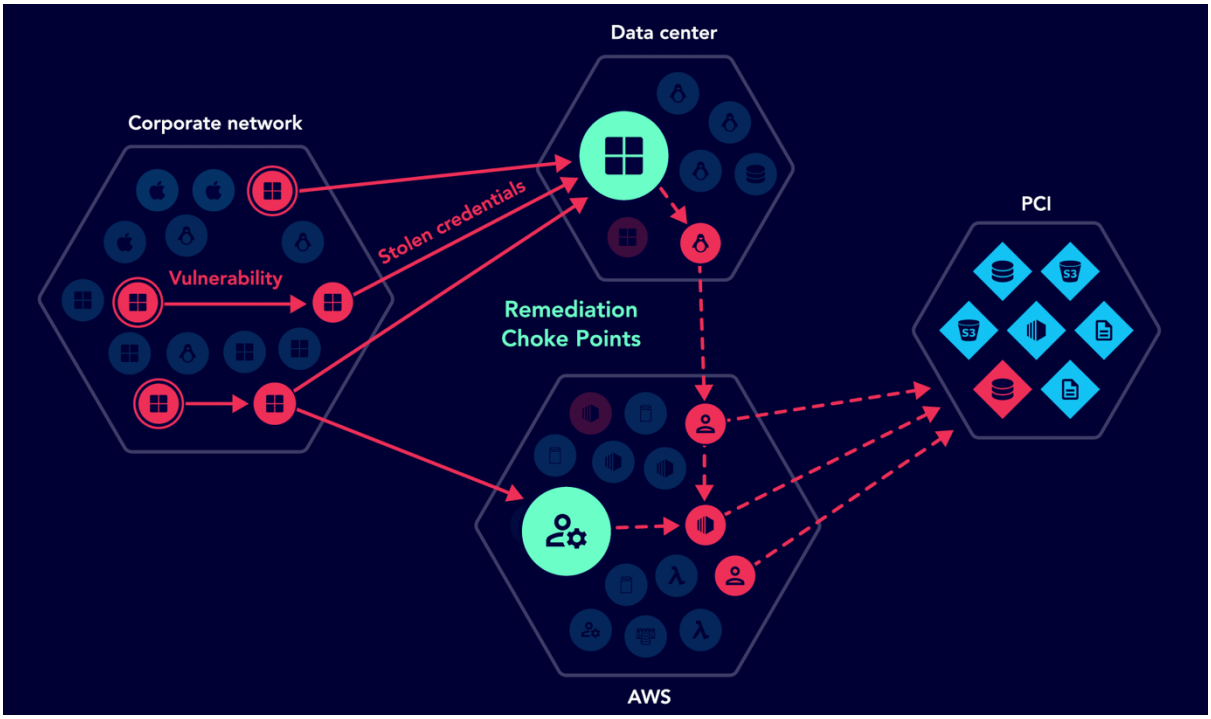
# Most Attack Paths Are Dead Ends, but 2% Lead to Critical Assets: Report

Only 2% of attack paths lead to critical assets. Securing the choke points through which they pass dramatically reduces risk.

Security posture management firm XM Cyber took tens of thousands of attack path assessments involving more than 60 million exposures affecting 20 million entities during 2022, anonymized the datasets and exported them to Cyentia Institute for analysis. The results are presented in its State of Exposure Management in 2023 report (PDF).

The primary findings of the analysis are the sheer volume of exposures (anywhere between 11,000 and 250,000 per month); the number of exposures that are dead ends that cannot be exploited by attackers (75%); and that 2% are located on choke points. A choke point is where multiple attack paths converge on the route to critical assets.



Since it is unrealistic to find and remediate all the exposures, securing the choke points should be a major and important priority. “If your organization is looking for quick wins to reduce considerable risk, these offer compelling focal points,” Zur Ulianitzky, VP of research at XM Cyber, told *SecurityWeek*. “By focusing on remediating choke points, your organization can practically eliminate all attack paths to critical assets.”

This doesn’t mean that an attacker’s presence can be ignored even on a dead-end path. “Threat actors in the environment can still do considerable damage, even if they don’t have immediate access,” warns Mike Parkin, senior technical engineer at Vulcan Cyber. “If they can gain persistence on a low value target, they have a chance down the line to escalate when a better opportunity presents itself.”

The report has more detailed findings. For example, “Techniques targeting credentials and permissions affect 82% organizations and exploit over 70% of all identified security exposures.” This has been an ongoing issue for years. “It’s also a common misconception that implementing a zero-trust architecture is sufficient to protect against all techniques that exploit forms of trust,” continues the report. “These results, however, make it clear that attackers prey upon trusted administrative services and identities.”

Parkin believes that the onus should be on vendors to distribute products with a secure-by-default configuration. “For users, even the growing use of MFA has only helped where it is deployed correctly,” he adds. “Users are still the greatest challenge in risk management.”

“We know from our own research,” adds Patrick Tiquet, VP of security and architecture at Keeper Security, “that at least a third of organizations leave it to their employees to create and manage their own passwords. In fact, our 2022 US Cybersecurity Census found 30% of the organizations we

surveyed don’t even provide guidance and best practices governing passwords and access management.”

The XM Cyber analysis also finds that, “Attackers can access 70% of critical assets in on-prem networks in just 3 steps. It’s even worse in the cloud, where 90% of critical assets are just one hop away from initial compromise.”

Furthermore, “71% of firms have exposures that enable attackers to pivot from their on-prem to cloud environment. Once there, 92% of critical assets lie just one hop away.” The implication is clear – attackers must be kept out of cloud infrastructures, but this cannot be achieved in absentia of protecting the on-prem infrastructure.

“Organizations face tough challenges in managing their diverse on-prem and cloud environments. Part of that struggle stems from failing to consider the big picture and only focusing on each piece in isolation,” adds the report.

When organizations don’t have a consolidated view of the distinct parts of their environment, it’s easy to miss common threads and otherwise obvious attack paths. “The biggest mistake organizations make when managing cloud identities is to attempt to manage them in the same way they did when everyone and everything worked on-prem,” suggests Tiquet.

However, he disagrees with the report’s downgrading of the importance of zero-trust. “The only realistic way to go about identity management in a cloud-based world is to adopt a zero-trust security model,” he says.

But the overall the statistics cannot lie. “Frankly, organizations can’t realistically remediate all exposures in their environment. Even with the existing prioritization tools the lists are still too long,” says XM Cyber’s Ulianitzky. “Unfortunately, our industry tends to over-rate everything as critical, while offering very little to help organizations determine whether a risk can be safely ignored, delayed, or

otherwise deprioritized.”

His recommendation is that all organizations take a new approach to remediation efficiency by focusing on the remediation of exposures that lie on choke points. Those are the exposures that provide attackers with a fast track to causing significant harm to the organization.

“By identifying and ignoring dead ends to reduce workload,” he told *SecurityWeek*, “organizations can free up resources to focus on choke points for remediation. Be sure to start with the choke points that indicate a large percentage of critical assets are at risk and continue from there.”

Tel Aviv, Israel-based XM Cyber was founded in 2016 by Boaz Gorodissky, Noam Erez, and Tamir Pardo. It raised a total of $49 million before being acquired by Germany’s Schwarz Group for $700 million in November 2021. The firm operates an attack simulation platform that demonstrates how attackers leverage weaknesses to compromise critical assets in cloud and on-prem environments.

**Related**: Vulnerabilities Being Exploited Faster Than Ever: Analysis

**Related**: The History and Evolution of Zero Trust

**Related**: Tackling the Challenge of Actionable Intelligence Through Context

**Related**: XM Cyber Unveils Automated Purple-Teaming at Speed and Scale

https://www.securityweek.com/most-attack-paths-are-dead-ends-but-2-lead-to-critical-assets-report/