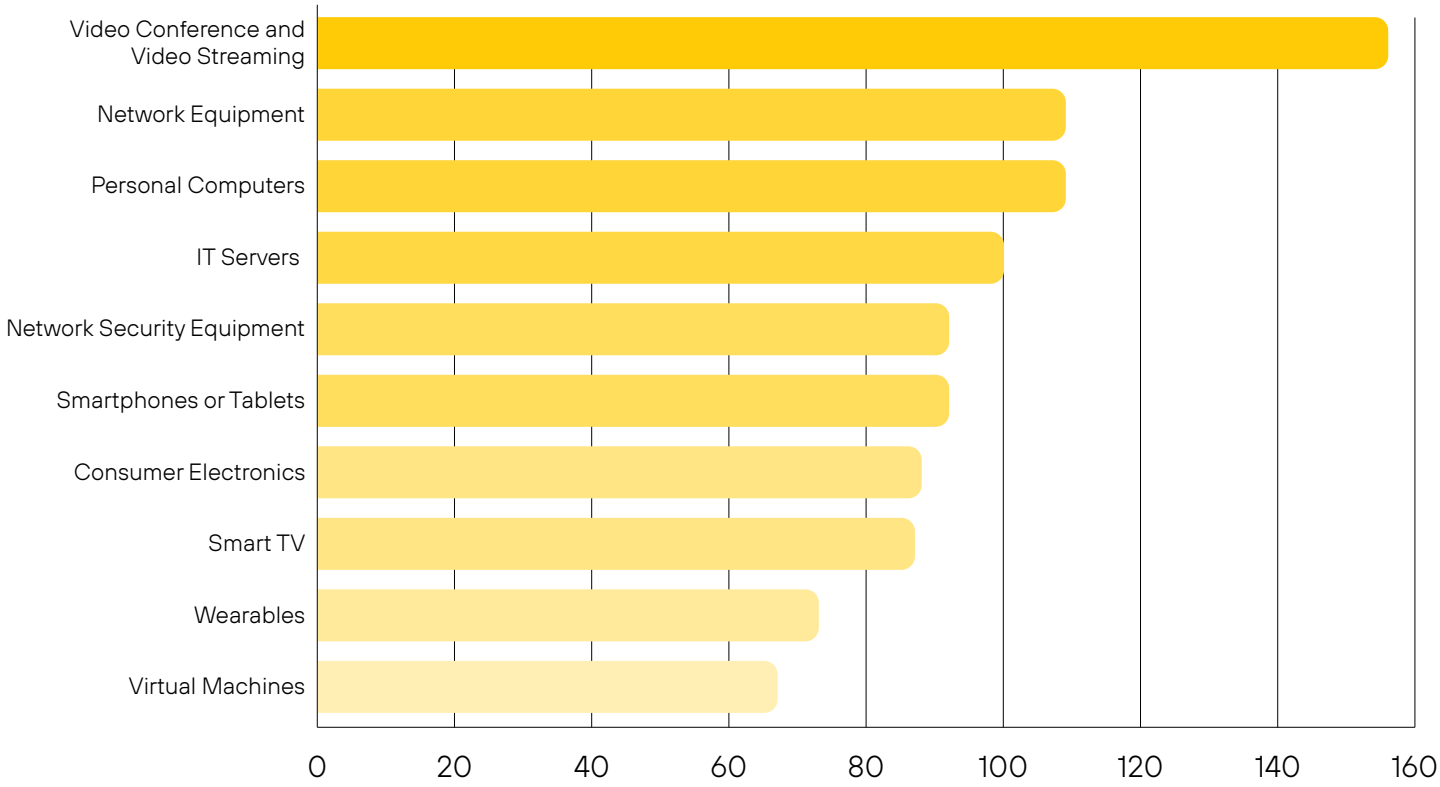


Figure 7. Device categories account for the highest number of known vulnerabilities

As shown in figure 7, device categories—such as video conferencing systems, video streaming devices, network equipment, and personal computers—account for the highest number of known vulnerabilities. These types of devices are present in most enterprise networks and often operate with broad access to internal services or user data, making them attractive targets for attackers. Monitoring the volume of unique CVEs associated with each category helps organizations identify which types of devices require broader patching strategies and long-term vulnerability management planning. Focusing remediation efforts here can significantly reduce the appeal of these high-value targets to attackers.

By developing a clear understanding of the threats that are most relevant to their specific environment, organizations can make more effective strategic decisions. This enables security leaders to better allocate resources, implement appropriate controls, and ultimately improve their overall risk management posture.

Insecure Protocols

Despite advances in endpoint and network visibility, insecure protocols remain common across connected environments. From our dataset of over 27 million devices:

- **SNMPv1**: Around 2 million devices (7.4%) still use SNMPv1, an outdated protocol known for weak authentication and exposure risks.
- **FTP**: Over 650,000 (2.4%) devices have FTP, a protocol with no built-in encryption.
- **Telnet and SMBv1**: Telnet (44,085 devices [0.162%]) and SMBv1 (31,421 devices [0.116%]), both long deprecated due to their susceptibility to interception and abuse, still appear in the dataset.
- **NTLMv1 and LLMNR**: NTLMv1 (431 devices [0.002%]) and LLMNR (23,992 devices [0.088%]), despite having a low percentage, their continued presence reflects gaps in protocol hardening.

These legacy protocols expand the attack surface and provide low-effort entry points for attackers already present inside the network. Disabling or replacing them with more secure alternatives is a critical step in reducing exposure and improving baseline security hygiene.

Cross-Domain Exposure Creates Attack Paths

Enterprises underestimate their complexity. Broader awareness yields better decisions.

Proactive Risk Assessment

Manual risk assessment is often subject to cognitive biases. A common tendency is to fixate on the severity of a potential outcome, which can lead to an inaccurate perception where the most severe risk is incorrectly viewed as the most probable one. Our risk score calculation incorporates multiple data sources to produce a detailed assessment.

Vulnerability analysis includes the base Common Vulnerability Scoring System (CVSS versions 2 and 3) score, the likelihood of exploitation as measured by the Exploit Prediction Scoring System (EPSS), and the current exploit status of the vulnerability. This calculation also considers the device's operational state. The factors include, for example, running an unsupported operating system, patchability, having direct internet exposure, the presence of an EDR or XDR agent, and the presence of both active security alerts and policy violation alerts.

The calculated technical risk is then adjusted using the device's assigned asset criticality, resulting in a final score that represents its overall risk to the organization. The result is a qualitative value: low, medium, high, and critical. This analysis can help organizations move from an undefined risk posture to a clearly identified, quantifiable, and controllable inventory.

The data also indicates that 48.2% of all observed connections originate from devices classified with a high-risk score. This large volume establishes a broad and persistent attack surface, pointing to a systemic issue where devices with notable risk factors, such as unpatched vulnerabilities or insecure configurations, are actively communicating with internal systems.

Within this high-risk traffic, a smaller and more urgent subset of devices was identified. A total of 4% of all connections originate from devices rated as critical risk. These devices represent the most severe problems, because a critical score is reserved for assets that exhibit drastic technical risks combined with high business importance, as defined by the scoring model.

This level of communication provides a direct path for security threats to spread from a compromised IoT device to core business systems. A successful breach along one of these paths could result in a disruption of business operations, sensitive-data compromise, and considerable financial costs.

This finding suggests that unrestricted communication between high-risk devices and critical assets is a notable security liability. Therefore, a strategic decision is to invest in and enforce network segmentation policies. By isolating high-risk devices from the broader network, an organization can effectively block these potential attack paths. This practice protects critical operations and helps ensure business continuity if an individual IoT device is compromised.

48.2%

of all connections from IoT to internal IT devices are from **high-risk IoT** devices

4%

of all connections from IoT to internal IT devices are from **critical-risk IoT** devices

Poorly Segmented (Flat) Networks

Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. This allows network administrators to control the flow of network traffic between subnets based on granular policies. Organizations use segmentation to improve monitoring, boost performance, localize technical issues, and most importantly, enhance security. The consequences of inadequate network segregation include: insufficient isolation, lack of granular control, increased attack surface, and easier lateral movement.

The quality of a subnet segment depends on the concentration of a device type in a subnet. A higher degree of network heterogeneity correlates with a higher exposure. To identify signs of weak network boundaries, we analyzed subnets that contain both IT and IoT devices. A subnet is considered inadequately segmented if it doesn't have a clear majority of one device type. This applies specifically if neither traditional IT devices (such as laptops and servers) nor IoT devices account for the devices on that subnet.

Table 2. Percentage of Segmentation Distribution vs. Network Segment Purity

Segmentation Distribution	Network Segment Purity
77.74%	55%
73.27%	60%
69.68%	65%
63.98%	70%
58.68%	75%
54.16%	80%
49.70%	85%
44.23%	90%
38.41%	95%

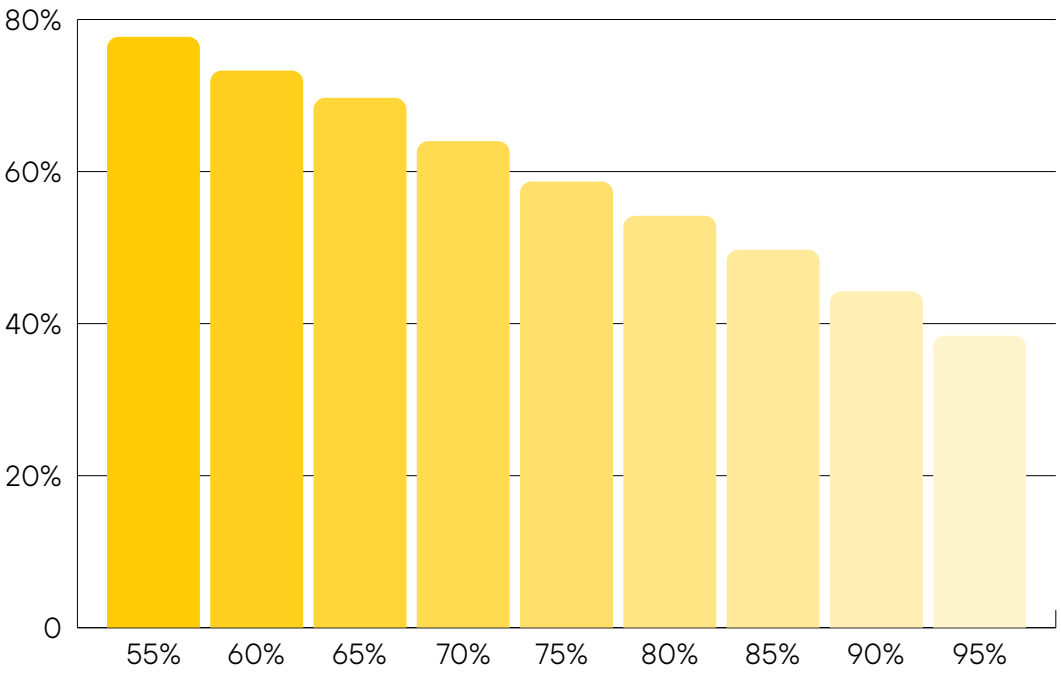


Figure 8. Percentage of segmentation distribution vs. network segment purity

Our analysis of the data reveals that poor network segmentation is the prevailing condition across most enterprise environments. We define a 100% pure segment as the segment with only IoT devices or only IT devices.

A majority of networks (77.74%) exhibit a low concentration of similar devices, with subnets containing a nearly even mix of IT and IoT assets (55% ratio). This indicates a widespread lack of clear boundaries.

Conversely, properly segmented networks are far less common. The data shows that only 38.41% of networks achieve a higher degree of segmentation where a single device type makes up 95% of the subnet.

This trend strongly indicates that most organizations are operating with flat, mixed-device environments, which broaden the attack surface and make it easier for threats to move laterally across the network. Implementing granular network segmentation is, therefore, critical to contain potential breaches and limit lateral movement. Notably, remote access protocols can also enable lateral movement when not properly segmented or monitored. In our dataset, 1.36% of devices expose Remote Desktop Protocol and 0.53% expose Virtual Network Computing (VNC). While these numbers might seem low, their presence in flat or poorly segmented networks introduces a high-risk pathway for attackers to pivot between systems. This is more evident when combined with weak credentials, insecure configurations, or existing footholds gained through phishing or malware.

Risk Device Categories

Our risk-scoring methodology combines vulnerability data, likelihood of exploitation, current exploit status, internet exposure, operating system support status, presence of security controls, and asset criticality. By using this method, we identified the 15 device categories with the highest overall risk.

On this scale, a score of 100 represents the maximum possible threat, signifying a strong combination of severe technical flaws, evidence of active exploitation, and high business criticality. This ranking reveals that this level of critical risk is not isolated to a single domain. Instead, it's distributed across the entire device ecosystem, from personal computers and smartphones to IP cameras and network equipment. If it's not properly secured and monitored, each of these categories provides a viable and high-value entry point for attackers, making them the top priorities for security and remediation efforts.

Table 3. Device Categories by Risk Score

Rank	Device Category	Risk Score
1	Smartphones and Tablets	100
2	Virtual Machines	100
3	Personal Computers (PCs)	99.8
4	IP Cameras and Security Surveillance Systems	98.48
5	Video Streaming Devices	96.4
6	Physical Security Systems	96.17
7	Wearable Mobile Computers	96
8	Printers	95.94
9	IT Servers	95.29
10	Energy Management Systems	95.09
11	Smart Environment Monitoring and Smart Temperature Monitoring	93
12	Network Attached Storage Devices	90.31
13	Smart Building Management Systems	90.14
14	Network Equipment	90
15	VoIP Communication Equipment	89.9

Device Identity and the Trust Boundary

A core principle of enterprise security is ensuring that all managed assets, particularly those joined to Active Directory (AD), have comprehensive endpoint protection. These devices have a greater level of trust and certain permissions to access internal resources, making them higher-value targets.

Our analysis reveals a critical gap in this security layer. Of the more than 200,000 devices in our dataset registered in AD, we observed that 38.75% do not have an active and properly functioning EDR or an XDR agent. This significant coverage gap means almost 2 out of every 5 trusted devices represent a security blind spot, creating a prime opportunity for attackers to conduct lateral movement undetected. Multiple factors contribute to this lack of comprehensive EDR deployment, such as unsupported devices, shadow IT servers, forgotten devices, and guest devices joining the corporate network.

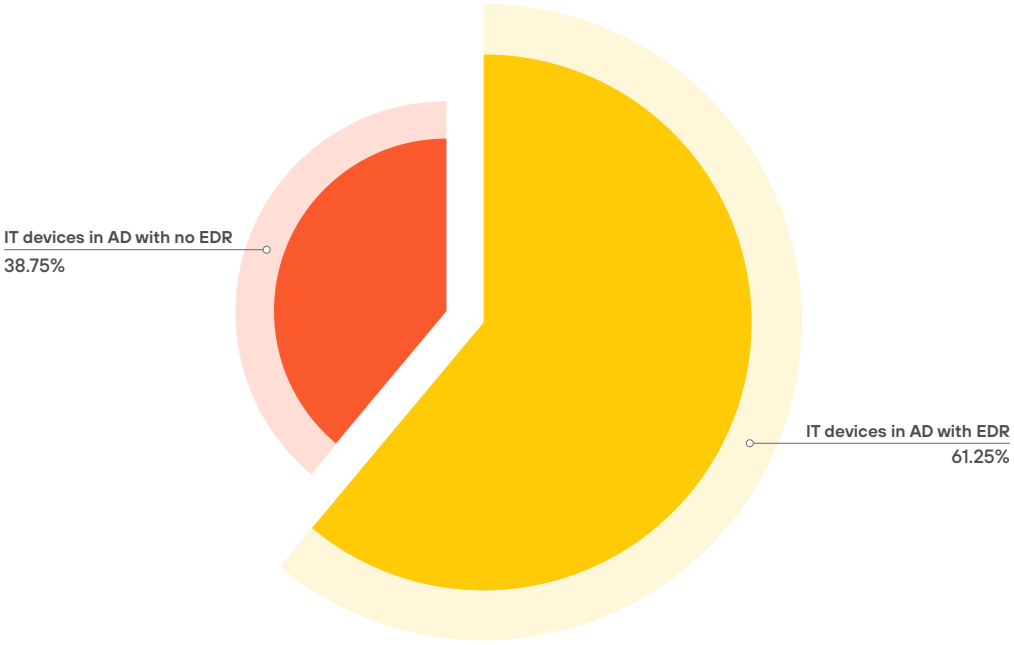


Figure 9. EDR status distribution in Active Directory

This nearly 39% gap in EDR coverage for trusted AD devices creates many security blind spots and opportunities for attackers to establish persistence and move laterally undetected. Organizations must ensure comprehensive EDR deployment on all managed IT assets to prevent these high-value targets from becoming easy entry points.

38.75%

of IT devices in Active Directory don't have EDR

In contrast, a complete risk analysis must also account for the large volume of BYODs, including PCs and mobile devices, guest devices, or IoT devices that are incompatible with traditional agent-based security, connecting to the network. These assets introduce a distinct challenge because they operate outside the scope of direct IT management and control.

Our data reveals the significant scale of this environment: These devices make up nearly one-third (32.5%) of the total device population. The substantial proportion of unmanaged devices in corporate networks means organizations must develop alternative security controls and policies for assets incompatible with traditional agents. This large presence of unmanaged endpoints expands the network's attack surface because these devices might not adhere to corporate security policies. Yet some of them might still be able to access internal resources.

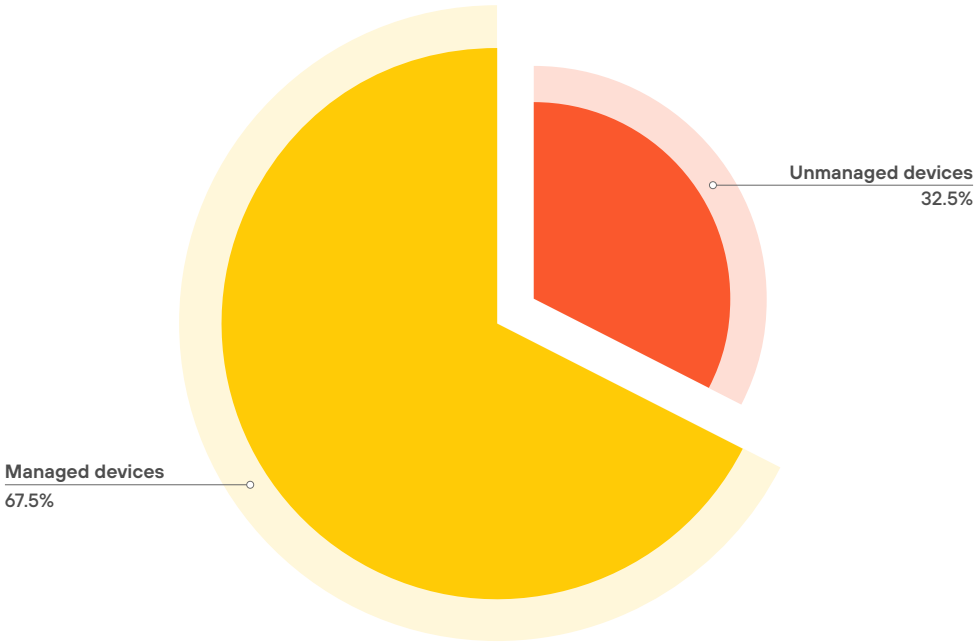


Figure 10. Device distribution

While both categories expand the network's attack surface, they do so from different operational contexts. One stems from a fundamental lack of IT monitoring and policy enforcement, and the other from a lack of traditional endpoint security measures.

32.5%

of devices in corporate networks are unmanaged

Malware Trends

Observations from the past year from Advanced WildFire® show that malware continues to disproportionately affect Windows systems, accounting for 97.58% of all observed malware-related activity. In comparison, Linux systems represent 2.16%, macOS 0.23%, and Android 0.02%.

The data reinforces the importance of maintaining visibility across all operating systems, especially in environments with a mixed infrastructure. Ransomware activity was also observed, with families, such as GandCrab, LockBit, and WannaCry, leading among known variants. The data reinforces the importance of maintaining visibility across all operating systems, especially in environments with a mixed infrastructure.

The data shows that while Windows is the primary target for malware (97.58%), the most common Linux threats are designed to hijack IoT devices and create massive botnets. For the business, this means a two-pronged threat: Windows malware directly targets corporate data and operations, while IoT malware threatens to weaponize the organization's own network infrastructure for large-scale attacks.

The strategic imperative is a differentiated defense strategy. Implement advanced, multilayered endpoint protection for all Windows systems. Also, simultaneously implement network-level security and segmentation to contain the risk from IoT and Linux devices where traditional security agents cannot be installed.

Table 4. Total Malware Count

Malware per OS	Percentage
Windows malware	97.58%
Linux malware	2.16%
MacOS malware	0.23%
Android malware	0.02%

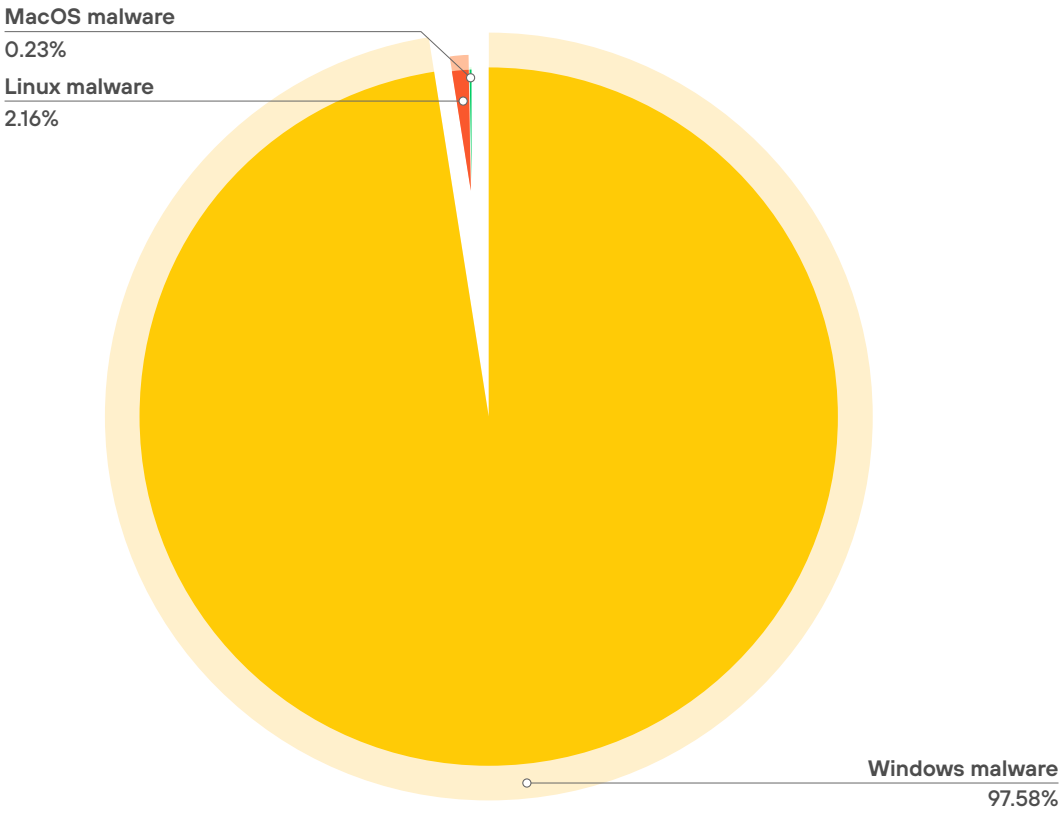


Figure 11. Total count by operating system

Windows Malware Families

Windows remains the primary target for malware, representing 97.58% of all activity observed. The most common malware families include Small, Vflooder, and various coinminer variants, which are often tied to credential theft, illicit cryptocurrency mining, or DDoS campaigns. Other families, such as Cymulate, Fareit, and Jadtre, further illustrate the diverse range of commodity threats that impact Windows environments. The high concentration of activity on this platform underscores its continued role as the primary attack surface for adversaries.

Table 5. Top Windows Malware Families

Windows Malware Family	Number of Malware Samples
Small	220,315
Vflooder	140,574
Coinminer	111,903
Msilzilla	77,243
Lazy	75,557
Knowbe4	68,886
Jadtre	61,845
Cymulate	61,526
Fareit	45,122
Padodor	37,634

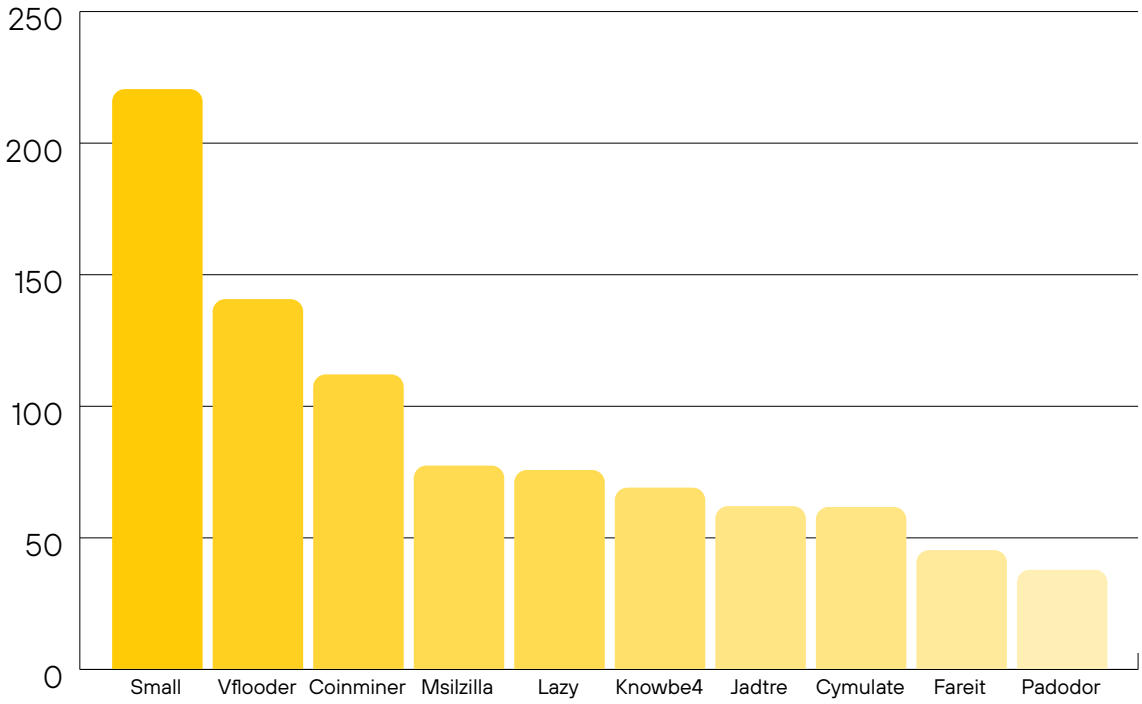


Figure 12. Top Windows malware families by record count

Linux Malware Families

Linux accounted for 2.16% of overall malware activity, with the majority linked to botnet and DDoS operations. Mirai and berbew remain the most widespread families, both commonly deployed to compromise IoT devices and enlist them into large-scale botnets. Additional families, such as Rekoobe, RudeDevil, and XorDdos, highlight the use of Linux malware for backdoors, resource hijacking, and DDoS attacks. Although smaller in volume compared to Windows, Linux malware maintains a critical role in adversary operations, particularly within server and IoT environments.

Table 6. Top Linux Malware Families

Linux Malware Family	Number of Malware Samples
botnet.Mirai	7,579
ddos.berbew	1,588
trojan.backdoor.gafgyt	1,550
trojan.miner.coinminer	1,010
trojan.ddos.chinaz	986
trojan.rudedevil	696
trojan.backdoor.rekoobe	599
hacktool.miner.bitcoinminer	593
linux.trojan.ddos.xorddos	575

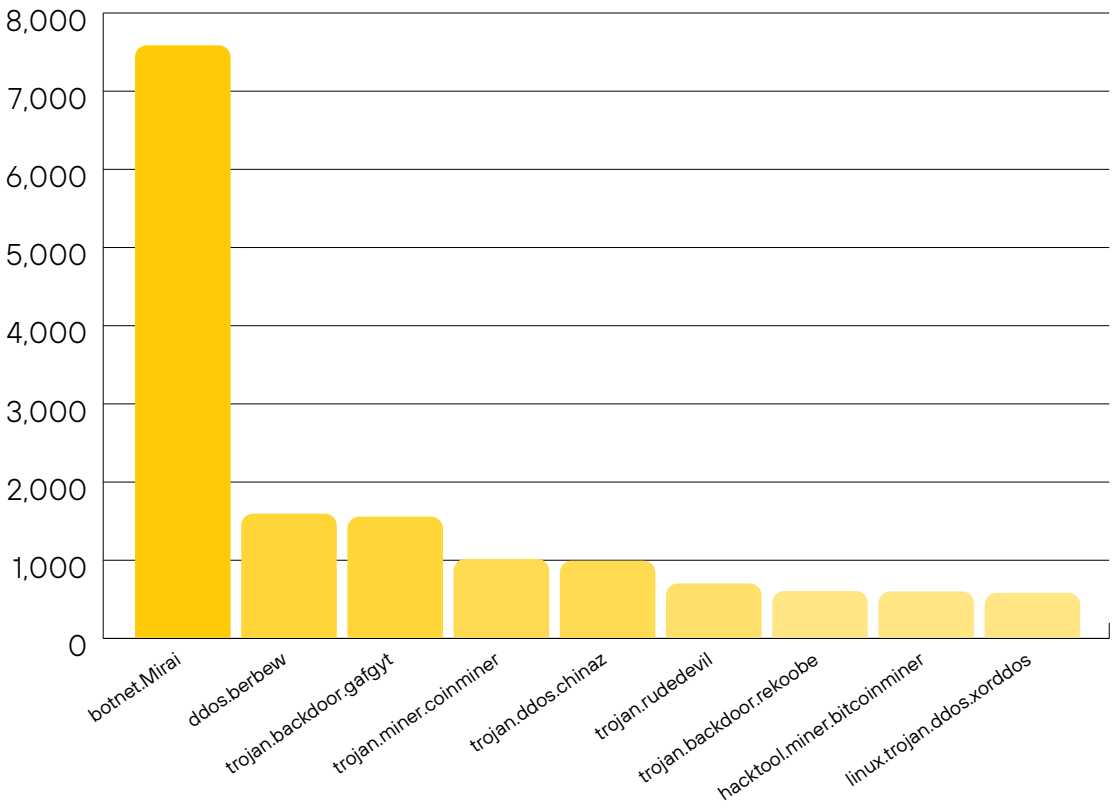


Figure 13. Top observed Linux malware families by record count

MacOS Malware Families

Malware affecting macOS represented only 0.23% of observed activity. Most detections fall into the category of commodity malware or potentially unwanted programs, with no single family dominating. The low prevalence of macOS malware compared to Windows and Linux reflects its smaller share in enterprise deployments but doesn't eliminate the need for monitoring, especially in organizations with mixed environments.

Table 7. Top MacOS Malware Families

MacOS Malware Family	Number of Malware Samples
Lamadai	2308
GetShell	903
EvilQuest	250
Pronto	121
Generic or Others	111
Olyx	40
AMOS	26
CloudMensis	20
NukeSped	18
LimeRain	15

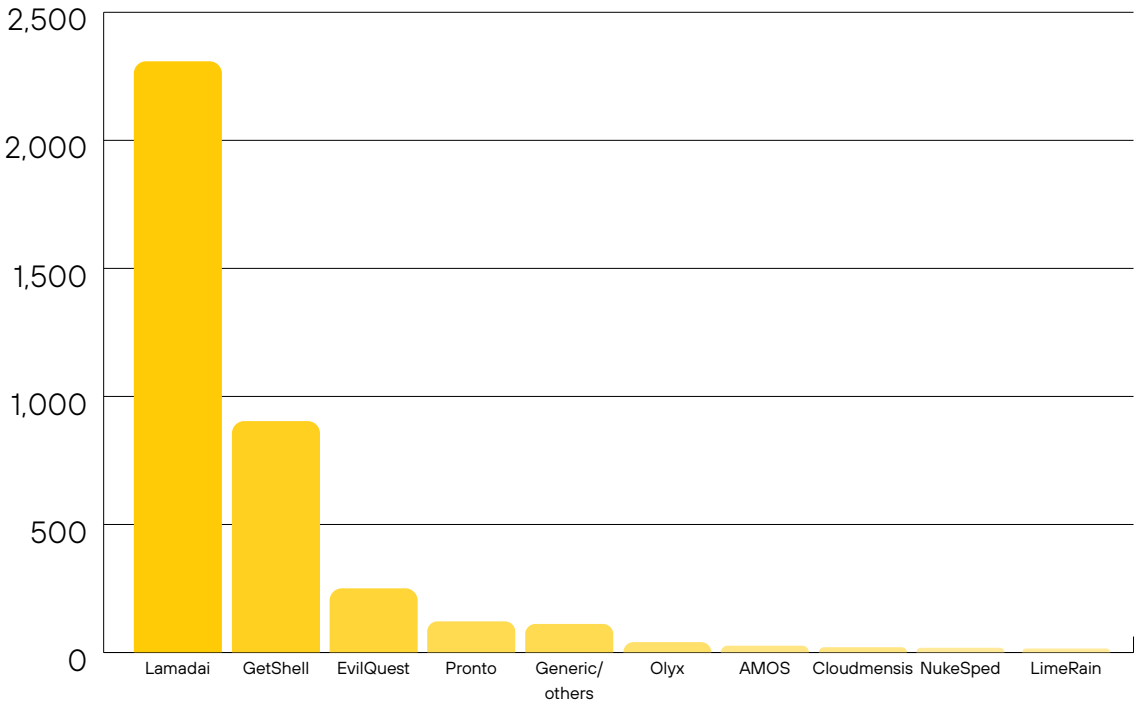


Figure 14. Top macOS malware families by record count

Ransomware

Ransomware remains one of the most disruptive categories of malware, with such families as GandCrab, LockBit, and WannaCry leading in observed activity. These families represent different stages in the evolution of ransomware, from the early WannaCry global outbreaks to LockBit's more sophisticated and financially motivated operations.

Ransomware activity continues to affect both enterprises and individual users, with adversaries targeting organizations of all sizes across sectors. In many cases, ransomware is delivered as a secondary payload following an initial intrusion, often leveraging phishing, commodity malware, or exploit-based access. The persistence of ransomware in the threat landscape highlights the importance of layered defenses, timely patching, and proactive detection measures to mitigate the risk of data loss, operational disruption, and financial impact.

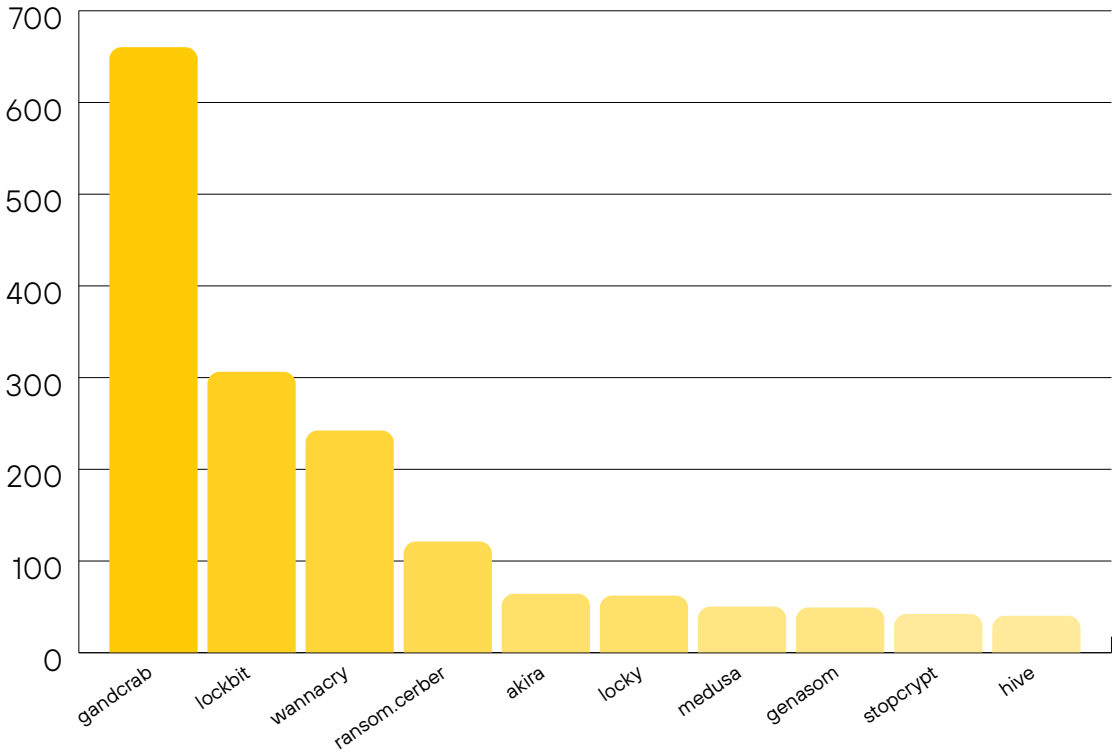


Figure 15. Top observed ransomware families

MITRE ATT&CK Tactics and Techniques

Understanding the tactics and techniques most frequently observed in attacker behavior is key to strengthening defenses. Over the past year, our telemetry from Cortex XDR® shows that attackers consistently exploit core postexploitation and reconnaissance tactics. The 10 most common MITRE ATT&CK® techniques include privilege escalation, defense evasion, and persistence. They are most effective in environments that suffer from poor hygiene, a lack of system hardening, common misconfigurations, and inadequate security countermeasures.

The data in table 8 highlights where attackers are focusing their efforts after they gain initial access. This data also helps guide detection engineering and hardening initiatives.

Table 8. Observed Techniques and Tactics

Rank	Technique ID	Technique Name	Tactic
1	T1068	Exploitation for Privilege Escalation	Privilege Escalation
2	T1014	Rootkit	Defense Evasion
3	T1211	Exploitation for Defense Evasion	Defense Evasion
4	T1203	Exploitation for Client Execution	Execution
5	T1070.001	Indicator Removal on Host: Clear Windows Event Logs	Defense Evasion
6	T1112	Modify Registry	Defense Evasion
7	T1505.003	Server Software Component: IIS Web Shell	Persistence
8	T1590.001	Gather Victim Host Information: Local System Information	Reconnaissance
9	T1055	Process Injection	Defense Evasion
10	T1059	Command and Scripting Interpreter	Execution

Global Exposure of Internet-Connected IoT Devices

Using data collected from Cortex Xpanse®, which continuously scans the internet, we assessed the global distribution of exposed internet-connected IoT devices over the past year. This data does not rely on internal telemetry but reflects a broad, external view of how devices are reachable across the internet. A heat map was generated to visualize the relative exposure levels by country, highlighting regions with significant concentrations of directly accessible systems. The map in figure 16 is based on the number of exposed devices detected per country, offering insight into geographic trends in internet-facing infrastructure. This visibility helps identify areas where unmanaged, misconfigured, or outdated assets can increase organizational and national risk.

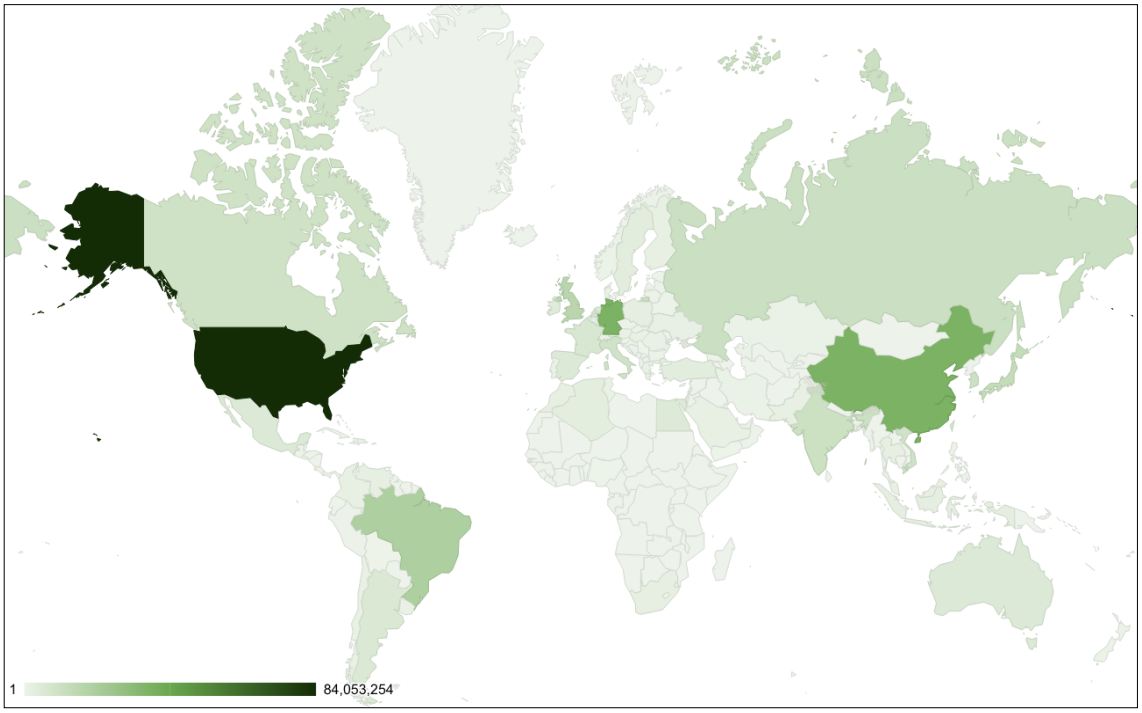


Figure 16. Relative exposure levels by country, showing concentrations of accessible systems

To complement the global view provided in the heat map, table 9 highlights the top 20 countries with the highest number of internet-exposed IoT devices observed during the scan period. While the map includes data for all countries, this list showcases a breakdown of those with the largest absolute counts to help contextualize regional exposure and assist in prioritizing risk assessments or outreach efforts.

Table 9. Top 20 Countries with the Most Internet-Exposed IoT Devices

Rank	Country	Exposed Devices
1	United States	84,053,254
2	Germany	36,449,448
3	China	36,331,092
4	Brazil	20,100,895
5	United Kingdom	15,991,229
6	Japan	13,122,851
7	Russia	10,859,934

Table 9. Top 20 Countries with the Most Internet-Exposed IoT Devices (continued)		
Rank	**Country**	**Exposed Devices**
8	India	10,729,782
9	Korea	10,664,978
10	Canada	9,668,190
11	Italy	9,262,511
12	Vietnam	9,204,064
13	Hong Kong	7,512,781
14	Taiwan	6,980,198
15	France	6,679,887
16	Argentina	6,099,802
17	Netherlands	5,643,514
18	Australia	5,508,936
19	Mexico	5,445,157
20	Spain	5,360,696

Over the past year, the number of exposed devices has remained relatively stable, fluctuating 33.7–35.4 million each month. The lowest point was observed in November 2024 with approximately 32.9 million devices, while the peak occurred in January 2025 with over 35.4 million. These variations are minor and suggest no significant reduction in overall exposure. This persistence highlights the need for continuous risk assessment and active mitigation efforts.Beyond geographic trends, it's

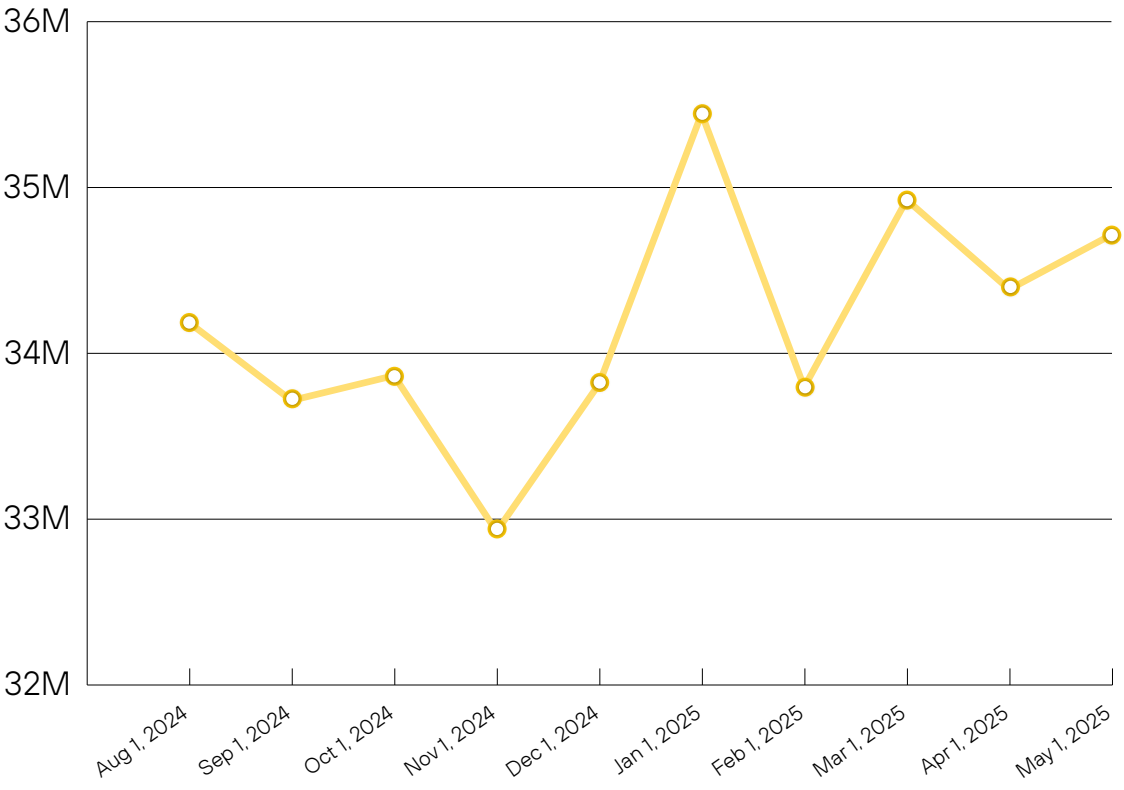


Figure 17. Fluctuations of exposed devices

also important to understand which types of IoT devices are most frequently exposed to the public internet. These categories provide insight into the kinds of assets that are commonly left accessible, whether intentionally or due to misconfigurations. Figure 18 highlights the top exposed IoT device categories observed globally, offering a clearer view of which technologies are most at risk when it comes to internet-facing exposure.

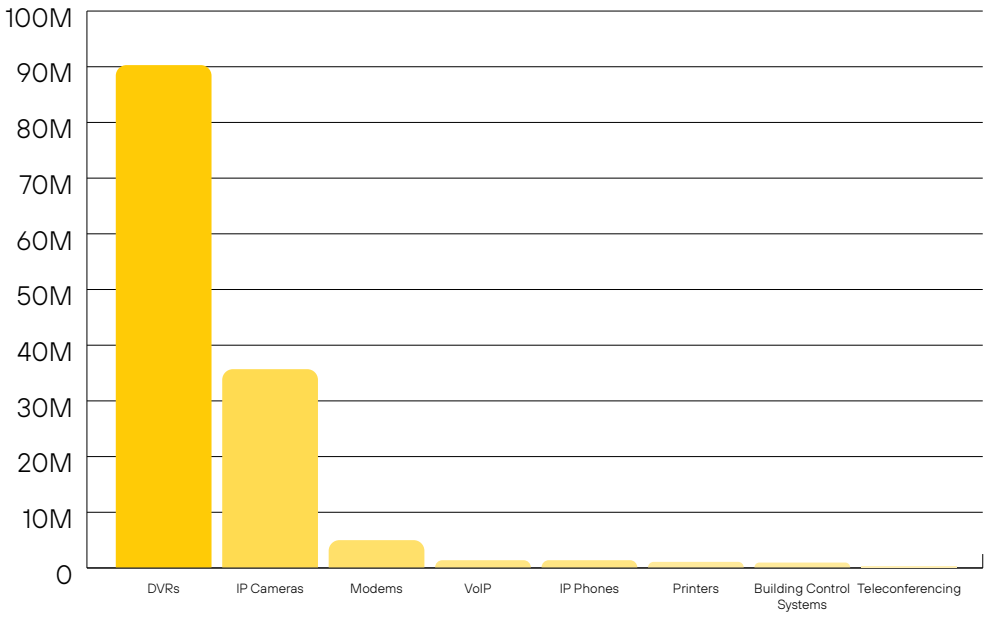


Figure 18. Top exposed IoT device categories observed globally

Unsurprisingly, digital video recorders (DVRs) and IP cameras account for the vast majority of exposed IoT devices, with tens of millions accessible directly from the internet. These devices are often deployed with minimal security hardening and are frequently targeted by botnets and opportunistic attackers.

Other categories, such as modems, VoIP gateways, and IP phones, also appear in large numbers, underscoring the ongoing risks associated with exposed telecommunications infrastructure. Notably, over 770,000 building control systems were found to be internet-accessible, highlighting a concerning intersection between IoT and operational technology environments where exposure could lead to physical or environmental manipulation. While teleconferencing systems and network printers appear in smaller numbers, their presence still represents an attack surface that is often overlooked in perimeter security strategies.

Conclusion

In conclusion, a modern security program must be proactive, integrating continuous monitoring of external threats with robust internal capabilities for timely detection and response. This proactive stance enables organizations to transition from an undefined risk posture to a quantifiable, controllable inventory. It fundamentally relies on deep, contextualized, and comprehensive asset intelligence—knowing what's there, what it does, how it is connected, how vulnerable it is, and its importance to the business.

This actionable intelligence empowers security leaders to understand their complete attack surface, effectively identify and prioritize risks, apply precise security policies, allocate resources strategically, and maintain continuous visibility across all operating systems.

Protecting an enterprise network in today's ubiquitous exposure is akin to managing a complex ecosystem where every inhabitant, no matter how small or seemingly insignificant, can influence the safety of the entire environment. True defense comes from deeply understanding the living, breathing dynamics of these inhabitants, identifying which are predatory, which are vulnerable, and how they interact, allowing for targeted intervention and proactive guardianship of the most vital resources.

Recommendations

Visibility is only the beginning. Defenders must take action with context, connecting exposures to real adversary behavior and understanding how attackers chain misconfigurations, credentials, and vulnerabilities to reach their objectives. This requires seeing how techniques like privilege escalation, process injection, and command execution play out in the environment, not in isolation, but as part of complete attack paths.

By mapping out how these techniques have been observed in the wild and where they intersect across assets, teams can identify the fastest and most impactful ways to reduce risk. Rather than chasing individual vulnerabilities or alerts, security programs should focus on disrupting entire attack flows, addressing multiple exposures at once through strategic and proactive remediations that target the techniques most often exploited.

Call to Action

1

Adopt a Zero Trust Architecture

The prevalence of unmanaged devices and flat networks makes this architecture essential to prevent catastrophic lateral movement.

Zero trust minimizes the damage of a breach by enforcing least privilege, segmenting access, and continuously verifying users and devices. It reduces attacker dwell time and lateral movement opportunities, while also improving visibility across hybrid environments. Beyond security, organizations that adopt zero trust have reported faster adoption of cloud services and stronger customer trust due to consistent policy enforcement.

2

Implement Comprehensive Endpoint Visibility and Control

With endpoints being the primary target, gaps in EDR and XDR coverage on managed and unmanaged devices are the single greatest source of risk.

Unified visibility and control across all endpoints makes it possible to detect threats earlier, contain compromised systems faster, and enforce policies consistently. It reduces the cost and duration of incidents, while lowering compliance and audit burdens. Organizations that have strong endpoint detection and response programs have shown significant reductions in mean time to detect (MTTD) and mean time to respond (MTTR).

3

Establish a Proactive Risk Management Program

The high volume of vulnerabilities and automated attacks means a reactive defense is doomed to fail. Organizations must prioritize vulnerabilities based on the attack path they pose to high-value assets in the organization, active exploitation, and business criticality (both impact and consequence).

Risk-based vulnerability management ensures teams focus on the threats that matter most, rather than chasing every vulnerability. This approach has been shown to improve remediation efficiency by over an order of magnitude, reduce exposure to actively exploited vulnerabilities, and optimize limited security resources. Organizations that embed such programs report an improved security posture, better communication of risk to leadership, and measurable reductions in the likelihood of a breach.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com