

Securin

Healthcare Sector Cyber Threat Intelligence Report

Q1 2026



Introduction

In Q1 of 2026, the healthcare sector solidified its position as the most consistently profitable target in the ransomware and threat actor economy.

This period saw 592 documented attacks involving 94 ransomware groups, 29 weaponized Common Vulnerabilities and Exposures (CVEs) and a broader threat actor ecosystem defined by escalating sophistication, relentless targeting and systemic exploitation of security fundamentals.

Every vulnerability observed in exploitation appears in the CISA Known Exploited Vulnerabilities (KEV) catalog. Attackers aren't relying on obscure or theoretical flaws, they're systematically targeting known weaknesses that remain unpatched in operational environments.

The pace of attacks reflects this structural exposure. During this period, healthcare organizations experienced an intrusion approximately every 10 hours, with ransomware accounting for 59% of incidents - the highest proportion across all sectors.

Securin's analysis shows a threat ecosystem that's both industrialized and predictable: attackers repeatedly exploit the same categories of weakness, follow similar operational playbooks, and focus on environments where remediation timelines are constrained.

KEY INTELLIGENCE FINDINGS

Total attacks analyzed 592 Jan 2025 – Feb 2026	Active ransomware groups 94 Attacking healthcare globally
Ransomware share of incidents 58.9% Highest across all verticals	US share of attacks 55.9% (331/592) Dominant target geography
Average inter-attack interval 0.4 days Attack occurs every ~10 hours	Weaponized CVEs tracked 29 All actively exploited
CISA KEV rate across CVEs 100% (29/29) Every CVE is catalog-confirmed	Zero-days in exploit set 48% (14/29) Near-majority were novel at exploit time
Peak month October '25 – 70 attacks 75% above monthly average	Dominant weakness class Authentication bypass 10 CVEs, most exploited category

BOTTOM LINE:

Healthcare's combination of life-or-death operational dependency, high-value protected health information (PHI), chronic underinvestment in security, and complex legacy infrastructure makes it the single highest-value target in the ransomware economy. The sector pays ransoms at a **68–72%** rate - almost double the cross-sector average - creating a self-reinforcing cycle of targeting.

What's in this report

Attack Volume & Temporal Patterns	01
Threat Actor Landscape	06
Adversary Tools, Techniques & Procedures (TTPs)	10
Vulnerabilities Exploited	16
Weakness Analysis	23
Attack vector analysis	27
Why Healthcare Pays	29
Mitigation Priorities & Regulatory Environment	32
Threat Outlook	36
Conclusion	38

Attack Volume & Temporal Patterns



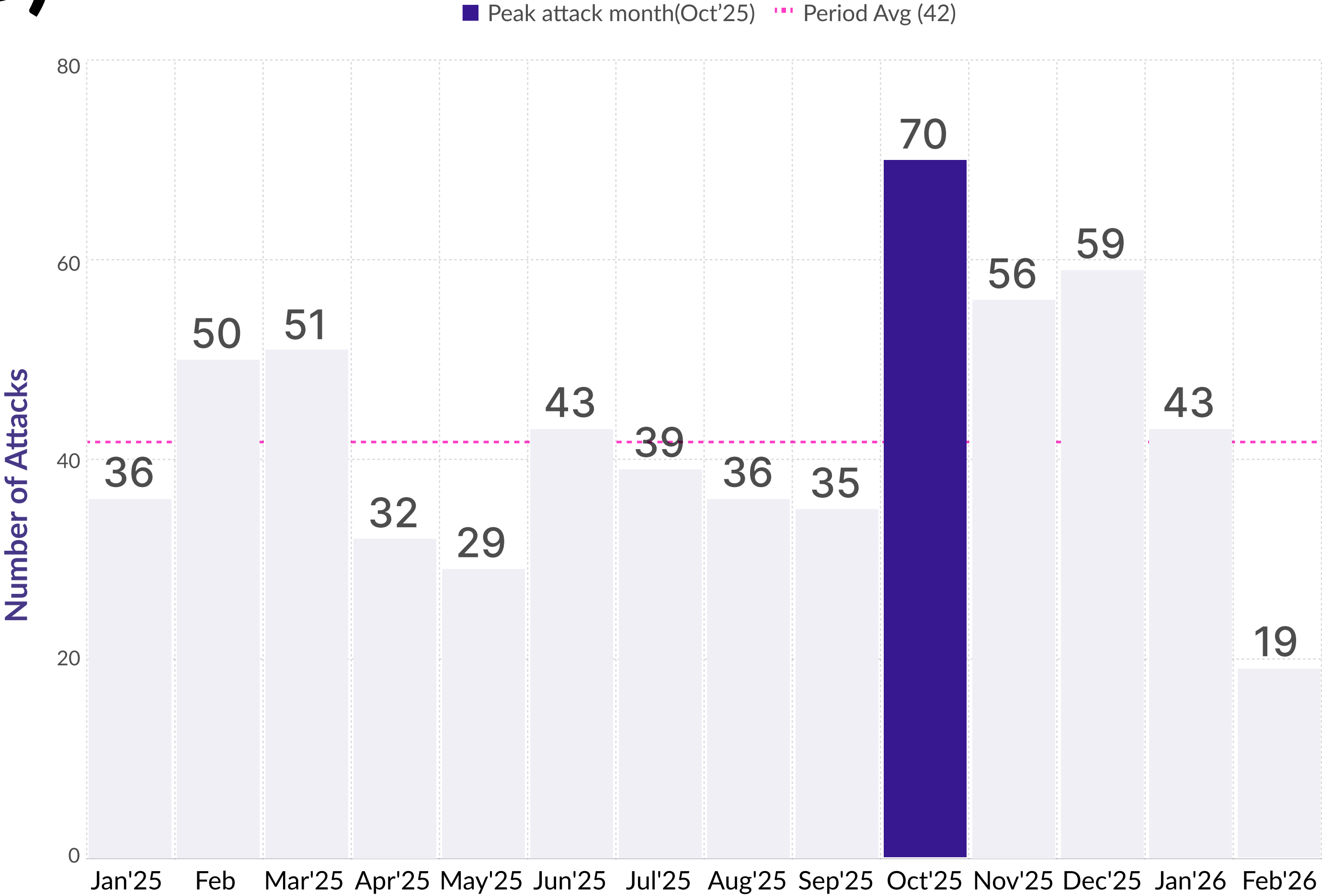
Monthly Attack Volume (Jan 2025 – Feb 2026)

Across the reporting period, healthcare organizations experienced 492 attacks, with activity accelerated through late 2025.

October 2025 recorded 70 attacks – 75% increase over the monthly average of 40 incidents. This surge was driven primarily by campaign activity from: Qilin, Sinobi and Incransom.

The broader Q4 period saw 179 attacks, accounting for 30% of all observed activity. Two operational factors likely drove this concentration: fiscal year-end pressures and known seasonal ransomware campaign cycles.

The resulting pattern reflects a mature ransomware economy that schedules campaigns to coincide with periods of maximum organizational vulnerability.

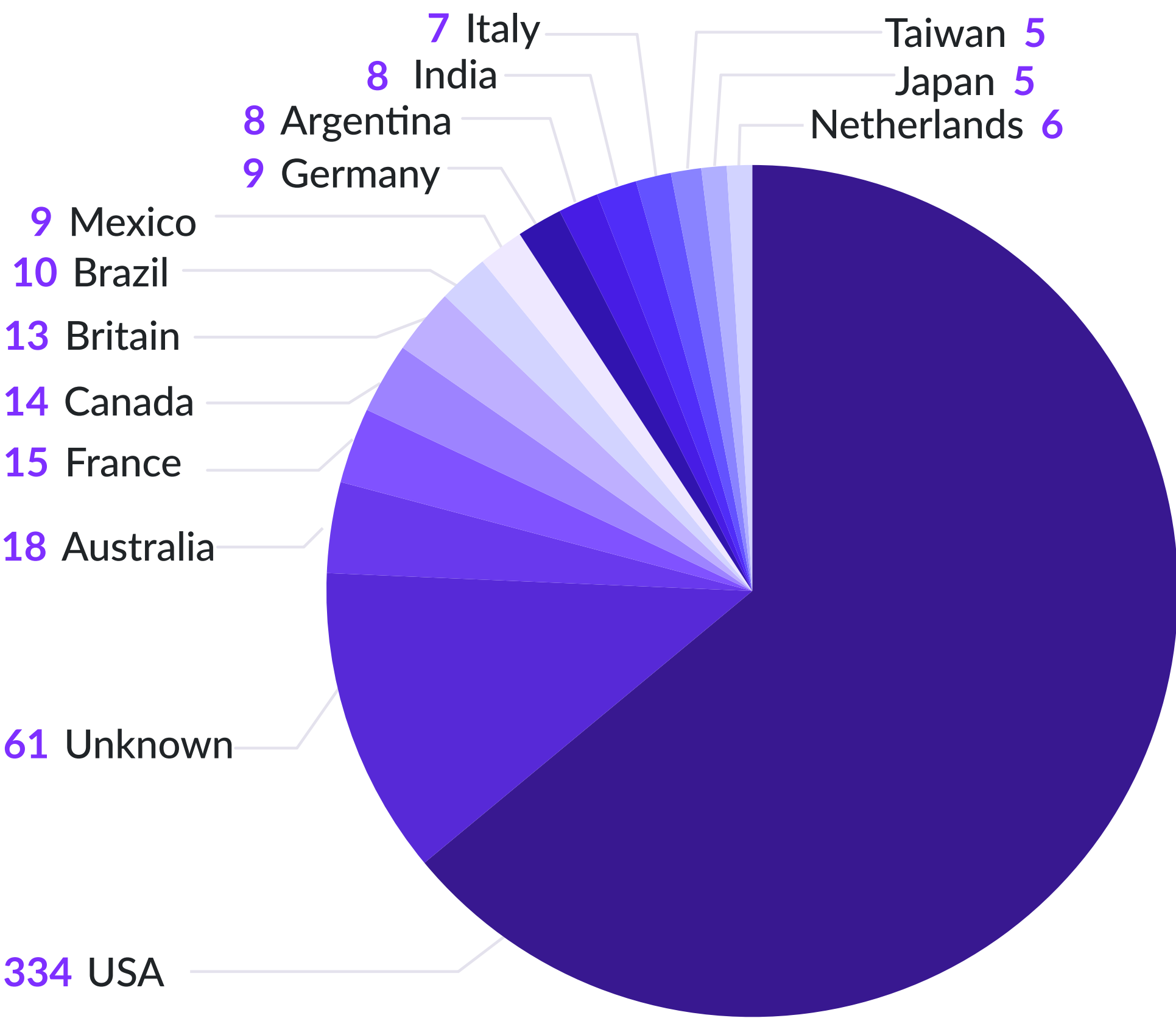


Geographic Targeting

The United States accounts for 56% of all attacks in our dataset - 331 of the 592 incidents analyzed. Several structural conditions explain this concentration:

-  Large and technologically complex healthcare networks
-  Extensive use of interconnected clinical and administrative systems
-  High cyber-insurance coverage levels
-  Regulatory pressure to restore operations rapidly (HIPAA)

Combined with the other Five Eyes nations, Anglosphere healthcare systems account for approximately 67% of observed attacks.



BOTTOM LINE:

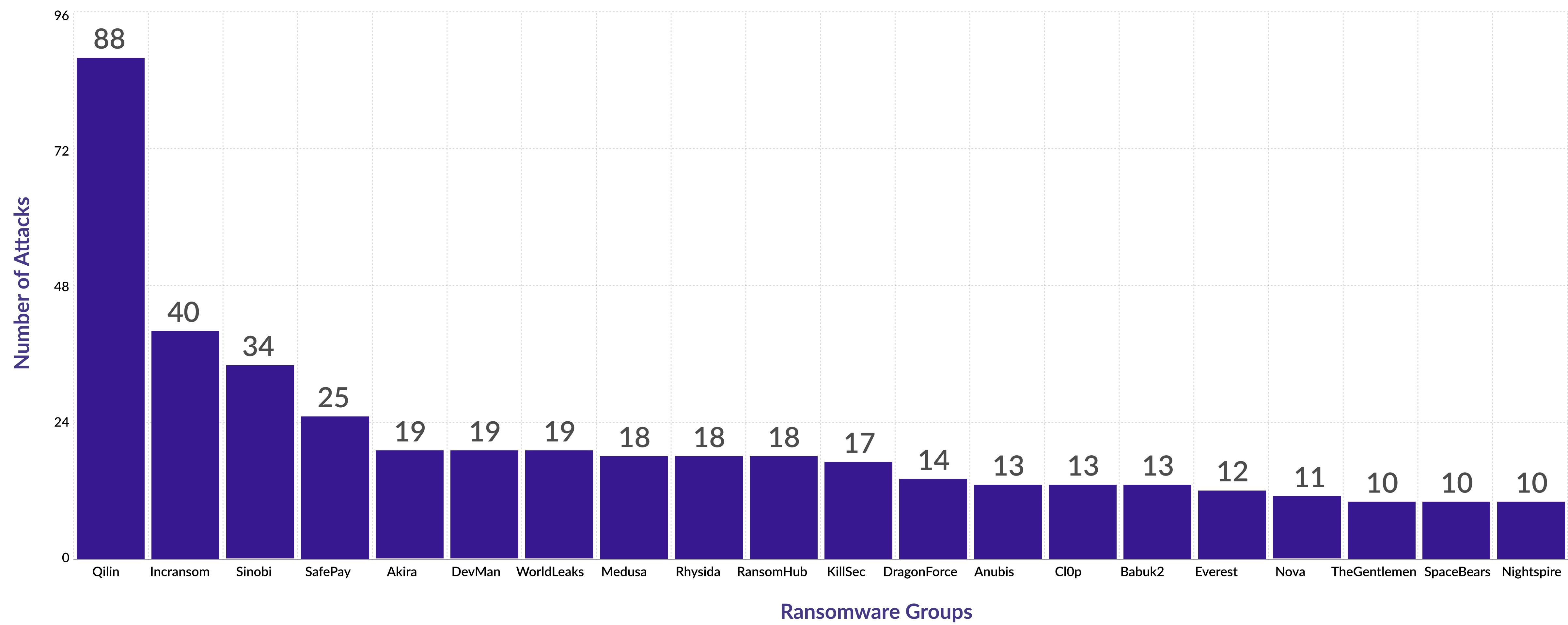
The most-attacked regions present a combination of large attack surface and predictable payment incentives, making them disproportionately attractive to ransomware operators.

Threat Actor Landscape



Top 20 Ransomware Groups by Attack Volume

(Jan 2025 – Feb 2026)



The top ransomware groups targeting healthcare

94 ransomware groups were observed targeting healthcare, but activity was concentrated among a smaller set of operators:

Qilin (88 attacks)

Qilin is the most prolific healthcare ransomware operator in this period by a significant margin. Built on Rust for cross-platform capability, Qilin encrypts Windows endpoints, Linux servers, and VMware ESXi hypervisors within a single attack sequence. The group's exploitation of CVE-2024-21762 (Fortinet FortiOS, Zero-Day, CISA KEV 2024-02-09) provided unfettered access to mid-market healthcare organizations using FortiGate SSL-VPN appliances.

ATTACK METHODOLOGY

Purchase initial access from IABs → establish Cobalt Strike C2 → conduct 3–4 week network reconnaissance → exfiltrate 50–500GB PHI → stage payload across ESXi hosts → Friday-evening execution for maximum dwell before discovery. ESXi encryption collapses hospital imaging (PACS), EHR databases, and VDI simultaneously. **Ransom range: \$200K–\$5M**



DOMINANT OPERATOR

Incransom (40 attacks)

High-volume operator with consistent targeting across US and European healthcare facilities. Relies on compromised RDP credentials and VPN exploitation rather than novel CVEs. Focus on mid-size hospitals and specialty practices where security tooling is lighter.



HIGH VOLUME OPERATOR

Sinobi (34 attacks)

Emerging group showing rapid acceleration through Q3–Q4 2025. Targets healthcare supply chain and managed service providers as a pivot mechanism into healthcare networks. Double-extortion model with a publicly operated leak site.



EMERGING GROUP

SafePay (25 attacks)

Financially disciplined operator with a notable pattern of targeting organizations with known cyber insurance coverage. Encrypts files with .safepay extension; leaves readme_safepay.txt ransom notes. Closely tracks victim revenue and insurance limits when setting demands.



CYBER INSURANCE TARGETER

Rhysida (18 attacks)

A consistent healthcare-targeting group known for attacks on hospital systems and healthcare networks. Uses phishing-based initial access followed by Living-off-the-Land (LotL) techniques to blend into normal operations during the dwell period.



HEALTHCARE SPECIALIST

Akira (19 attacks)

Akira maintains the most comprehensive CVE exploitation portfolio in this dataset — 9 distinct CVEs including Fortinet (CVE-2019-6693, CVE-2022-40684), Cisco ASA (CVE-2020-3259, CVE-2023-20269), VMware (CVE-2021-21972, CVE-2024-37085), and Veeam (CVE-2023-27532, CVE-2024-40711). Upon initial access, Akira operators create both domain and local accounts for persistence before lateral movement.

 TECHNICAL SOPHISTICATION LEADER

Medusa (18 attacks)

Exploits SimpleHelp RMM software (CVE-2024-57727, CISA KEV 2025-02-13) to gain footholds in organizations that use this remote monitoring tool for IT management — particularly relevant to healthcare IT managed service providers.

 IMPACTS HEALTHCARE MANAGED SERVICE PROVIDERS

RansomHub (18 attacks)

Operates with the widest network infrastructure exploit set: EternalBlue (CVE-2017-0144), CVE-2023-27997 (Fortinet), CVE-2023-3519 (Citrix), CVE-2023-46604 (Apache ActiveMQ), CVE-2023-46747 (F5 BIG-IP), and CVE-2023-22515 (Atlassian Confluence). RansomHub affiliates are distinguished by opportunistic exploitation of any unpatched perimeter device.

 BROAD EXPLOIT COVERAGE

ClOp (13 attacks)

ClOp's healthcare impact disproportionately exceeds its attack count due to mass-exploitation campaigns. The MOVEit campaign (CVE-2023-34362, Zero-Day) and GoAnywhere campaign (CVE-2023-0669, Zero-Day) each compromised dozens of healthcare organizations simultaneously. ClOp's 2025 activity leverages CVE-2025-61882 (Oracle E-Business Suite, Zero-Day) and CVE-2024-55956 (Cleo file transfer, Zero-Day) to maintain this pattern.

 MASS EXPLOITATION SPECIALIST

Adversary Tools, Techniques & Procedures (TTPs)



Adversary tools, techniques and procedures (TTPs)

Healthcare ransomware operations aren't defined by isolated tools or one-off exploits. They follow a repeatable operational pattern built from a shared arsenal of commodity tools, credential abuse, lateral movement frameworks and well-understood ATT&CK-mapped behaviors.

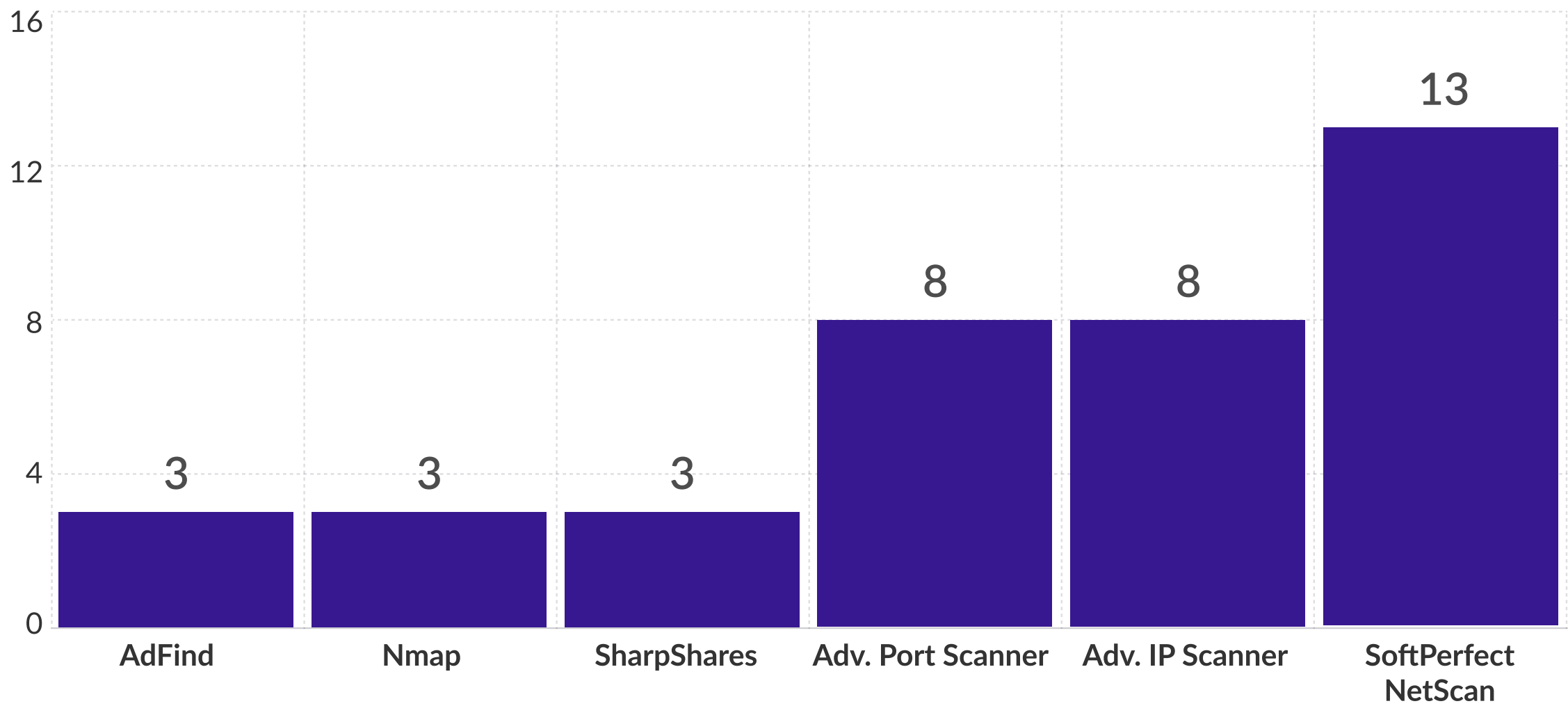
Across the 94 groups we tracked, the specific malware and exploit paths vary, but the underlying tradecraft is strikingly consistent.

BOTTOM LINE:

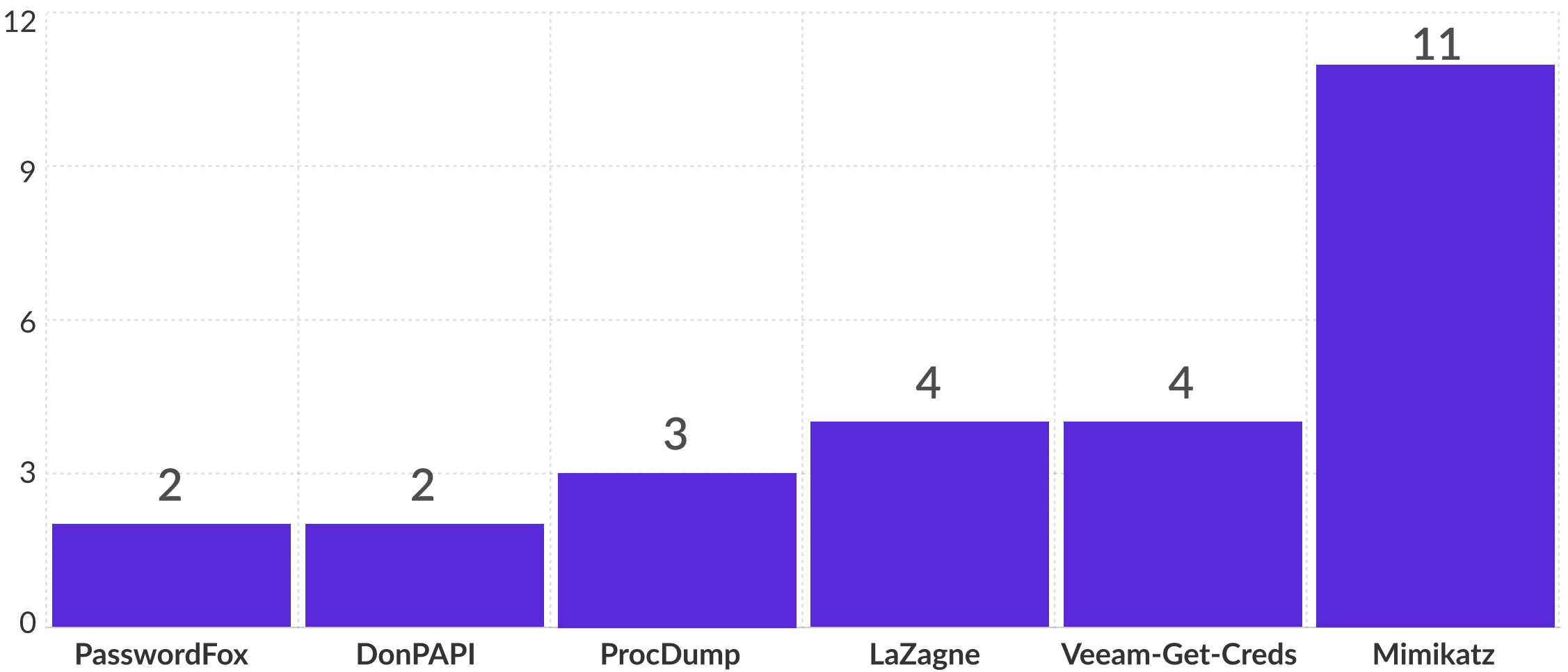
The exploit of the month changes, but the operational logic doesn't.

Ransomware Group Tool Arsenal - Top Tools by Category (94 Groups Analyzed)

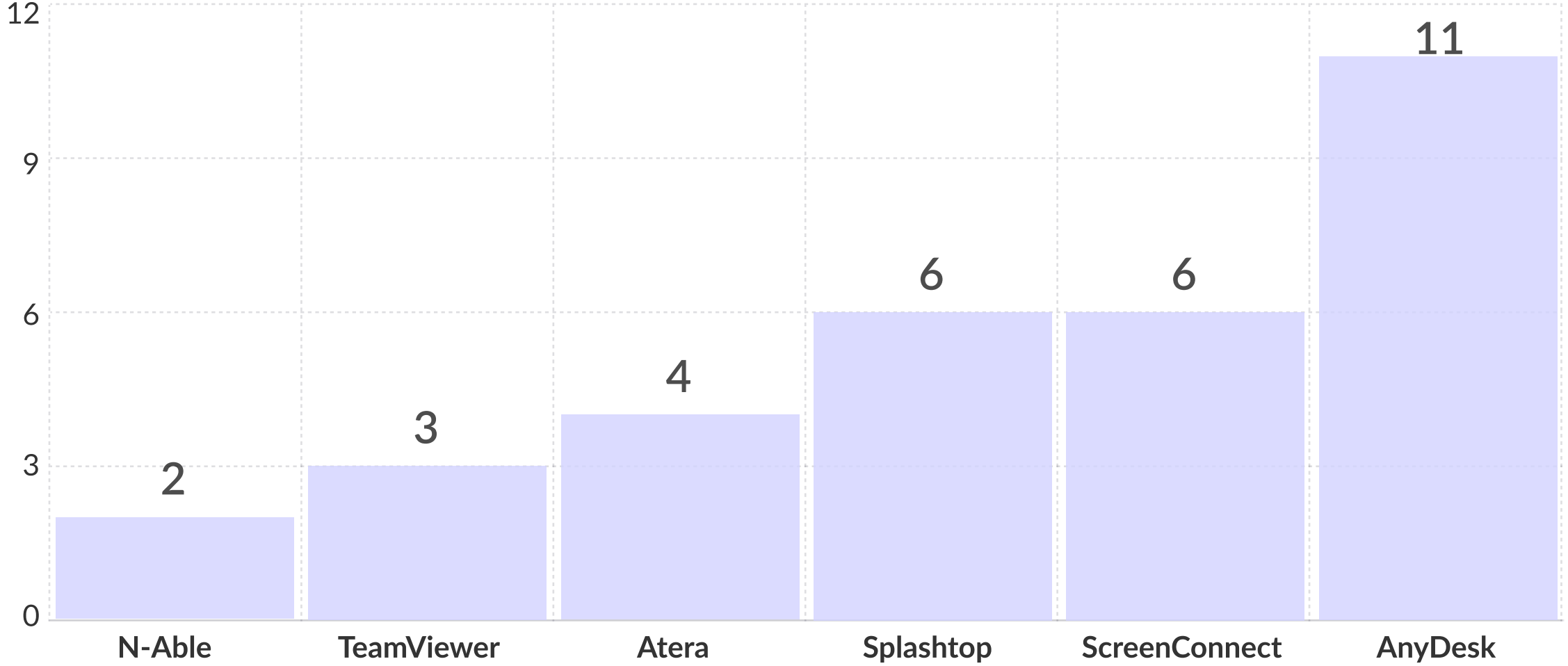
DISCOVERY & ENUMERATION



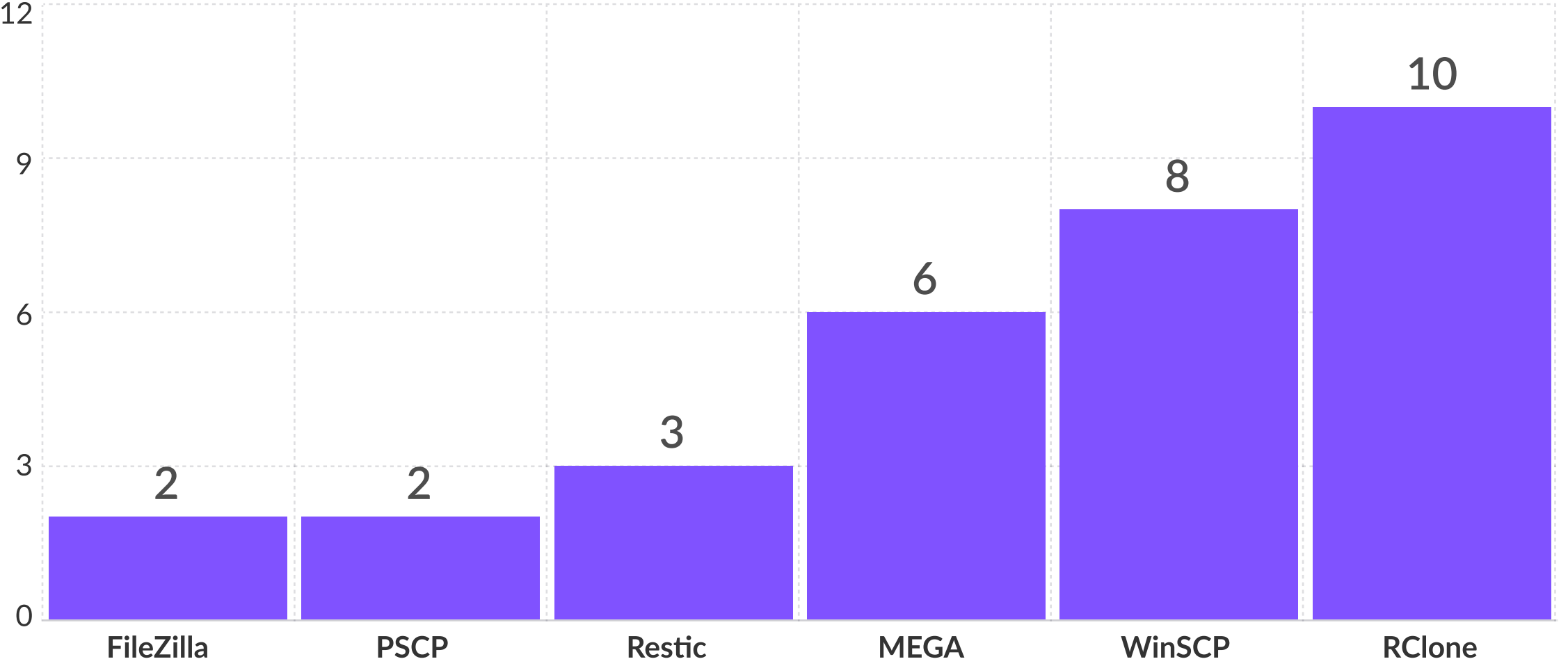
CREDENTIAL THEFT



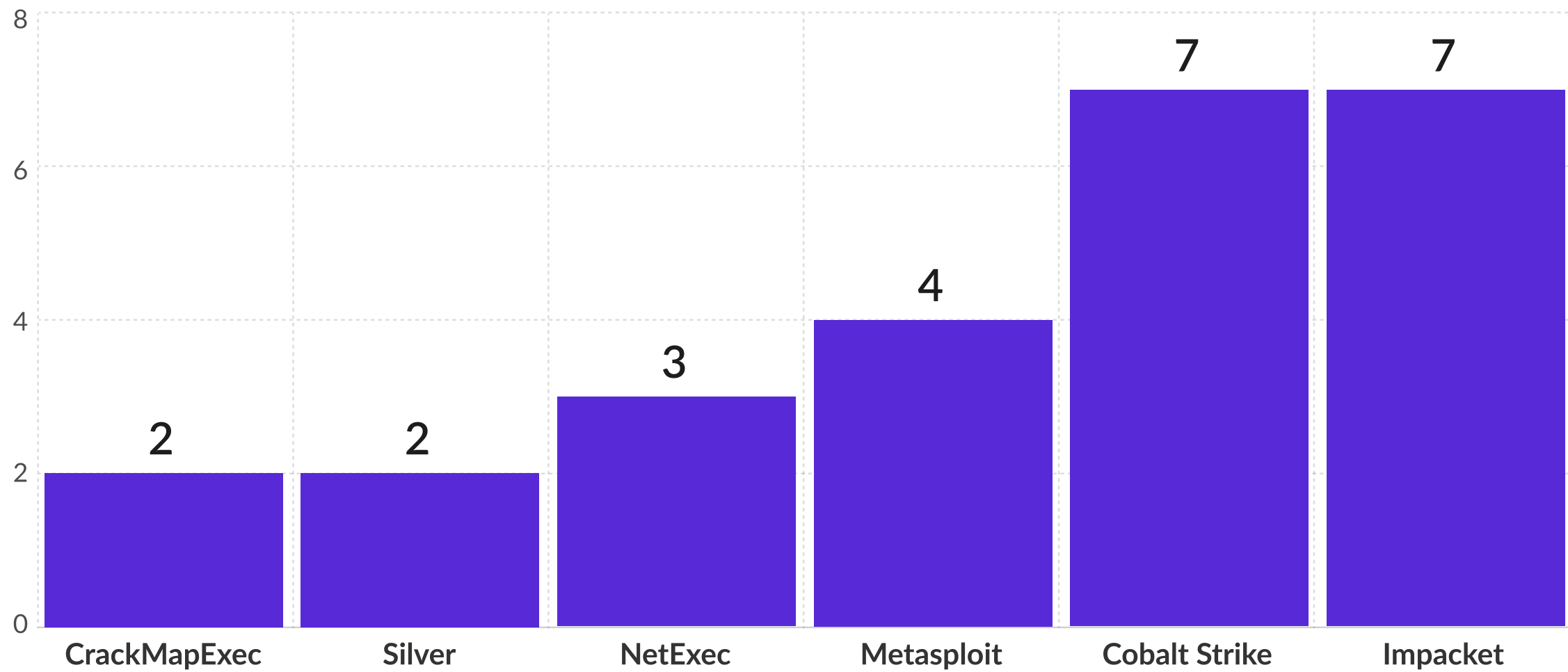
REMOTE MANAGEMENT



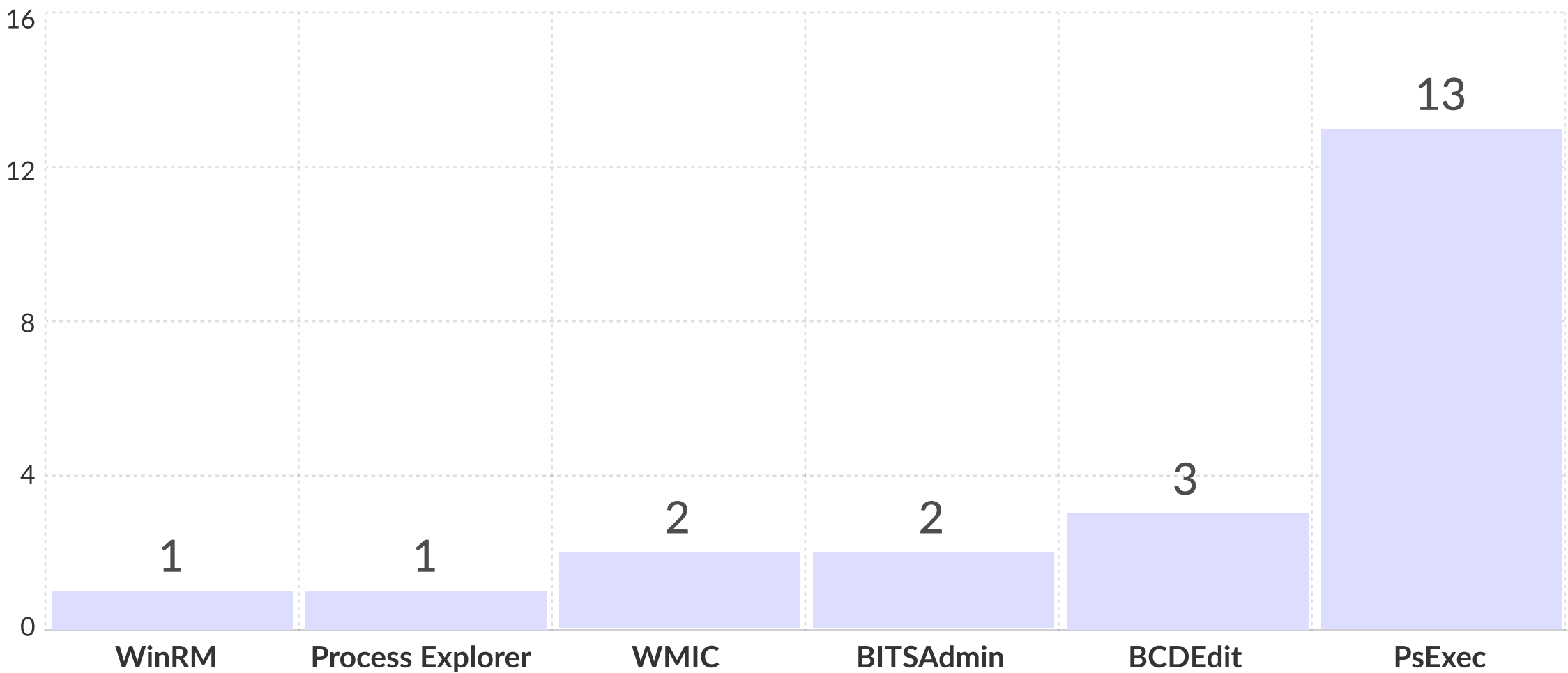
EXFILTRATION



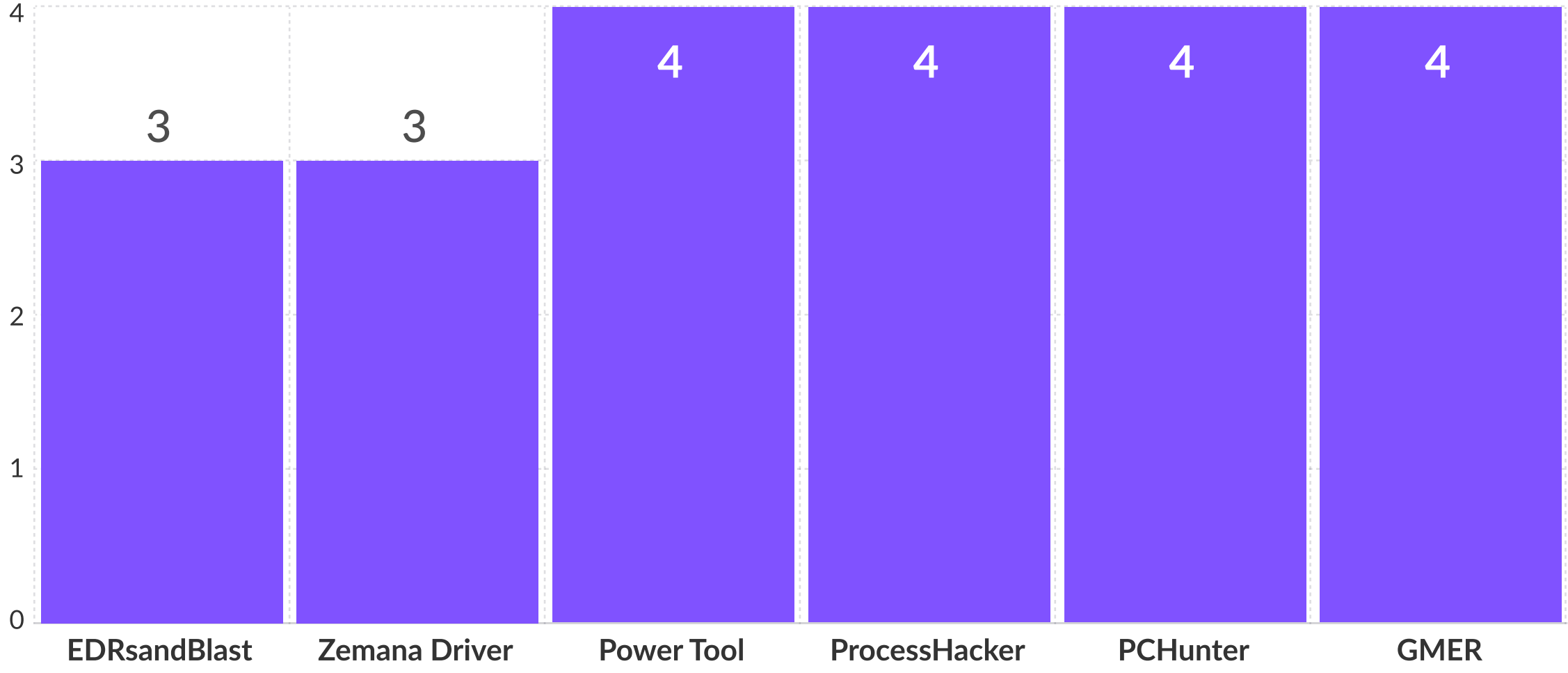
OFFENSIVE SECURITY



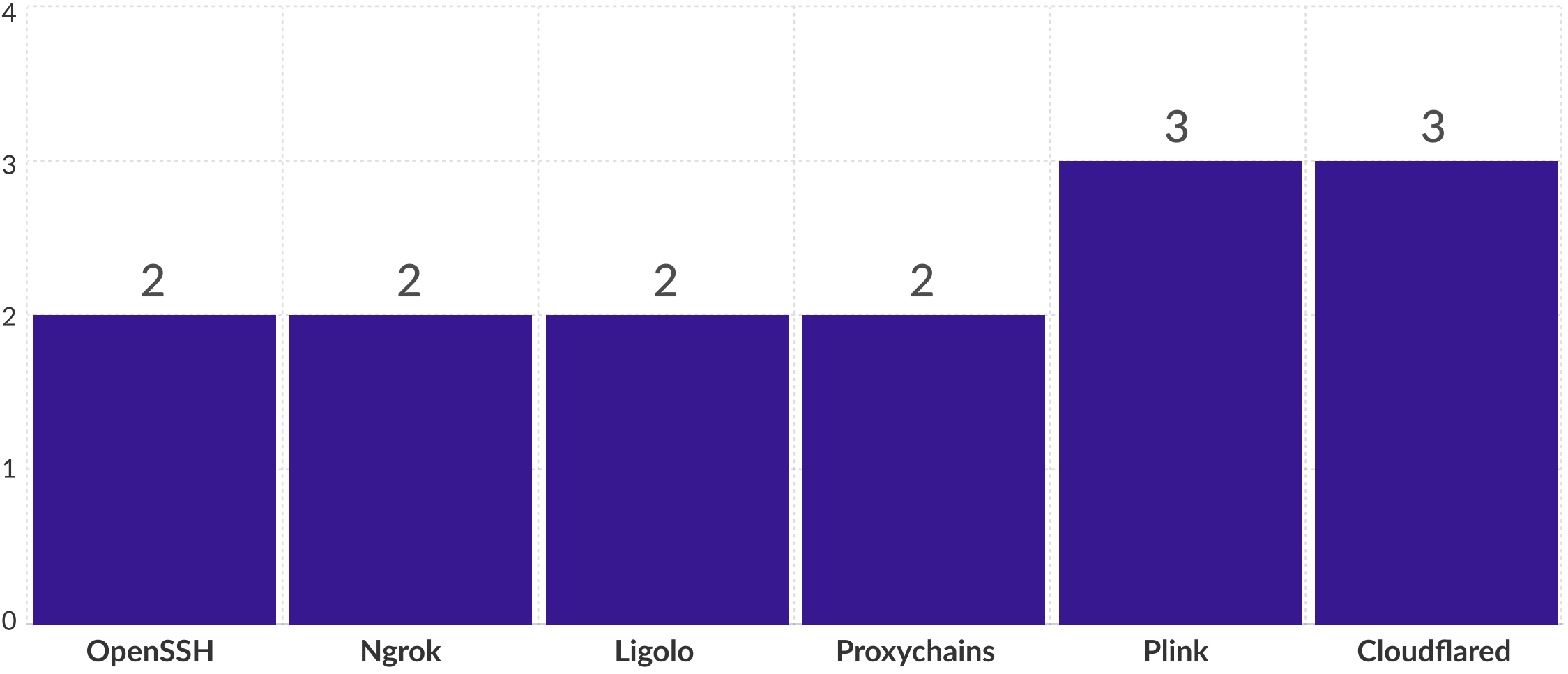
LOLBAS



DEFENSE EVASION



NETWORKING/ TUNNELING



MITRE ATT&CK Technique Prevalence – Healthcare Ransomware Groups

94 Groups | Scores reflect observed frequency across group TTPs



Attack lifecycle - consolidated kill chain

The following represents the composite attack lifecycle derived from observed TTPs across 94 ransomware groups, synthesized into a single unified pattern:

Initial Access (Days 1-3)

Attackers gain entry through one of three primary vectors: exploitation of public-facing applications (T1190) using known CVEs against VPN appliances, firewalls, or file-transfer software; use of compromised valid accounts (T1078) purchased from initial access brokers or obtained via brute force; or spearphishing delivery (T1566) of malicious Office documents triggering CVE-2017-0199 or similar execution exploits.



PHASE 1

Establishment (Days 1-7)

Persistence via account creation (T1136) and registry autostart entries (T1547). Cobalt Strike or Sliver C2 framework deployed. Defense evasion through disabling of Windows Defender (T1562), event log clearing (T1070), and in-memory execution to avoid on-disk signatures



PHASE 2

Reconnaissance (Days 7-35)

Credential harvesting via Mimikatz (T1003), LSASS dumping, and browser credential extraction. Network enumeration with SoftPerfect NetScan and Advanced IP Scanner. Active Directory mapping via BloodHound, AdFind, and PingCastle. Backup infrastructure identification -



PHASE 3

Staging (Days 30-48)

Data exfiltration using RClone (T1567.002) to cloud storage - MEGA, S3-compatible endpoints. Ransomware binary distributed to key servers via PsExec and lateral tool transfer (T1570). Backup destruction initiated. Weekend or after-hours execution scheduled.



PHASE 4

Phase 5 - Impact (Hours 0-1)

Simultaneous, multi-threaded encryption across all staged endpoints (T1486). Shadow copy deletion (T1490). IIS service termination (T1489) to encrypt web application data. ESXi hypervisor encryption targeting virtual disk files. Ransom notes deployed. C2 infrastructure decommissioned.



PHASE 5

Vulnerabilities Exploited



Vulnerabilities exploited

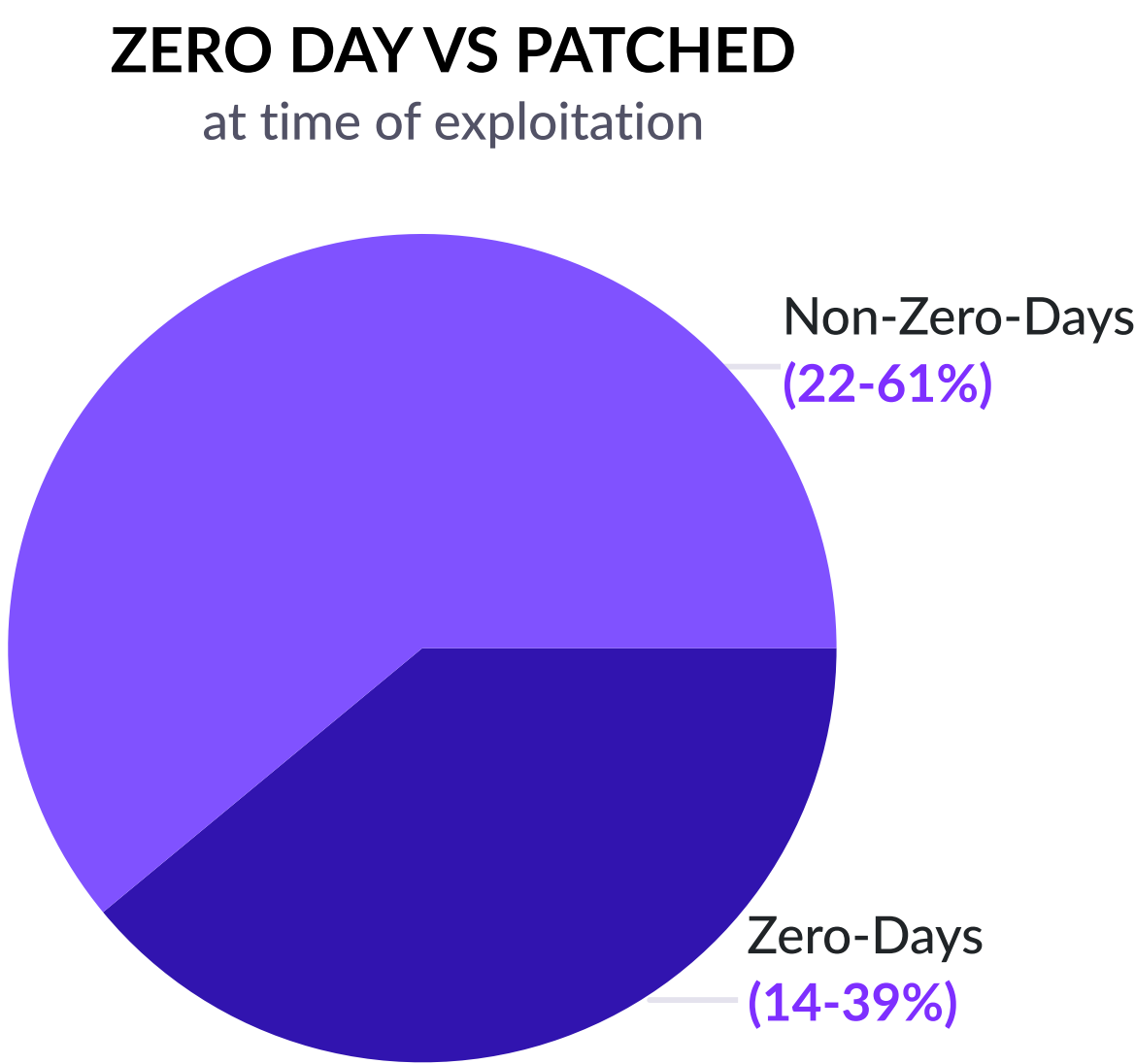
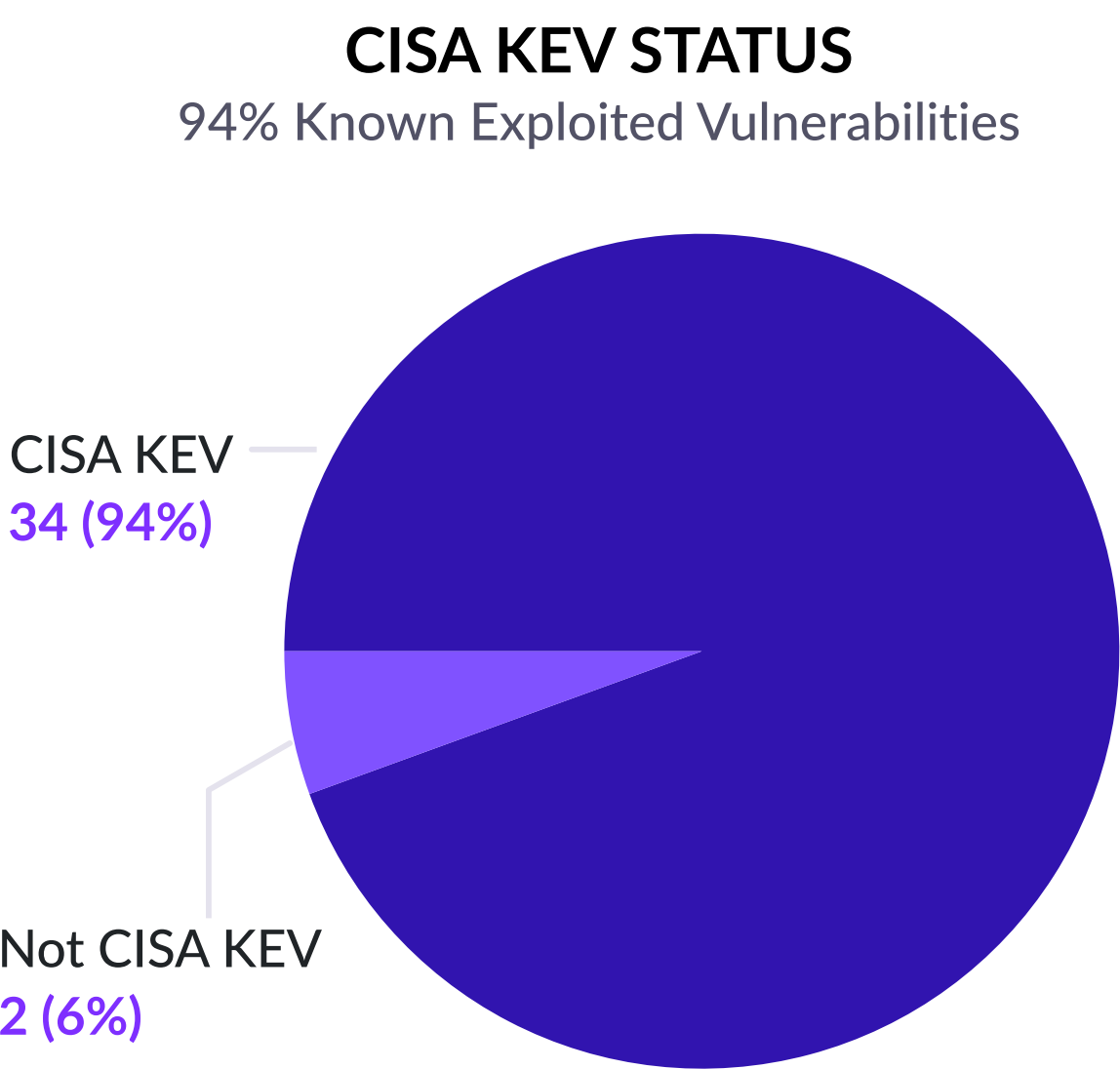
The vulnerabilities analyzed reflect a consistent pattern: attackers aren't searching for obscure weaknesses, but systematically exploiting known, high-impact exposures that persist in healthcare environments. The same vulnerabilities appear repeatedly because they continue to work.

EXPLOIT INTELLIGENCE OVERVIEW

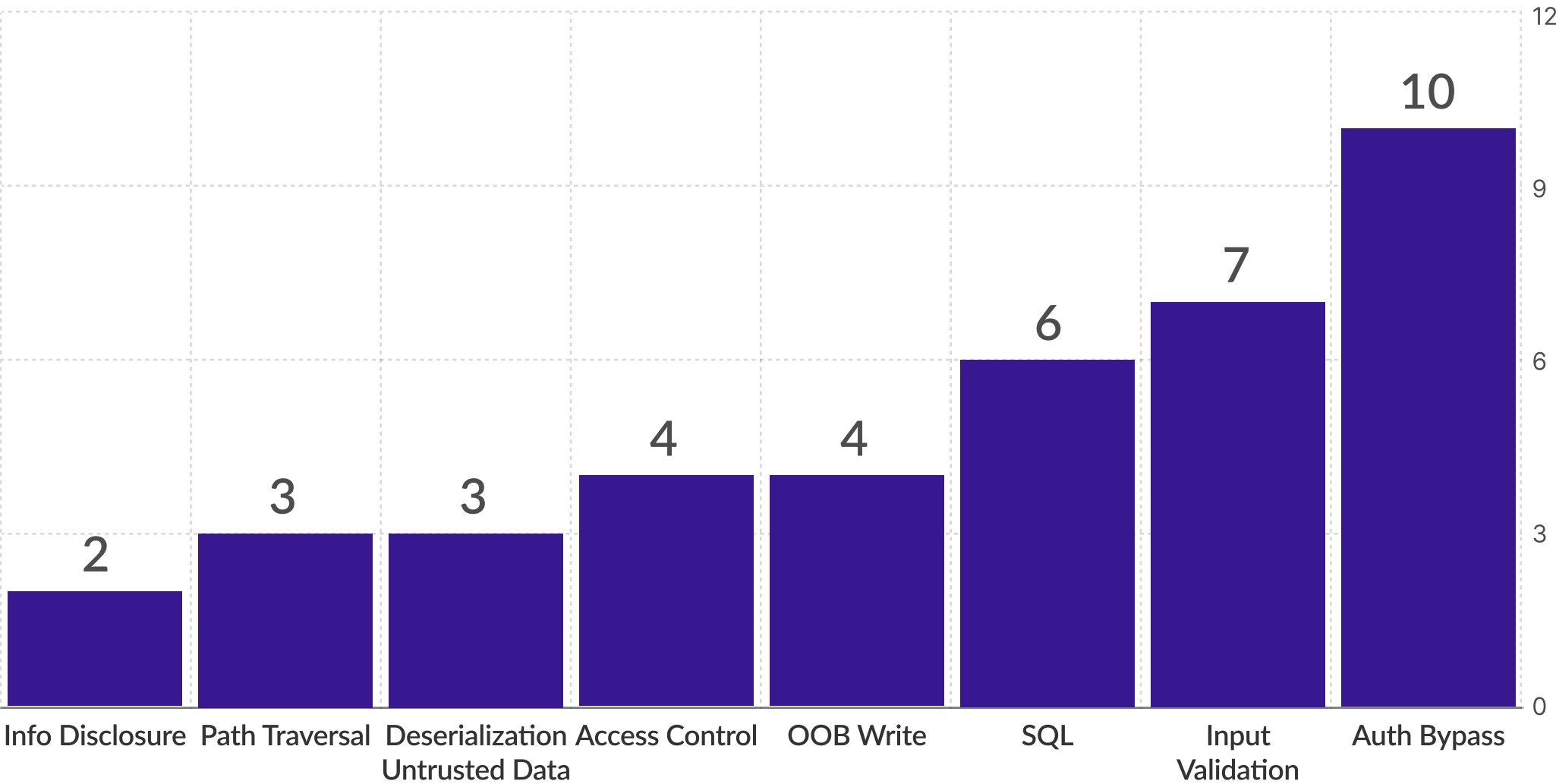
Twenty-nine CVEs were observed in active exploitation against healthcare organizations.

Every vulnerability appears in the CISA KEV catalog, confirming that attackers rely heavily on known but unremediated weaknesses.

Almost half of the vulnerabilities (48%) of the vulnerabilities were zero-days at the time of exploitation. CVE-2023-20263 and CVE-2023-27351 are the only entries not on the CISA KEV list, confirming their role as secondary or supporting exploitation steps rather than primary initial-access vectors.



CVE WEAKNESS CATEGORIES



COMPLETE EXPLOITED CVE REFERENCE

CVE	VENDOR / PRODUCT	ZERO-DAY	CISA KEV	KEV ADDED	ASSOCIATED WEAKNESSES	USED BY
CVE-2017-0144 (EternalBlue)	Windows SMBv1	✓	✓	2022-02-10	Improper Input Validation	RansomHub
CVE-2017-0148 (EternalBlue)	Windows SMBv1	✗	✓	2022-04-06	Improper Input Validation	WannaCry, Conti, Ryuk
CVE-2017-0199	Microsoft Office/WordPad	✓	✓	2021-11-03	Improper Privilege Mgmt, Improper Input Validation	80+ groups; Lokibot, Petya
CVE-2019-6693	Fortinet FortiOS	✗	✓	2025-06-25	Use of Hard-coded Credentials	Akira
CVE-2020-0787	Windows BITS	✗	✓	2022-01-28	Improper Link Resolution (Link Following)	RansomHub
CVE-2020-1472 (ZeroLogon)	Windows NetLogon	✗	✓	2021-11-03	Improper Authentication	RansomHub
CVE-2020-3259	Cisco ASA & FTD	✗	✓	2024-02-15	Exposure of Sensitive Info to Unauthorized Actor	Akira
CVE-2021-21972	VMware vSphere Client	✗	✓	2021-11-03	Path Traversal	Akira
CVE-2021-27101	Accellion FTA	✗	✓	2021-11-03	SQL Injection	CI0p

CVE	VENDOR / PRODUCT	ZERO-DAY	CISA KEY	KEY ADDED	ASSOCIATED WEAKNESSES	USED BY
CVE-2021-27102	Accellion FTA	×	✓	2021-11-03	OS Command Injection	CI0p
CVE-2021-27103	Accellion FTA	✓	✓	2021-11-03	Improper Input Validation	CI0p
CVE-2021-27104	Accellion FTA	×	✓	2021-11-03	Improper Input Validation	CI0p
CVE-2021-35211	SolarWinds Serv-U FTP	✓	✓	2021-11-03	Out-of-bounds Write, Memory Buffer Restriction	CI0p
CVE-2022-40684	Fortinet FortiOS	×	✓	2022-10-11	Improper Authentication	Akira
CVE-2023-0669	Fortra GoAnywhere MFT	✓	✓	2023-02-10	Deserialization of Untrusted Data	CI0p
CVE-2023-20263	Cisco ASA & FTD	×	×	-	URL Redirection (Open Redirect)	Akira
CVE-2023-20269	Cisco ASA & FTD	✓	✓	2023-09-13	Incorrect Authorization, Auth Bypass via Alternate Path	Akira
CVE-2023-22515	Atlassian Confluence	✓	✓	2023-10-05	Improper Authentication, Improper Input Validation	RansomHub
CVE-2023-27350	PaperCut Application Server	×	✓	2023-04-21	Improper Access Control	CI0p

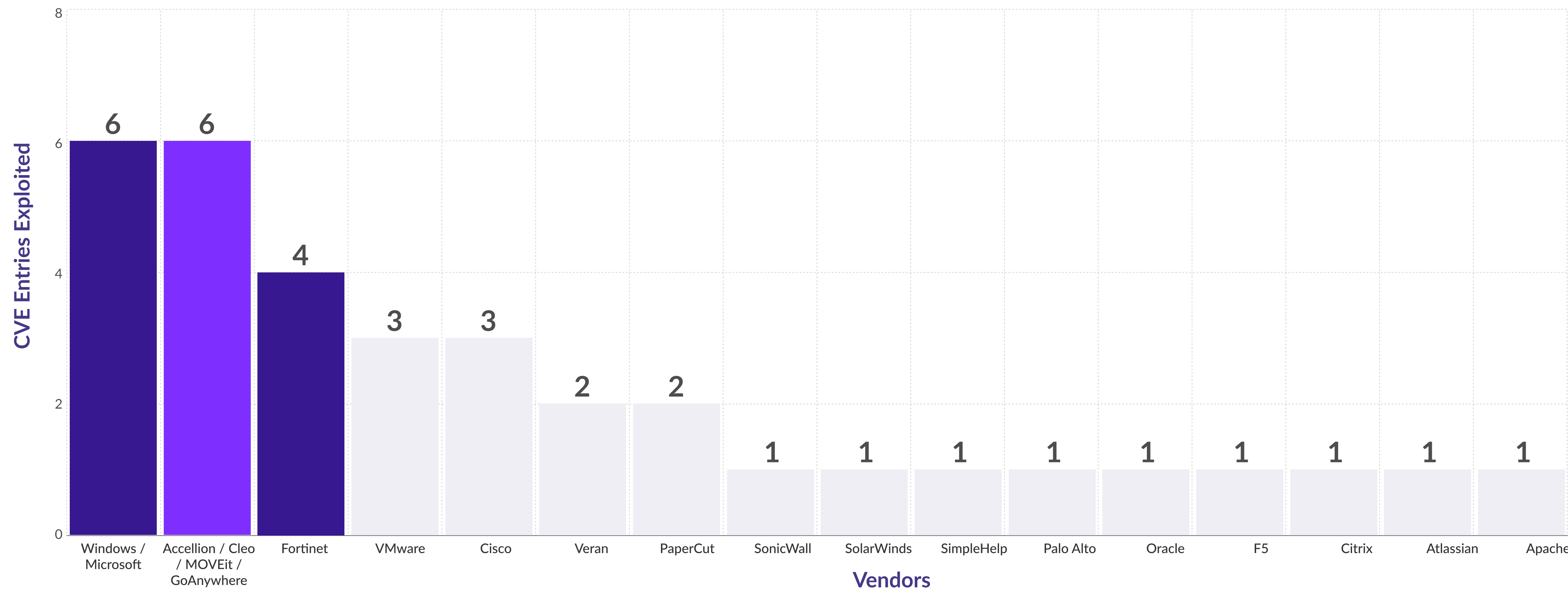
CVE	VENDOR / PRODUCT	ZERO-DAY	CISA KEY	KEY ADDED	ASSOCIATED WEAKNESSES	USED BY
CVE-2023-27351	PaperCut Application Server	×	×	-	Improper Authentication	ClOp
CVE-2023-27532	Veeam Backup & Replication	×	✓	2023-08-22	Missing Authentication for Critical Function	Akira
CVE-2021-27104	Fortinet FortiOS SSL-VPN	✓	✓	2023-06-13	Out-of-bounds Write, Memory Buffer Restriction	RansomHub
CVE-2023-28252	Microsoft Windows CLFS	✓	✓	2023-04-11	Out-of-bounds Write, Heap-based Buffer Overflow	BrainCipher
CVE-2023-34362	Progress MOVEit	✓	✓	2023-06-02	SQL Injection	ClOp
CVE-2023-3519	Citrix NetScaler ADC/ Gateway	✓	✓	2023-07-19	Code Injection	RansomHub
CVE-2023-46604	Apache ActiveMQ	×	✓	2023-11-02	Deserialization of Untrusted Data	RansomHub
CVE-2023-46747	F5 BIG-IP	×	✓	2023-10-31	Missing Auth for Critical Function, Auth Bypass via Alternate Path	RansomHub
CVE-2023-48788	Fortinet FortiClientEMS	×	✓	2024-03-25	SQL Injection	RansomHub,Akira

CVE	VENDOR / PRODUCT	ZERO-DAY	CISA KEY	KEY ADDED	ASSOCIATED WEAKNESSES	USED BY
CVE-2024-21762	Fortinet FortiOS (SSL-VPN)	✓	✓	2024-02-09	Out-of-bounds Write	Qilin
CVE-2024-3400	Palo Alto PAN-OS GlobalProtect	✓	✓	2024-04-12	Command Injection, Improper Input Validation	Multiple affiliates
CVE-2024-37085 (ESX Admins)	VMware ESXi	✗	✓	2024-07-30	Auth Bypass by Primary Weakness, Improper Authentication	Akira
CVE-2024-40711	Veeam Backup & Replication	✗	✓	2024-10-17	Deserialization of Untrusted Data	Akira
CVE-2024-40766	SonicWall SonicOS SSL- VPN	✗	✓	2024-09-09	Improper Access Control	Akira
CVE-2024-55956	Cleo VLTrader / Harmony / LexiCom SonicOS SSL-VPN	✓	✓	2024-12-17	Command Injection, Incorrect Default Permissions	CI0p
CVE-2024-57727	SimpleHelp RMM	✗	✓	2025-02-13	Path Traversal	Medusa
CVE-2025-61882	Oracle E-Business Suite	✓	✓	2025-10-06	Missing Authorization, Improper Authentication	CI0p

Vendor Exposure Profile

Microsoft/Windows and Fortinet together account for 10 of 36 CVE entries

This concentration reflects both vendors' ubiquity in healthcare IT environments, and the sustained adversarial focus on systems that provide network perimeter access or administrative control. File-transfer infrastructure (Accellion, Cleo, MOVEit, GoAnywhere) is the highest-impact single attack surface: ClOp's mass-exploitation campaigns across these platforms account for a disproportionate number of breach notifications.



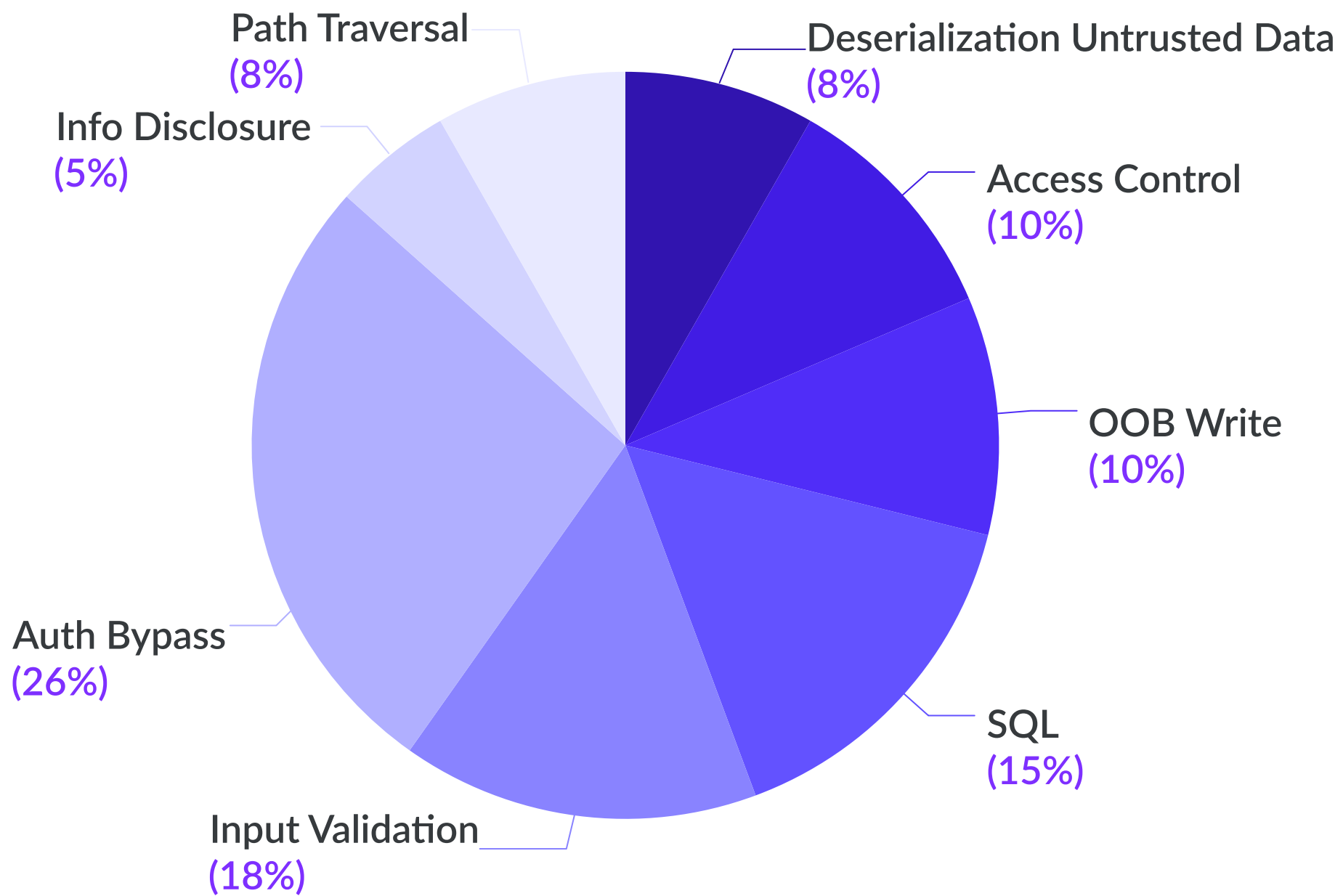
Weakness Analysis



The Anatomy of Healthcare Exploitation

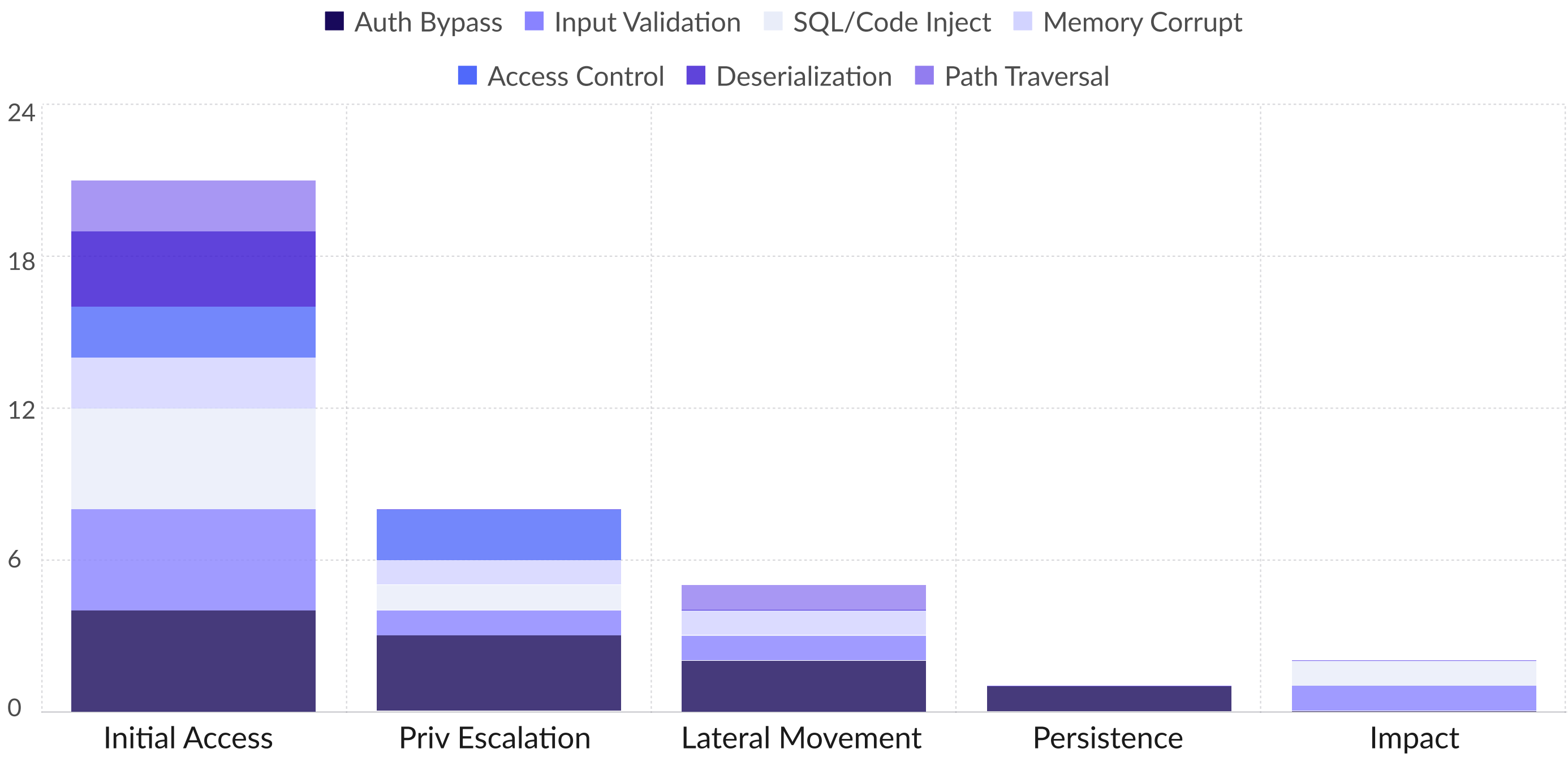
The exploited CVEs don't operate in isolation. They cluster into a small number of recurring weakness patterns that attackers repeatedly exploit to move from access to full compromise. Understanding these weakness categories, not just individual CVEs, enables durable defensive investment.

CWE CATEGORY DISTRIBUTION ACROSS 36 CVE ENTRIES



WEAKNESS CLASSES BY ATTACK PHASE

(Where each CWE primarily enables entry)





Authentication Bypass

(10 CVEs)

Authentication bypass is the single most prevalent weakness category, present across ZeroLogon (CVE-2020-1472), Fortinet FortiOS (CVE-2022-40684), Atlassian Confluence (CVE-2023-22515), Cisco ASA (CVE-2023-20269), Veeam (CVE-2023-27532), F5 BIG-IP (CVE-2023-46747), VMware ESXi (CVE-2024-37085), and Oracle E-Business Suite (CVE-2025-61882). The exploitation chain is consistent across all: a missing, bypassed, or incorrectly implemented authentication check provides direct access to a privileged function or network service — no credentials required.

Healthcare's particular vulnerability to this class stems from the sector's complexity. Authentication controls that are well-implemented in purpose-built clinical applications frequently fail at integration points — the API connectors, administrative interfaces, and backup platforms that stitch together disparate systems. These interfaces were designed for operational efficiency rather than security, and they constitute the realistic initial access surface for most ransomware intrusions.

DEFENSIVE PRIORITY:

Multi-factor authentication, network access controls on administrative interfaces, and zero-trust access policies directly mitigate this entire weakness class



DOMINANT WEAKNESS CLASS



Input Validation & Injection Chains

(13 CVEs Combined)

Input validation failures (7 CVEs) and their downstream exploitation as SQL injection, OS command injection, and code injection (6 CVEs) form an interconnected attack surface. CVE-2024-3400 (Palo Alto, Command Injection, Zero-Day) and CVE-2024-55956 (Cleo, Command Injection, Zero-Day) demonstrate that even security-focused vendors ship products with injection vulnerabilities that attackers exploit before patches exist.

The Accellion FTA campaign (CVE-2021-27101 through 27104) shows how a single product with multiple injection flaws — SQL injection, OS command injection, and SSRF — can be chained into complete system compromise.

Healthcare web applications, patient portals, and legacy clinical systems present a disproportionate attack surface for these vulnerabilities because they were developed before secure coding practices were standardized and operate in environments where security testing is constrained by clinical workflow dependencies.



DISPROPORTIONATE ATTACK SURFACE



Memory Corruption

(4 CVEs)

Out-of-bounds write and heap-based buffer overflow vulnerabilities (CVE-2021-35211, CVE-2023-27997, CVE-2023-28252, CVE-2024-21762) concentrate on perimeter-facing infrastructure: SolarWinds Serv-U FTP, Fortinet FortiOS SSL-VPN, Windows CLFS kernel component, and Fortinet FortiOS again. Three of four were zero-days at exploitation time. Memory corruption vulnerabilities in perimeter devices are especially valuable to attackers because they execute before any internal detection controls are reached.



PERIMETER DEVICE TARGETING



Deserialization

(3 CVEs)

Deserialization vulnerabilities (CVE-2023-0669 in GoAnywhere, CVE-2023-46604 in Apache ActiveMQ, CVE-2024-40711 in Veeam) produce reliable, low-noise remote code execution — a preferred class for both CI0p (GoAnywhere mass exploitation) and Akira (Veeam targeting). These vulnerabilities require minimal exploitation skill once proof-of-concept code is available, making them favored by RaaS affiliates operating at scale.



HIGH-RELIABILITY EXPLOITATION

THE PATCHING CONSTRAINT REALITY

Healthcare organizations face a structural constraint that distinguishes them from other sectors: patching is operationally constrained. FDA regulations require revalidation of medical device firmware after software changes. EHR systems require weeks of testing before updates can be deployed to prevent clinical errors. Critical infrastructure — laboratory systems, imaging networks, pharmacy management platforms — cannot be taken offline during business hours. The result is that known, actively exploited vulnerabilities (all 29 on the CISA KEV list) remain present in healthcare environments for months to years after disclosure, creating reliable and persistent attack opportunities.

Attack Vector Analysis



Attack vector analysis



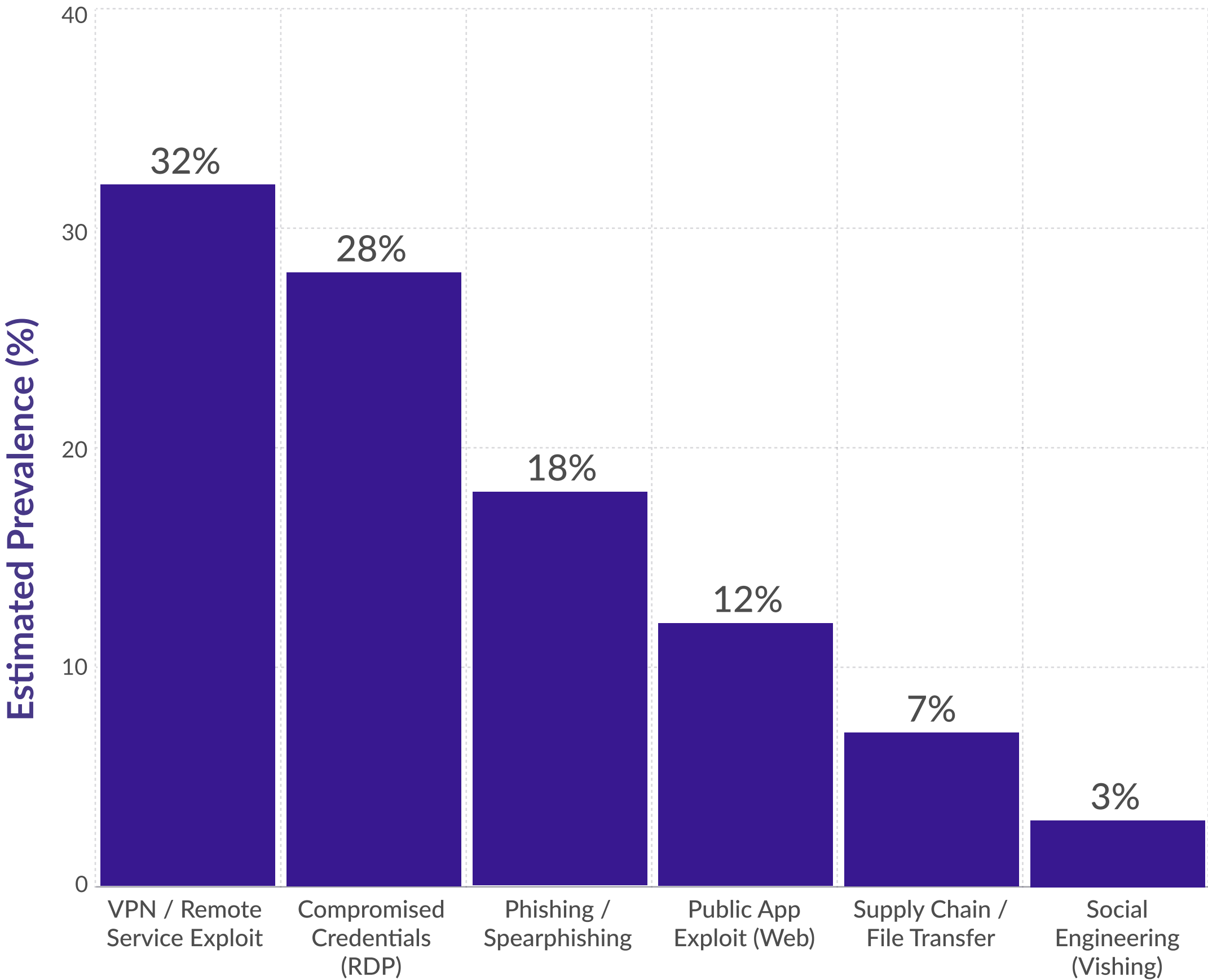
VPN and remote service exploitation (T1190/T1133) is the leading initial access vector, accounting for approximately 32% of tracked intrusions. This reflects the explosion of healthcare remote access infrastructure - accelerated by telehealth adoption - combined with the concentration of CVEs against SSL-VPN products from Fortinet, Cisco, SonicWall, and Citrix. A single unpatched VPN appliance provides direct access to the internal network without triggering perimeter defenses.



Compromised credentials via RDP brute force or purchased initial access (T1078) accounts for 28%. The initial access broker market has matured significantly: specialized threat actors compromise healthcare organizations and sell authenticated network access for \$2,000–\$50,000, lowering the barrier to entry for ransomware affiliates who lack technical exploitation skills.



Phishing (T1566) drives 18% of initial access, concentrated in groups targeting research institutions (GTG-2002) and in opportunistic campaigns by groups like TA584. CVE-2017-0199 (Microsoft Office RCE, Zero-Day) remains among the most exploited vulnerabilities globally precisely because phishing is effective and Office document workflows are deeply embedded in healthcare operations.



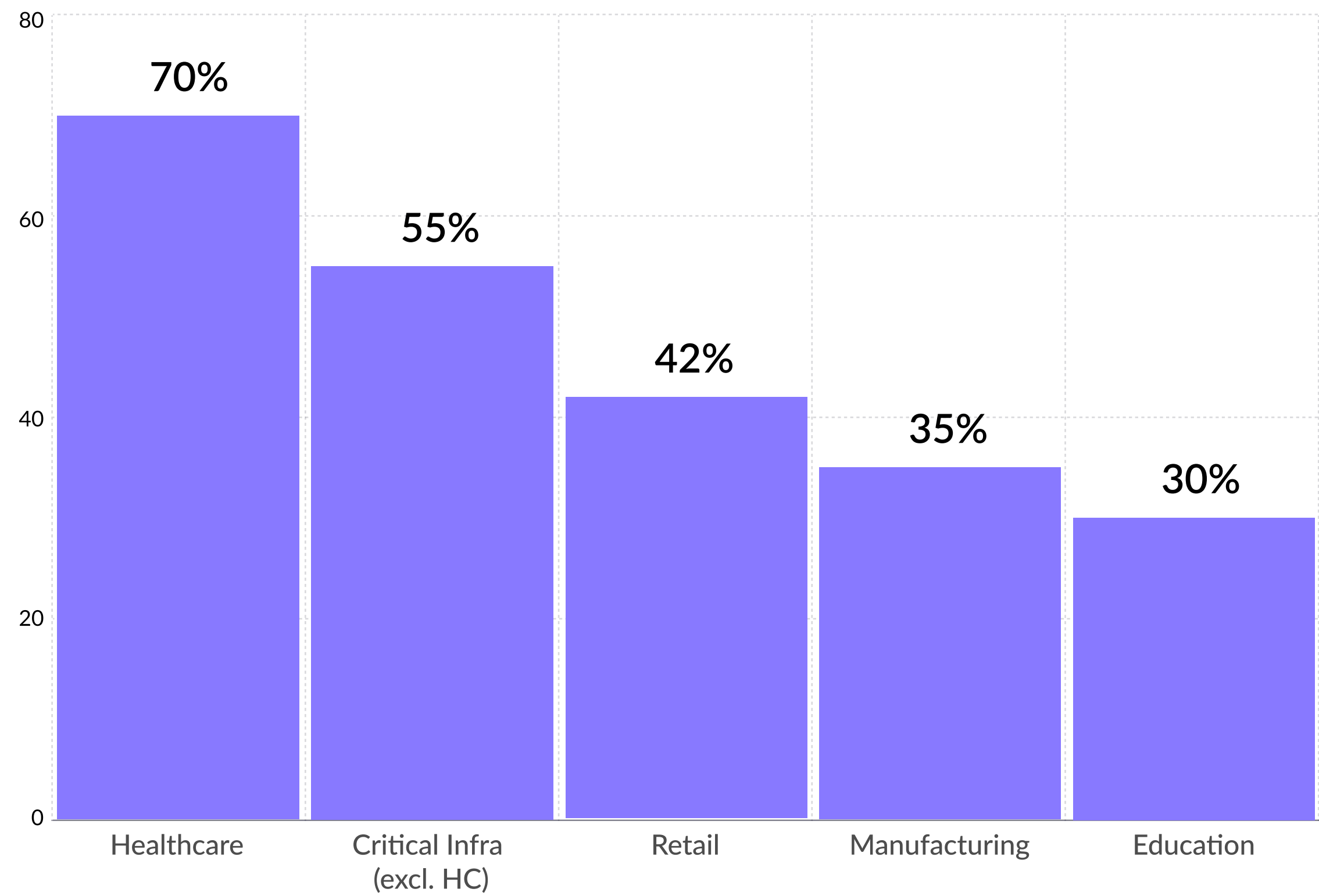
Why Healthcare Pays



The Economic Calculus

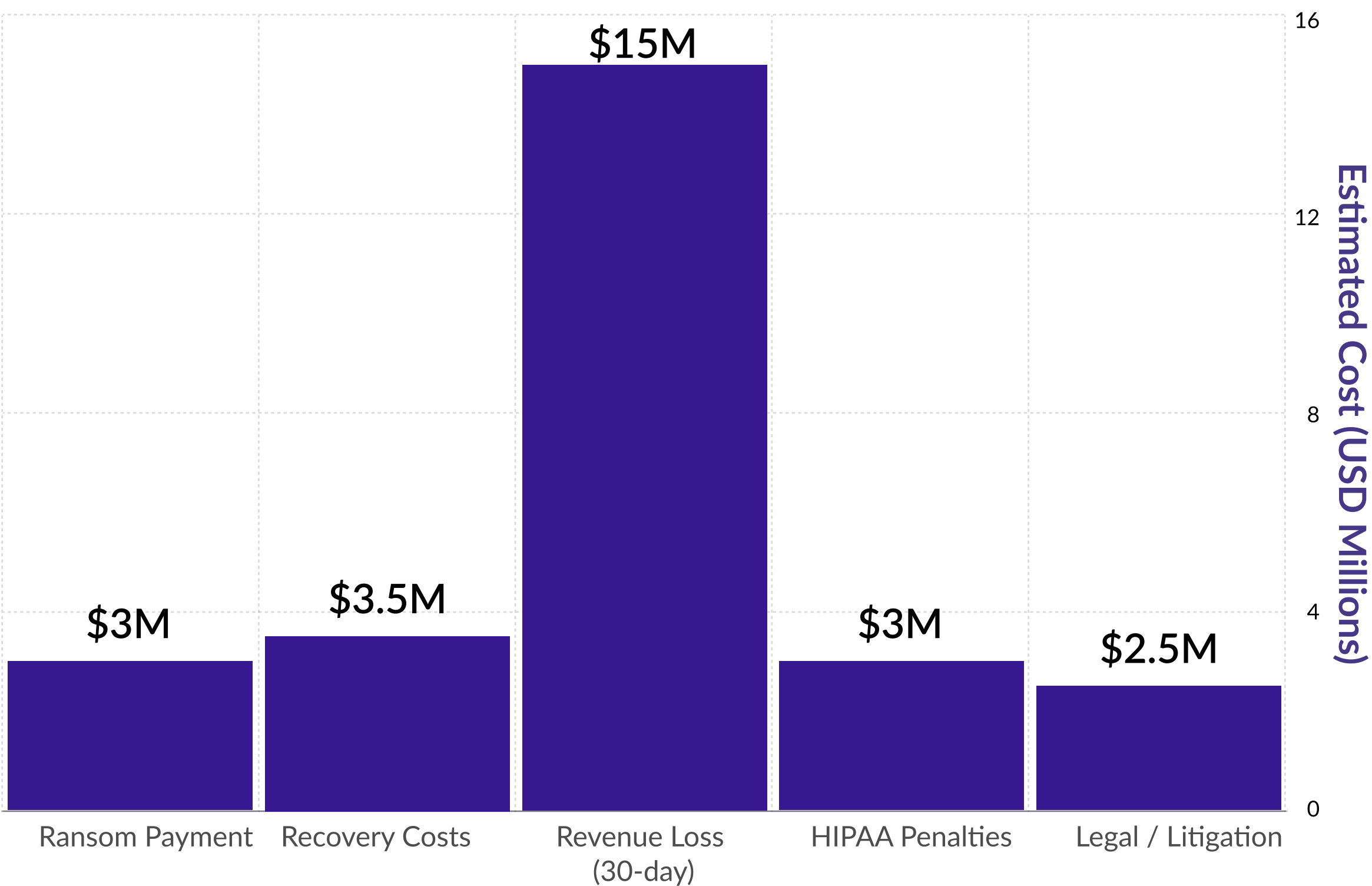
Healthcare pays ransoms at a **68–72% rate**, compared to a cross-sector average of approximately 40%. This elevated payment rate is self-reinforcing: it signals to threat actors that healthcare is reliably profitable, driving further targeting and specialization.

RANSOM PAYMENT RATE BY SECTOR



TOTAL INCIDENT COST BREAKDOWN

Mid-Sized Hospital (~400 beds)



Payment Drivers

Operational Criticality

Healthcare is unique in that downtime carries direct patient safety risk. Emergency departments diverting ambulances, cancelled surgical procedures, pharmacy system failures, and inaccessible electronic health records create clinical liability and regulatory exposure that accelerates payment decisions. A hospital losing \$1–2M per day in cancelled procedures will typically pay a \$3M ransom by day three rather than endure three weeks of manual operations

Data Value

Protected Health Information commands \$250–\$1,000 per complete record on underground markets — an order of magnitude above credit card data (\$5–\$15). Medical records contain Social Security numbers, insurance data, prescription histories, and diagnosis codes, making them suitable for insurance fraud, drug fraud, identity theft, and tax fraud. Unlike financial credentials that can be cancelled, medical histories are permanent. Ransomware operators exploit this with double-extortion: payment for decryption, followed by threats to publish PHI if further demands are unmet.

Insurance Coverage

90%+ of hospital systems carry cyber insurance with ransom coverage. Insurers routinely recommend payment as the lower-cost option compared to extended recovery. The existence and limits of coverage (\$5M–\$10M typical) are researchable by attackers, who calibrate demands to policy maximums.

Regulatory Pressure

HIPAA requires timely access to medical records and mandates breach notification for incidents affecting PHI. Extended downtime creates a compliance violation independent of the ransomware payment decision. OCR investigations follow, with average enforcement actions reaching \$1.5M–\$5M.

Mitigation Priorities & Regulatory Environment



Mitigation Priorities: defensive action framework

Effective defense against this threat landscape requires addressing the root weakness categories driving the majority of exploitation, not reactive patching of individual CVEs.

Immediate Actions (0–30 days)



Multi-factor authentication (MFA) addresses the dominant weakness class - 10 CVEs relating to authentication bypass are neutralized when MFA is enforced at the network perimeter and all administrative interfaces. **No other single control eliminates more attack surface.**



CISA KEV patch prioritization provides a deterministic, intelligence-backed patch queue. The 100% CISA KEV rate across all 29 tracked CVEs means the KEV catalog is a direct map of the active exploit set targeting healthcare. Establish a policy: KEV vulnerabilities patched within 14 days for internet-facing systems, 30 days for internal systems.



Backup integrity validation with offline/immutable copies is the primary recovery capability. Ransomware groups invest heavily in backup discovery and destruction. WORM (Write Once Read Many) storage for backup repositories, HSM-protected decryption keys, and tested restoration procedures reduce recovery time objectives to hours rather than weeks.



Endpoint detection and response (EDR) deployed across clinical and administrative endpoints provides the visibility needed to detect credential harvesting (Mimikatz), lateral movement (PsExec, WMI), and staging behavior in the 10–50 day dwell period preceding encryption.



Network segmentation of IoMT devices, EHR platforms, and administrative networks contains the blast radius of any successful intrusion. EternalBlue-class vulnerabilities (CVE-2017-0144, CVE-2017-0148) propagate across flat networks — segmentation turns a domain-wide incident into a contained one.

Short-Term (30–90 days)



Privileged access management (PAM) for administrative and service accounts. VPN replacement with zero-trust network access (ZTNA). Monthly phishing simulations with healthcare-specific scenarios - fake patient referrals, spoofed vendor updates, ClickFix CAPTCHA lures. Quarterly credential audits and forced resets for privileged users.

Long-Term (90–365 days)



Zero-trust architecture adoption Migration of legacy systems where clinical workflow dependencies allow. Threat intelligence program integration to operationalize CVE and threat actor intelligence. Healthcare-specific incident response playbooks covering clinical continuity during cyber events. Enrollment in H-ISAC for sector-specific threat sharing.

Regulatory & insurance environment



HIPAA Ransomware Exposure

Any ransomware incident affecting PHI is presumed a breach under HIPAA absent documented evidence to the contrary. The **60-day OCR notification requirement** creates regulatory pressure independent of the payment decision. OCR enforcement actions for ransomware-related HIPAA violations have averaged \$1.5M-\$5M with multi-year corrective action plans. OCR scrutiny focuses on pre-breach security practices: MFA deployment, vulnerability assessment frequency, staff training records



Cyber Insurance Tightening

Healthcare sector **premiums increased 300-500%** between 2022 and 2025. MFA and EDR are now underwriting prerequisites - absence of either typically results in claim denial or coverage rescission. Insurers increasingly include known-unpatched-vulnerability exclusions: if a CVE older than 90 days appears on a vulnerability scan at the time of incident, the claim may be denied. Offline backup requirements are becoming standard policy conditions

Threat Outlook

Threat Outlook



Near-term (Q2–Q3 2026)

Qilin and ClOp will continue to dominate attack volume. ClOp's pattern of zero-day mass exploitation against file-transfer infrastructure will produce the next major healthcare breach wave, likely targeting a new file-transfer or MFT product. ESXi-targeting ransomware becomes standard capability across mid-tier groups as virtualized healthcare infrastructure expands.



Structural shifts

The initial access broker ecosystem is maturing and lowering barriers to entry, increasing the total number of groups capable of targeting healthcare. Social engineering via AI-generated voice and text (Scattered Spider model) will become more widespread as technical exploitation becomes commoditized. Oracle E-Business Suite exploitation (CVE-2025-61882) signals adversarial expansion into ERP-layer healthcare infrastructure.



Signal to watch

RansomHub's broad CVE coverage and affiliate model positions it for sustained growth. Groups like Anubis (13 attacks) and DragonForce (14 attacks) are showing accelerating activity that may reach top-tier status within one to two quarters.

Conclusion

Conclusion

The healthcare sector faces a persistent, structurally entrenched cyber threat environment. Ninety-four ransomware groups are actively targeting an industry where operational disruption carries immediate consequences, and where sensitive data retains long-term value.

The most striking intelligence signal in Securin's dataset is the 100% CISA KEV coverage across exploited vulnerabilities. Attackers aren't relying on obscure techniques; they're exploiting weaknesses that are already publicly known and widely documented.

Organizations that successfully reduce risk consistently implement the same core controls:



Enforced multi-factor authentication (MFA)



Immutable online backups



Endpoint detection with continuous monitoring



Network segmentation



KEV-prioritized vulnerability remediation

These measures don't eliminate the threat, but they significantly reduce the attack surface that ransomware groups currently exploit at scale.

Closing the gap between exposure and exploitation

Securin enables healthcare organizations to move from reactive patching and vulnerability management to intelligence-driven exposure management. By continuously mapping real-world exploit activity to your specific attack surface, Securin prioritizes vulnerabilities for remediation based on active threat relevance, not theoretical severity. The result is a proactive defense posture where remediation isn't assumed complete, but continuously tested and proven effective against the same techniques adversaries use in real-world attacks.

You don't need more data, you need to know if you're exposed - and that your remediation works. Securin helps healthcare defenders to answer those questions definitely.

Think about it. We do.

Securin is an AI-driven cybersecurity company helping organizations identify, validate, and eliminate real-world risk, before it becomes a breach. Trusted by enterprises and government organizations, Securin combines AI and human expertise to prioritize the risks that actually matter, so teams can act faster and stay ahead.

