INFO~TECH
RESEARCH GROUP

Evaluation of runZero as a Threat Exposure Management Solution

Carlos E. Rivera
Principal Advisory Director,
Info-Tech Research Group

Introduction to Continuous Threat Exposure Management

Organizations today face persistent challenges in maintaining security across expanding footprints; threats can emerge from overlooked assets or misconfigurations. Continuous threat exposure management (CTEM), offers a structured method to address these issues by continuously assessing and reducing potential attack surfaces. Originally outlined by Gartner as a five-phase cycle, CTEM emphasizes proactive identification and mitigation over reactive responses to incidents. The process begins with scoping the attack surface and moves through discovery of assets and exposures, prioritization based on severity, validation of real-world impacts, and mobilization to drive remediation actions.

At Info-Tech Research Group, we have refined this framework into a pyramid of core tenets – Visibility, Assurance, and Remediation – to provide a clearer hierarchy for implementation. This normalization aligns the phases into foundational layers, where Visibility forms the base by encompassing scoping and discovery to ensure complete awareness of all assets. Assurance builds on this by integrating prioritization and validation to confirm risks and their implications. Remediation sits at the core, focusing on actionable steps to mitigate identified threats. This pyramid approach helps organizations build upward from strong visibility to effective risk reduction, ensuring resources are allocated where they matter most.

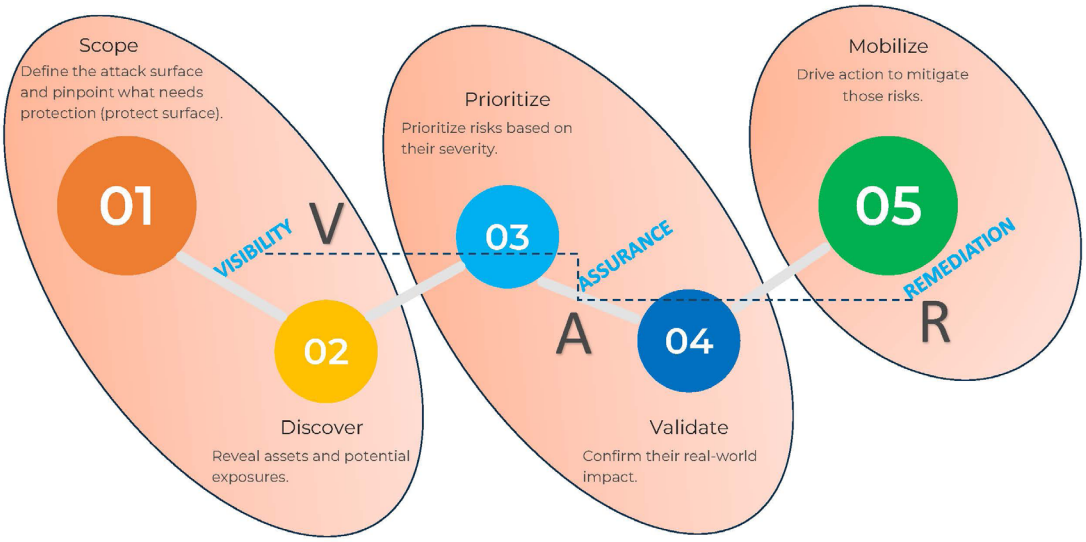
The CTEM model diagram on the next page illustrates how the five phases flow together seamlessly.

01. **Scope**: Define the attack surface and pinpoint what needs protection.
02. **Discover**: Reveal assets and potential exposures.
03. **Prioritize**: Prioritize risks based on their severity.
04. **Validate**: Confirm their real-world impact.
05. **Mobilize**: Drive action to mitigate those risks.

We used overarching labels to highlight Visibility (V) linking the first two phases, Assurance (A) connecting the middle two and providing strong support, and Remediation (R) at the end but still core to a threat exposure management program. At the end of the day, you need to take action to mitigate risks or respond to threats. This visual representation underscores the interconnected nature of the process, reminding practitioners that skipping foundational visibility can undermine later assurance and remediation efforts. By adopting this model, security teams can shift from siloed vulnerability scans to a holistic program that adapts to dynamic environments.

How the CTEM Model Works

The CTEM model flows through five phases that work together seamlessly.



Source: Info-Tech Research Group

Background and Company History

runZero traces its origins to the typical challenges encountered during penetration testing engagements circa 2016. At that time, security researchers and practitioners, including runZero founder HD Moore, noticed a persistent gap in handling unmanaged devices within organizational networks. You may be aware of Moore already, widely regarded as a cyber expert and known for creating the

Metasploit Framework. Metasploit has been a key tool in offensive security testing since the early 2000s. Moore's expertise helped tackle this issue, and his contributions benefit many penetration testers and security experts daily. These unmanaged assets often escaped traditional inventory tools, leaving blind spots that attackers could exploit. This realization led to the development of initial prototypes focused on active and passive discovery techniques to identify and catalog such devices without requiring invasive agents or privileged access.

By 2018, this effort formalized into the founding of the company, initially named Rumble Network Discovery, headquartered in Austin, Texas. The early focus was on building a platform that could provide comprehensive network visibility, drawing from Moore's extensive background in vulnerability research and exploitation frameworks. Over the next few years, the company expanded its capabilities to include vulnerability management and assessment tools, as well as integrated data from external sources to enhance asset contextualization – high fidelity, enriched data that served as actionable intelligence. In 2022, the company rebranded to runZero, a name chosen to reflect its emphasis on reducing exposure from unknown assets – essentially aiming for zero unmanaged risks through rapid discovery, a high bar. The same year, the company closed a Series A funding round that supported further product development and market expansion.

runZero has since grown to serve a diverse customer base, with strength in sectors like financial services, manufacturing, and technology. These industries often deal with large-scale physical assets, such as operational technology (OT) in factories or distributed IT in banking networks, where traditional security tools are often tested to their limits. The company's evolution reflects a commitment to solving real-world problems observed in client environments, with ongoing investments in research to stay ahead of emerging threats.

Source: runZero, Analyst Briefing Deck (May 2025)

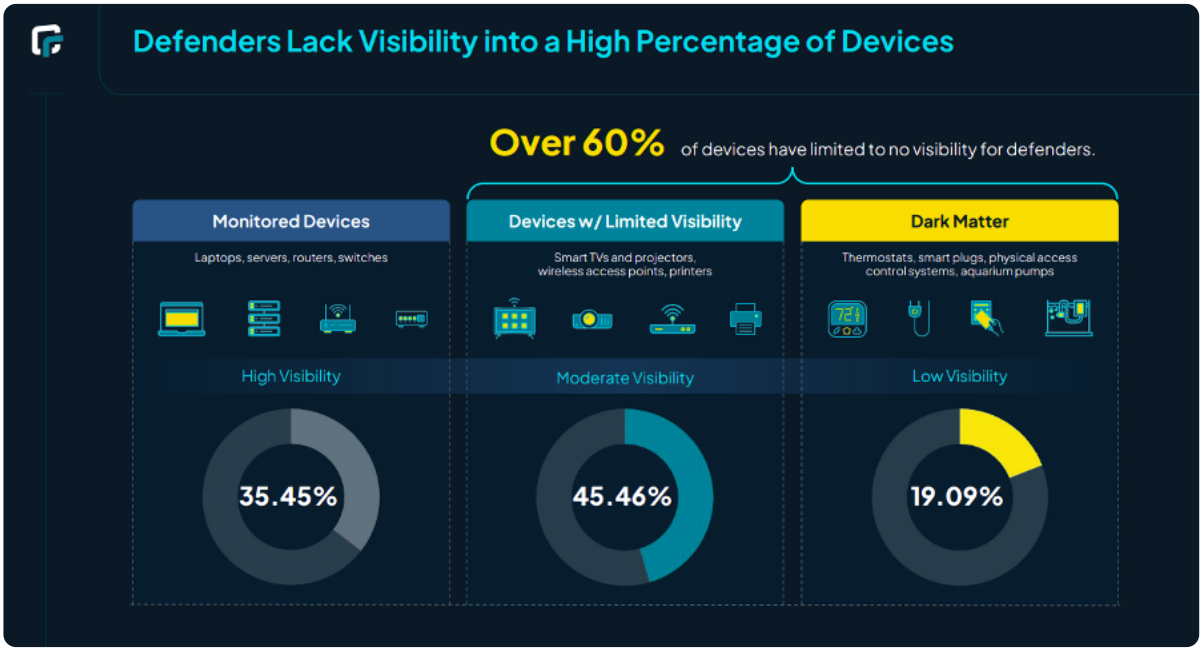
Offering and Value Proposition

runZero positions itself as a specialized provider in the threat exposure management space, delivering tools that help organizations discover, assess, and mitigate vulnerabilities across both physical and cloud-based infrastructures. At its core, the offering addresses the security category of CTEM, a framework that we see as transformational in providing a modern, structured approach to threat mitigation with an emphasis on ongoing visibility and assurance. CTEM also provides organizations with the flexibility to choose the best remediation approach to reduce attack surfaces. Unlike traditional vulnerability scanners that rely heavily on known common vulnerabilities and exposures (CVE) databases, runZero acts as an overarching platform, expanding the scope to include a much broader range of exposures such as misconfigurations, network segmentation flaws, and unmanaged assets, which often represent the bulk of exploitable risks in modern environments.

The value proposition centers on providing agentless discovery and management as well as data enrichment. Imagine you've got a variety of good but incomplete data sources for some asset information. runZero will aggregate, deduplicate, and reconcile that data, as well as perform deeper, more comprehensive discovery of its own that does not require installed software on endpoints or servers. This makes it particularly suited for environments with limited control, such as legacy

manufacturing floors, university campuses, or hybrid cloud setups where deploying agents is impractical or risky. By combining active scanning with passive monitoring and integrations from public data sources like Shodan and Censys, runZero ensures organizations gain a holistic view of their attack surfaces and assets, including those tied to domain names, IP ranges, or often overlooked autonomous system numbers (ASNs). This comprehensive scoping capability is crucial in the initial phases of CTEM, where identifying all relevant assets – internal and external, managed and unmanaged – prevents oversight of critical exposures.

In practice, runZero helps organizations move beyond reactive patching driven by CVEs. CVEs typically account for only a fraction of real-world exploits or are often significantly dated or unvalidated, leaving gaps in areas like weak configurations or improper access controls. runZero's approach counters this by focusing on broader exposure detection and prioritization, enabling faster responses to emerging threats and better resource allocation. For clients in high-stakes sectors, this translates to reduced downtime and compliance risks, as the platform supports accurate reporting and auditing without disrupting operations.



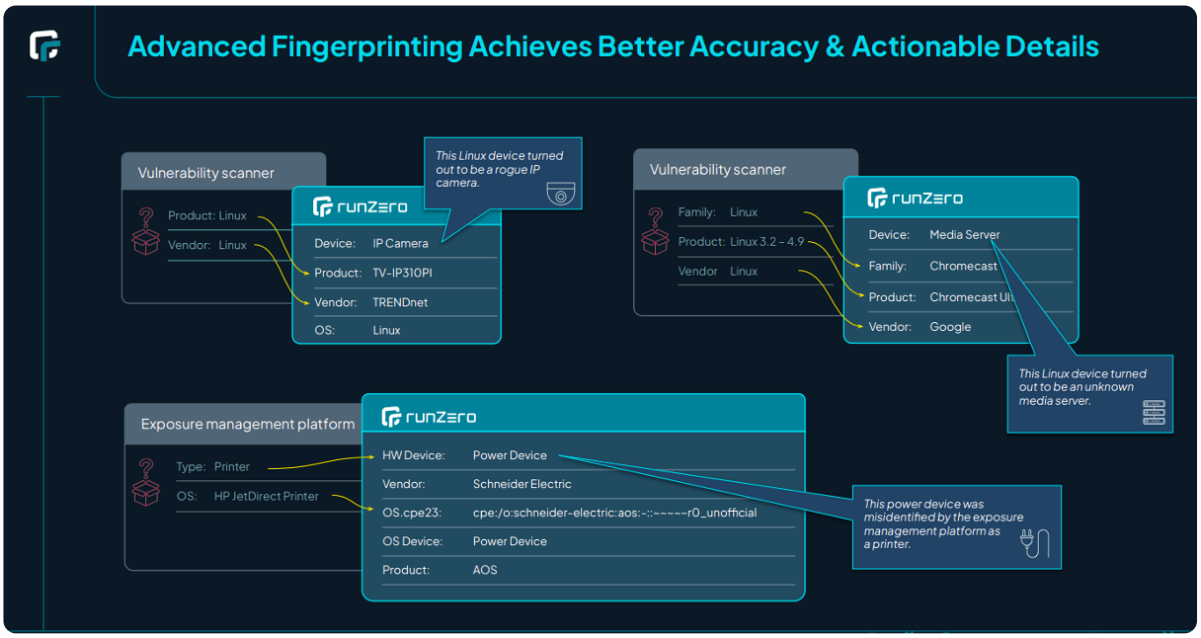
Source: runZero, Analyst Briefing Deck (May 2025)

Features and Capabilities

runZero's platform offers a robust set of features designed to deliver high-fidelity asset discovery and exposure assessment. Central to its capabilities is the use of active scanning techniques that probe networks without credentials, extracting detailed fingerprints from services like TCP ports, TLS certificates, and SSH host keys. This allows the system to identify installed software, network adapters, and even secondary IP addresses on devices, providing context that goes beyond basic inventory lists. Passive discovery complements this by monitoring network traffic to catalog assets in real-time, capturing elusive devices that might not respond to active queries – extremely clever, and effective!

Integration with external intelligence sources enhances these core functions. For instance, runZero correlates internal fingerprints with data from Shodan and similar repositories, matching exposed devices by unique identifiers like TLS hashes or cryptographic keys. This correlation ensures organizations can pinpoint if an internal asset is visible externally, flagging potential risks immediately. The platform also ingests data from API connections to tools like Microsoft Intune or cloud providers, unifying visibility across IT, OT, IoT, mobile, and cloud environments.

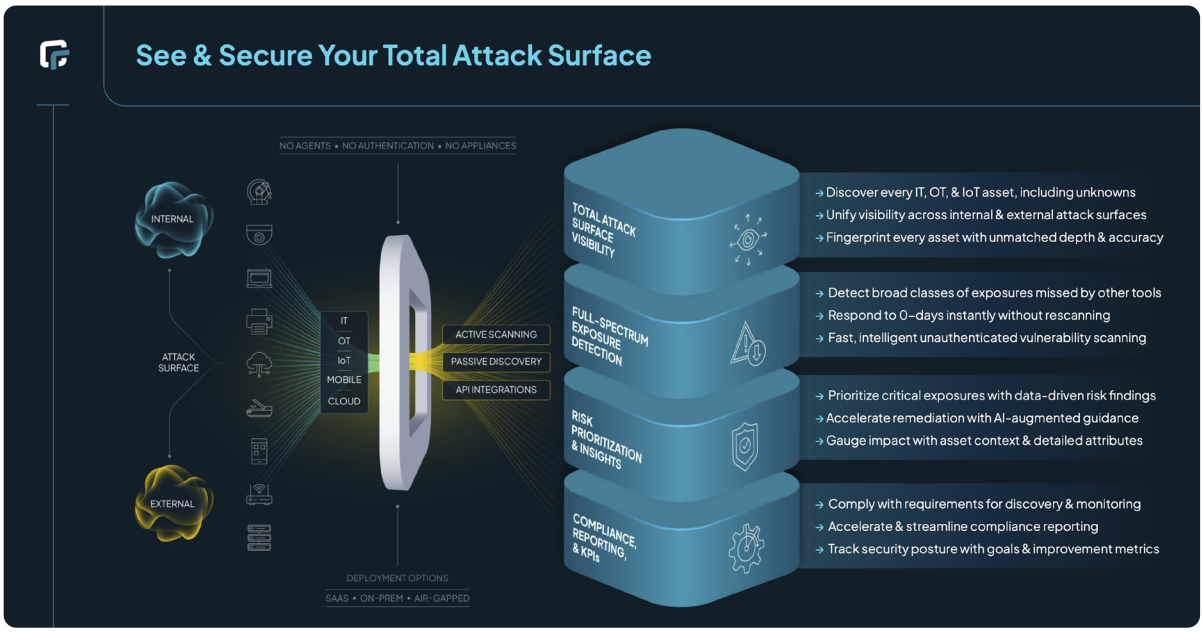
Moore highlights that prioritization of exposures is handled with a focus on precision and speed. Rather than waiting for CVE assignments, runZero validates vulnerabilities through direct network interactions, categorizing them based on factors such as connectivity, user access, and endpoint protection status. This results in notifications within minutes of threat detection, allowing for proactive mitigation. The system emphasizes the importance of accurate data for effective prioritization, timely responses, efficient resource use, compliance, and overall security posture improvement. Inaccurate data can lead to wasted efforts on false positives, but runZero's methods minimize this through rigorous validation.



Source: runZero, Analyst Briefing Deck (May 2025)

Deployment is straightforward and adaptable, with options for SaaS hosting in multiple regions or on-premises installation via a single binary. This binary runs on various operating systems, including older versions of Windows, Linux, macOS, and FreeBSD. Regardless of whether a SaaS or on-premises installation is chosen, runZero uses lightweight, simple-to-install Explorers within a customer's network to perform active and passive scans and report data back to a central console. Large enterprises typically deploy 20 to 30 Explorers across segmented networks, while smaller setups might use just a single Explorer. The lightweight design ensures it does not strain resources, even on popular consumer-grade devices like the Raspberry Pi.

Licensing follows an asset-based model, charging based on the total number of discovered assets across all deployments rather than per instance or deployment type. This provides flexibility for distributed environments without additional costs. A free Community Edition supports up to 100 assets, ideal for trials or small-scale use, allowing organizations to evaluate the platform before committing.



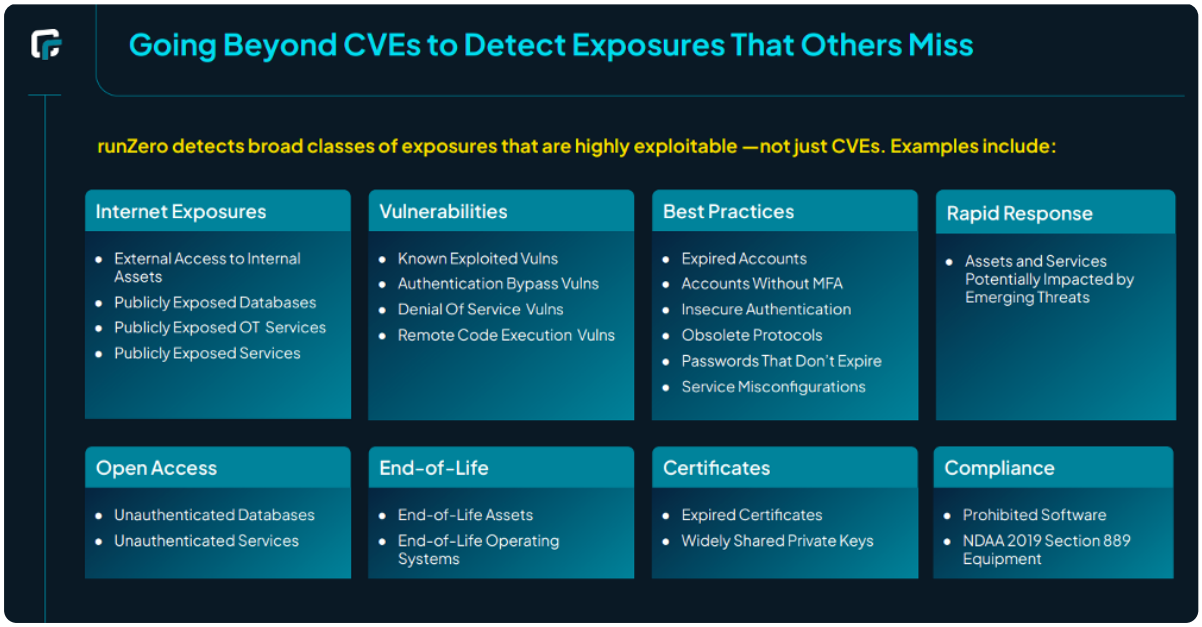
Source: runZero, Analyst Briefing Deck (May 2025)

Differentiating Features and Roadmap

What sets runZero apart is its agentless architecture combined with high-accuracy discovery, achieved through advanced protocol analysis and unauthenticated scanning. For example, by analyzing responses from ports like 135/TCP (endpoint mapper), the platform uncovers deep insights into device configurations that agent-based tools might miss due to deployment barriers. This is especially valuable in OT- or IoT-heavy environments where agents could introduce risks or compatibility issues.

Another key differentiator is the full-spectrum exposure detection, which extends beyond vulnerabilities to include issues like segmentation failures, misconfigurations, and external exposures. runZero's advanced fingerprinting and active scanning engine can identify unique asset signatures from internal scans and compare those with external data to identify and match like assets, helping trace ownership (a core requirement in several cyber programs) and uncover unintentionally exposed devices to mitigate risks swiftly. Unlike CVE-centric tools, runZero's rapid validation reduces the typical two-to-three-week lag in response times, addressing edge-facing threats before exploitation.

On the roadmap front, runZero continues to evolve with regular updates focused on enhancing visibility, exposure management, and integration. Recent releases have improved passive discovery, added support for new API integrations, and refined exposure prioritization algorithms. Looking ahead, the company plans to deepen OT and cloud coverage, incorporate more AI-driven analytics for threat prediction and intelligence, and introduce new advanced remediation workflows to accelerate mobilization efforts. These developments align with emerging CTEM trends, ensuring the platform remains adaptable to new attack vectors. runZero has proven to be attentive to community feedback. Much of that feedback drives features like enhanced reporting and custom widgets, which reflect user needs.



Source: runZero, Analyst Briefing Deck (May 2025)

Our Take

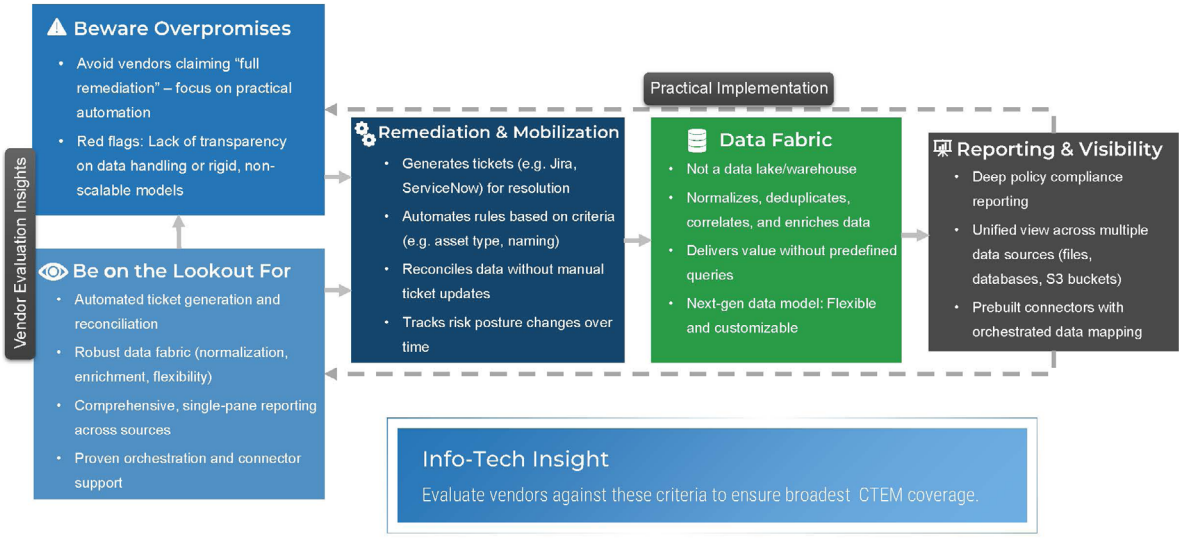
In reviewing the analyst briefing and demo of runZero, it becomes clear that the platform effectively bridges gaps in traditional vulnerability management by emphasizing comprehensive asset visibility and rapid exposure detection and prioritization. The agentless approach, coupled with integrations from diverse data sources, provides a practical solution for organizations grappling with hybrid

environments, delivering actionable insights without the overhead of extensive, time-consuming deployments. This aligns well with the demands I hear in weekly advisory calls, where clients worldwide seek tools that enhance CTEM scoping while minimizing disruption.

Overall, runZero stands out as a reliable, innovative option for threat exposure management, particularly for sectors with complex environments, physical assets, or segmentation challenges. Its focus on accuracy and speed supports stronger security postures, and the flexible licensing encourages broad adoption. As cybersecurity landscapes shift toward proactive risk handling, platforms like this offer tangible value in reducing blind spots and enabling timely mitigations.

Implementing CTEM

Practical Steps & Vendor Evaluation



Source: Info-Tech Research Group

Want to Know More?

[Build a Cloud Security Strategy | Info-Tech Research Group]

[Secure Your Hybrid Workforce | Info-Tech Research Group]

[Identify the Components of Your Cloud Security Architecture | Info-Tech Research Group]

[Attack Surface Management Software | SoftwareReviews]

[runZero: Total Attack Surface & Exposure Management]