Exploited Vulnerabilities and the Cost of Downtime

A federal-data brief — plus how AlwaysRecover reduces downtime with Disaster Recovery as a Service (DRaaS).

KEV snapshot date: 2025-12-15T18:15:53.1952Z • KEV entries: 1,477

One-sentence thesis

Known exploitation tells you what can happen. Recovery time tells you what it costs. When attackers exploit real vulnerabilities at scale, slow restoration is what turns incidents into expensive events.

KEV highlights: 1,477 exploited vulnerabilities; 303 flagged as used in known ransomware campaigns (20.5%).

Cost highlights: the CISA Office of the Chief Economist (OCE) shows heavy■tailed losses — medians are reasonable, means get pulled by rare disasters. Planning based on “average incident cost” is a repeatable mistake.

If you’ve been in this industry long enough, you’ve seen the cycle: headlines, vendor fear■math, and dashboards that don’t restore operations. **This brief is calmer:** federal data + plain language + charts you can defend in a boardroom.

KEV trend analysis (Known Exploited Vulnerabilities)

KEV is maintained by the Cybersecurity and Infrastructure Security Agency (CISA). Each entry references a CVE (Common Vulnerabilities and Exposures) identifier for the underlying vulnerability.

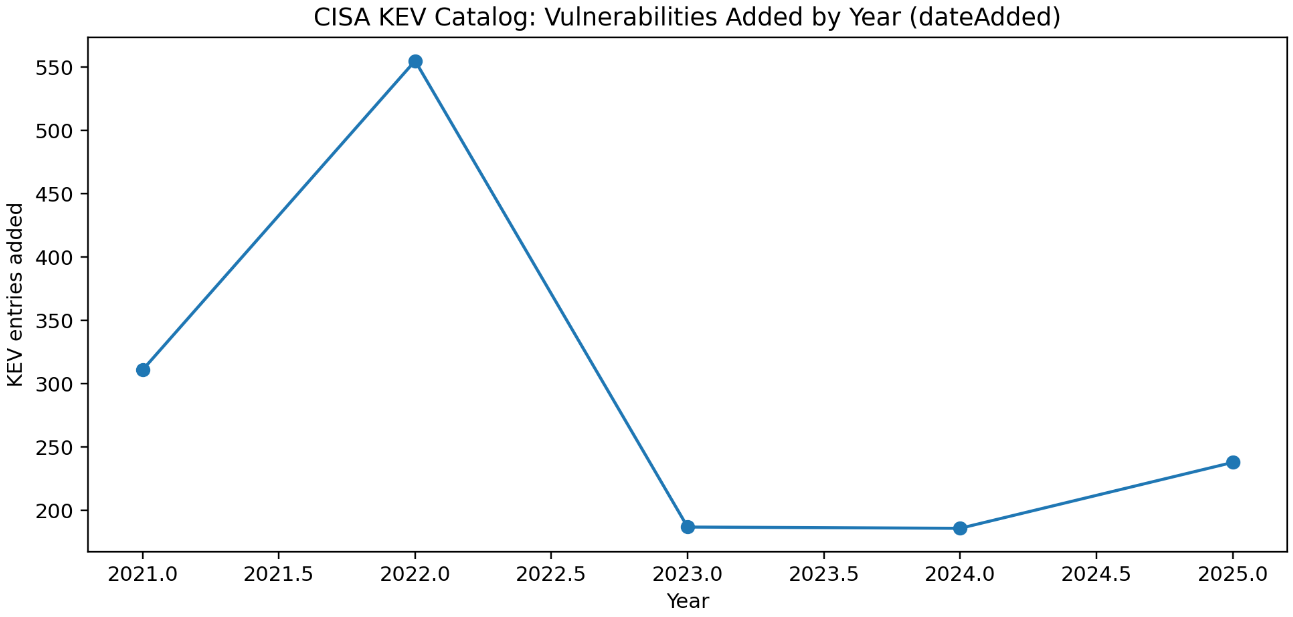

Figure 1. KEV entries added by year (dateAdded).

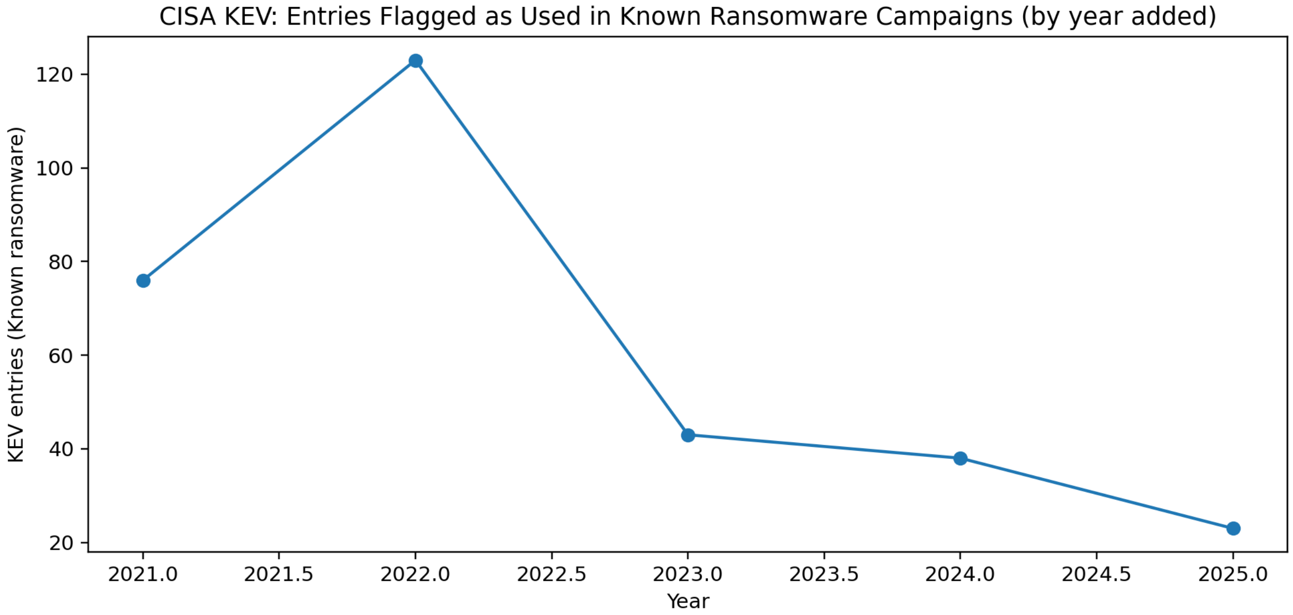

Figure 2. KEV entries flagged as used in known ransomware campaigns, by year added.

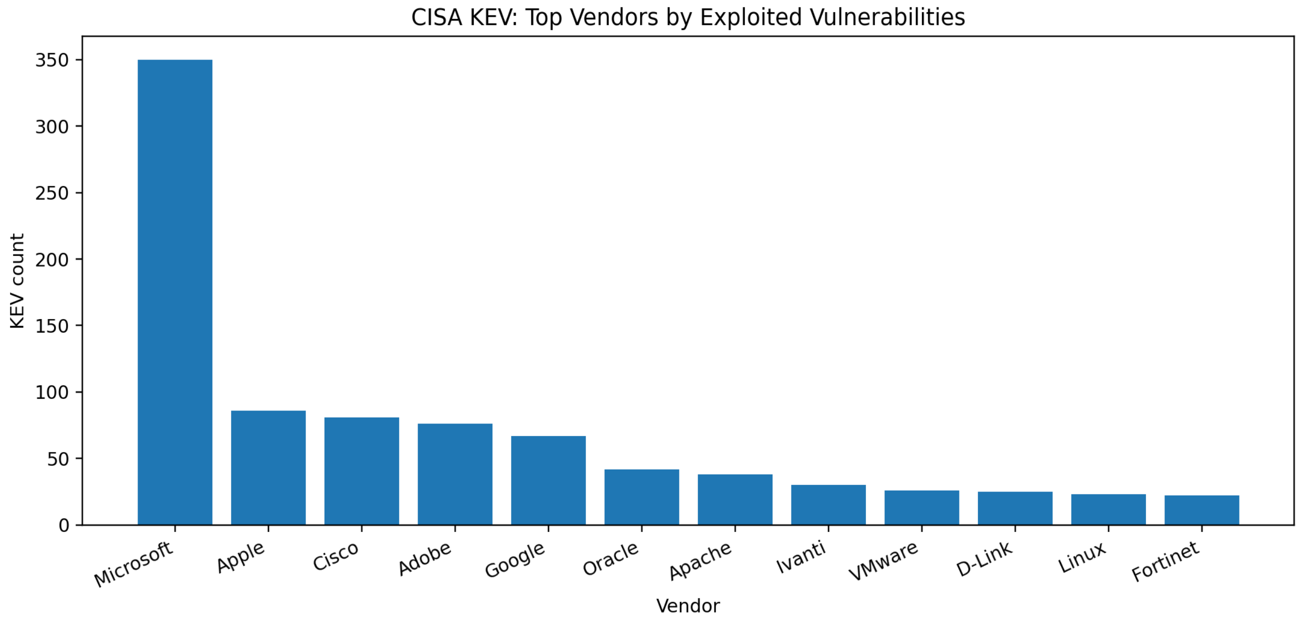

Figure 3. Top vendors by KEV count.

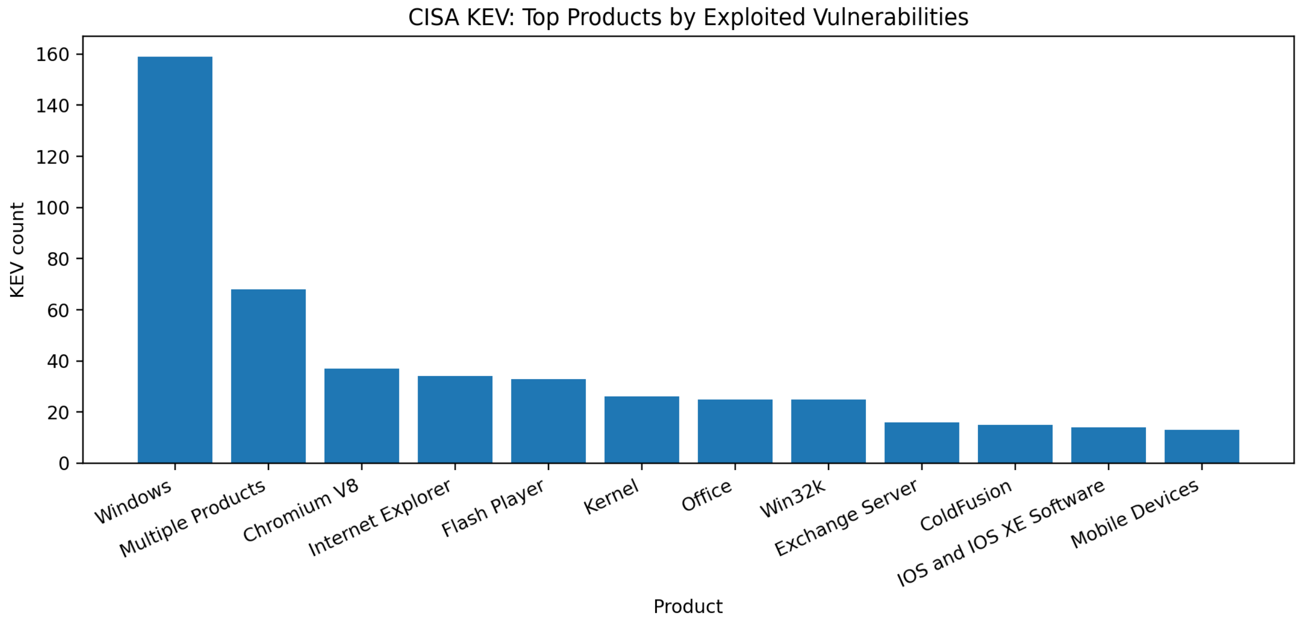

Figure 4. Top products by KEV count.

What KEV implies about exploit outcomes

Some vulnerabilities enable RCE (Remote Code Execution): attackers can run code on your systems. Others enable command injection, privilege escalation, or authentication bypass. Outcome matters because it determines recovery complexity.

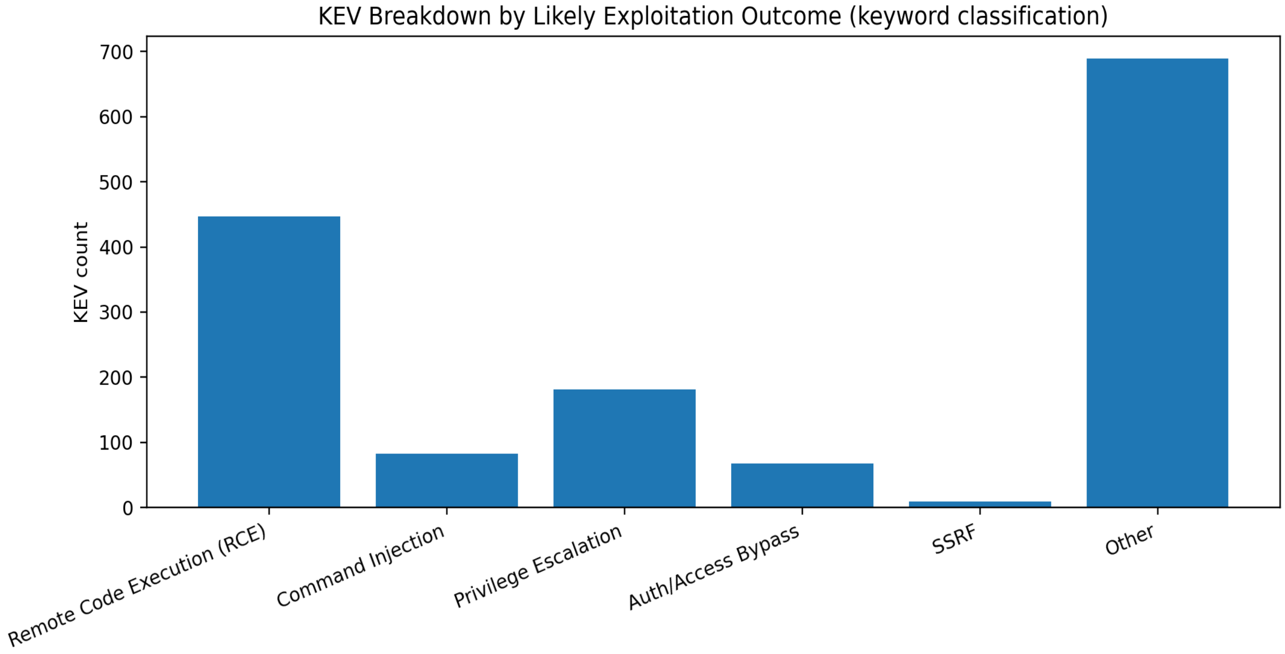

Figure 5. Outcome classification using conservative keyword matching on KEV titles/descriptions.

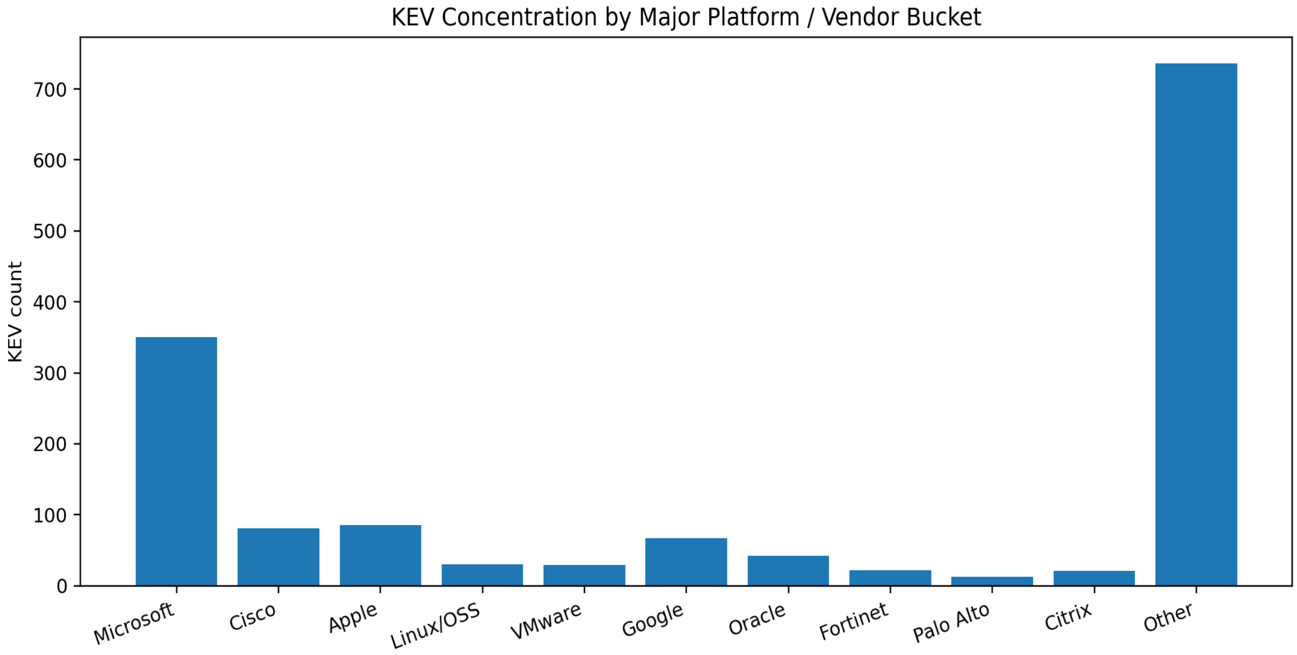

Figure 6. Vendor/platform concentration buckets.

The cost side (Office of the Chief Economist)

The OCE synthesis shows heavy■tailed loss: most incidents cost far less than the mean, but a small fraction become wildly expensive when recovery drags and operations stay down.

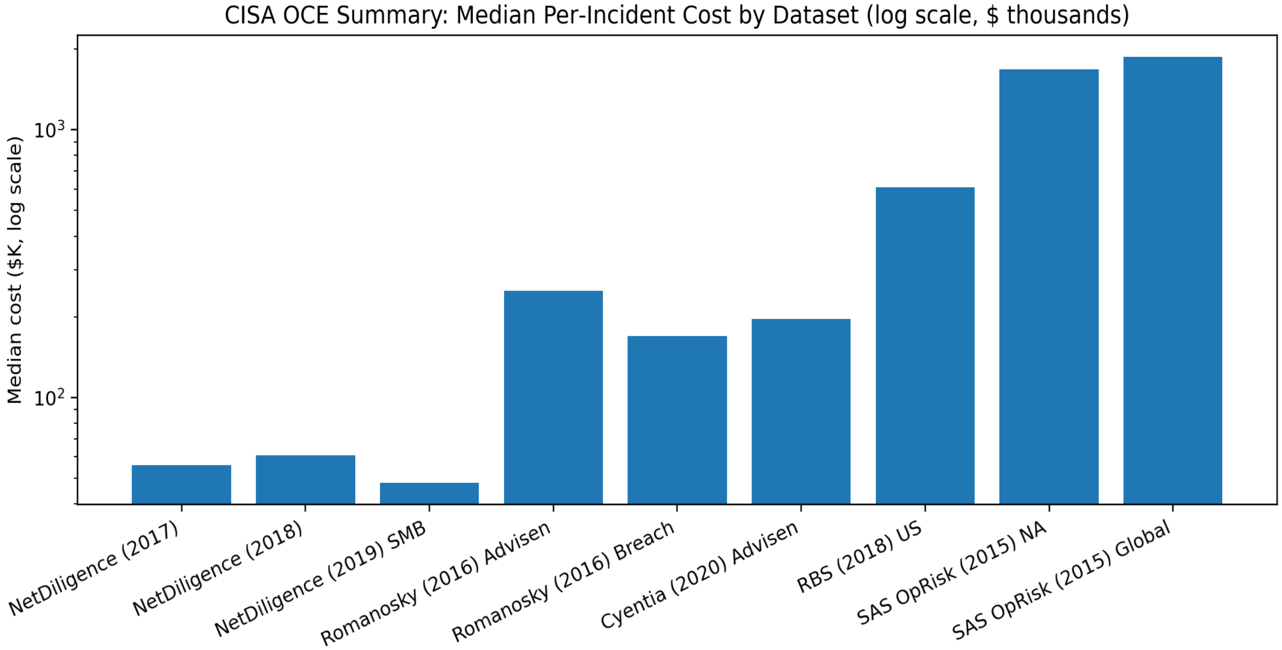

Figure 7. Median per■incident costs by dataset (log scale). Values summarized from the OCE report Table 1.

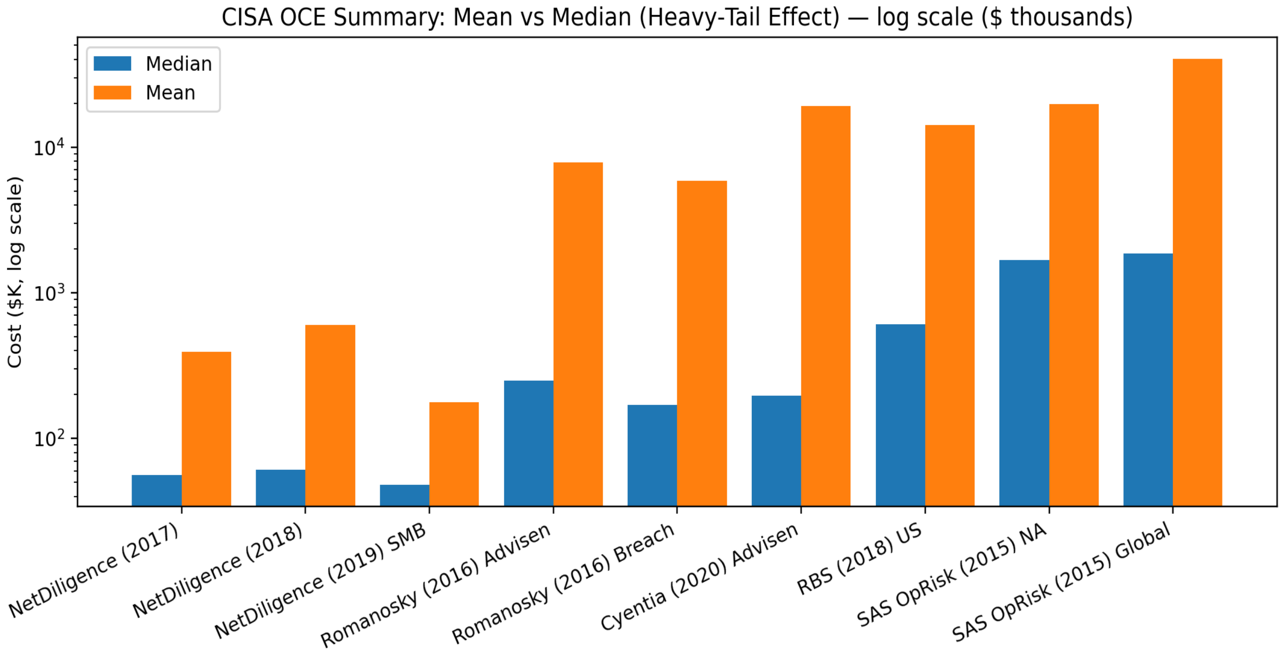

Figure 8. Mean vs median (heavy■tail effect) — log scale.

So what do you do about it? DRaaS in plain English

DRaaS (Disaster Recovery as a Service) is a managed capability to restore critical systems and workloads after disruptive events — including ransomware and destructive attacks. In practice, DRaaS reduces downtime by ensuring you have tested recovery paths, clean restoration procedures, and operational runbooks that work under pressure.

AlwaysRecover's stance: You can't control whether someone tries to break in. You can control whether recovery is slow and chaotic.

Typical DRaaS outcomes that matter to executives:

- Faster restoration of core workloads
- Lower operational disruption (fewer days of partial operations)
- Reduced decision chaos during an incident (clear runbooks and roles)
- Higher confidence in recovery assumptions (tested, not hoped)

Key terms (plain English)

Term	Meaning
CISA	Cybersecurity and Infrastructure Security Agency — U.S. federal agency that publishes KEV and econom
KEV	Known Exploited Vulnerabilities — vulnerabilities confirmed to be exploited in real attacks.
CVE	Common Vulnerabilities and Exposures — standardized identifier for a specific vulnerability.
OCE	Office of the Chief Economist — CISA group that produced the incident-cost synthesis.
RCE	Remote Code Execution — attacker can run code on a system remotely.
DRaaS	Disaster Recovery as a Service — managed recovery capability to restore systems and operations after d
Downtime	Time systems are unavailable; often the main driver of business impact.
Recovery	Restoring systems and operations (and re-establishing trust) after an incident.