

KEY FINDINGS

Cyber Threat Index 2024

Businesses faced an onslaught of digital risks in 2023. Threat actors leveraged common vulnerabilities and exposures (CVEs), risky technologies, and outdated software to execute cybercrimes. Coalition Security Labs' research into cyber risk can provide businesses with the insights and resources they need to stay one step ahead of threat actors.

 **CVEs expected to increase in 2024**

- Coalition anticipates the number of CVEs to increase by 25% in 2024 — a projected number of nearly 35,000 new vulnerabilities
- Security teams will need to prioritize and respond to the most critical of roughly 2,900 monthly vulnerabilities

 **Honeypots are the new CVE North Star**

- Coalition research revealed honeypot (sensor) activity spiked 1,000% more than two weeks before the MOVEit security advisory was issued¹
- Honeypots monitor for spikes in activity to identify the biggest CVEs so policyholders can take action before an incident can occur

 **Threat actors focus on risky technologies**

- Scans from unique IP addresses looking for risky technologies like Remote Desktop Protocol (RDP) increased by 59% from Jan. to Oct. 2023
- Coalition claims data shows that businesses with internet-exposed RDP are more likely to experience a ransomware event

 **Threat actors target outdated software**

- Unpatched and end-of-life (EOL) versions of databases containing sensitive customer or business data are prime targets for threat actors
- Coalition scans found 10,000 businesses running the EOL database Microsoft SQL Server 2000 and over 100,000 businesses running EOL Microsoft SQL servers.

Progress Software, [MOVEit Transfer Critical Vulnerability \(May 2023\) \(CVE-2023-34362\)](#).

Help your clients prioritize digital risk

Every digital service a business offers and every new technology they employ presents a new risk. As a risk advisor, your role is to **guide your clients and help them prioritize** reducing their attack surface — and we're here to help. Coalition provides several resources to help businesses prioritize remediating vulnerabilities to protect against new and emerging threats.

5 TIPS TO STAY AHEAD OF CYBER THREATS

1. Update all critical business software to the latest version
2. Use multi-factor authentication (MFA) on all online accounts
3. Implement a process of regularly patching all software
4. Use security controls to protect services exposed to the public internet
5. Use a managed detection and response (MDR) service for 24/7 protection

Join us on our mission

Our mission at Coalition is to help protect the unprotected as the world digitizes. We share these insights to help empower brokers and businesses prioritize their security posture and make changes to reduce their overall risk.

[Download the Cyber Threat Index](#) →