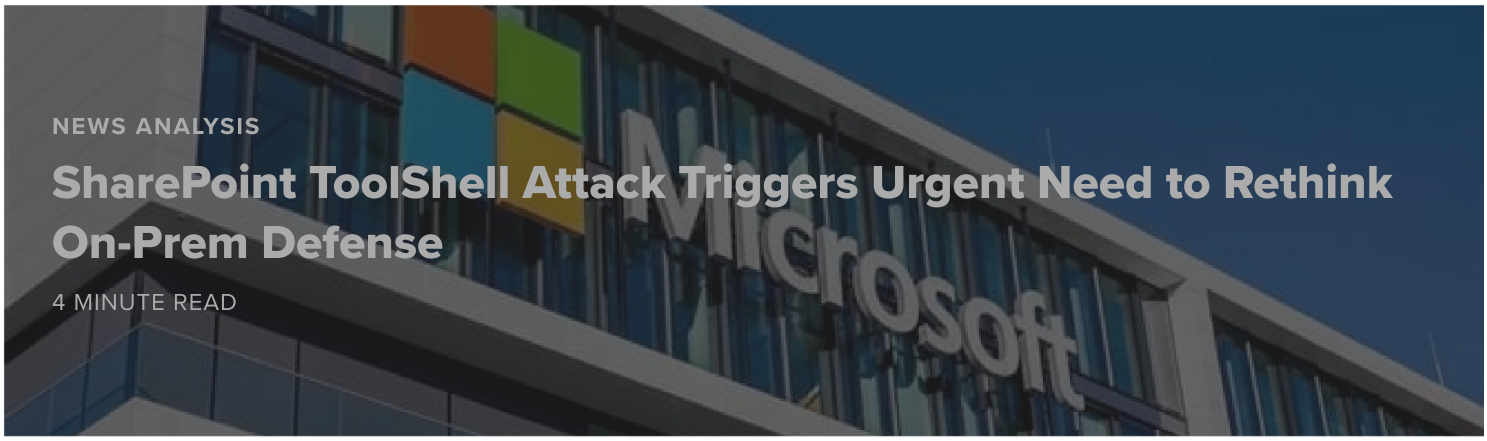

JULY 25, 2025 | INFORMATION MANAGEMENT

By David Barry

Once the immediate risks of the ToolShell attack are contained, businesses with on-prem SharePoint servers face some big questions.

The early July cyberattacks exploiting the zero-day ToolShell vulnerability revealed significant weaknesses in on-premises SharePoint servers. Exploiting this flaw allowed attackers to execute arbitrary code, take full control of systems and exfiltrate sensitive data — all without authentication.

The attacks affected customers around the globe, including U.S. government agencies like the Department of Homeland Security, the Department of Energy and the National Nuclear Security Administration. The attacks appear to have escalated due to an incomplete patch Microsoft released for 2020 vulnerabilities.

SharePoint Online, by contrast, remained unaffected.

Businesses with on-premises SharePoint deployments should take immediate action if they haven't already.

"Microsoft's own threat-hunt guidance is blunt: if spinstall0.aspx is present, assume full compromise," said Richard Harbridge, Microsoft MVP at ShareGate by Workleap. He urged organizations to take immediate action if they haven't already, taking servers offline, rotating service credentials and

machine keys, rebuilding machines with signs of tampering, scanning for persistence tools like ToolShell and applying all security patches.

"These systems should be updated immediately if they contain any sensitive information or are not isolated," said Ron Reiter, co-founder and CTO at Sentra.

Once the immediate threat is contained, organizations with on-premises SharePoint servers will face other, more strategic questions.

The Risks of On-Premises SharePoint

The diverse security controls and network designs that characterize on-premises SharePoint typically prioritize business continuity over strict security, which opens businesses up to risk.

"On-premises services almost certainly have separate security and access controls and network segmentation. Often, permissions may be liberally configured to have minimal business impact — and therefore on-prem may represent a higher risk from insider activities," said Reiter. This configuration, he added, can unintentionally lead to data over-exposure or leaks.

In some cases, limiting external access can offer advantages. "On-prem companies that limit external access to their SharePoint resources would be unaffected," noted Atlantic.Net CEO Marty Puranik.

However, the need for strong control over data remains a critical selling point for on-premises deployments.

"With digital information becoming increasingly crucial to protect, companies worldwide are looking to have control over their data. Having critical systems on-prem is the only way to reliably do this," said Adam Maurer, COO at Connecting Software. Businesses must take steps such as implementing zero-trust architectures, data loss prevention and air-gapped networks to safeguard sensitive environments.

Does This Mean It's Time to Migrate to the Cloud?

The breach raises questions around migrating from on-premises SharePoint to cloud environments. Cloud platforms offer specific functionality that contributes to a more resilient security posture, specifically, "real-time threat detection, automated logging, and continuous patch cycles that outpace adversaries," said Harbridge.

Hybrid and multi-cloud strategies serve varied business needs, often preventing rapid cloud-only shifts. "There has been and will continue to be a migration to cloud due to its compelling advantages of agility, scalability and lower operational costs," said Reiter, but he recognizes the ongoing relevance of on-premises systems due to legacy workloads and compliance demands.

On-premises solutions address security, compliance, access or usability requirements, which often prevent their wholesale replacement. “There may be some nudging by large cloud vendors to move to their cloud products because they are more profitable," cautioned Puranik. But the needs on-premises solutions address aren't going away, he continued. This suggests a gradual transition to the cloud would be preferable over abrupt changes.

How to Limit Risk in On-Premises SharePoint

SharePoint’s integration with identity services such as Active Directory magnifies the potential damage of compromises. Once attackers gain control of a SharePoint server, escalation and lateral movement across enterprise domains become possible.

"Compromised machine keys let attackers impersonate any user and exfiltrate sensitive files at scale … even if you patch tomorrow, every document the attacker touched today is already outside your control,” Reiter said. Such exposures may cause compliance violations under GDPR, HIPAA, SOX and other regulations.

Prevention of lateral movement depends on layered security controls. Maurer urges adoption of zero-trust architectures and data loss prevention mechanisms to safeguard critical environments.

Owning the full risk profile in on-premises deployments demands vigilance, said Sergio Tenreiro de Magalhaes, chief learning officer at Champlain College Online. “Running systems locally means owning the full risk profile end to end,” he continued. This translates to consistent patching, authentication management and monitoring.

Defense improvements in on-premises SharePoint involve both technology and process. “Continuous data discovery and classification, real-time threat detection, automated workflows and attacker resilience scoring” are some of the ways Reiter recommended to strengthen security.

Isolation and limited access are also crucial, Puranik said. “Isolate and limit access to people who need access to SharePoint resources (and really all resources); for remote access add VPNs to limit external threats.” XiiD CTO Federico Simonetti agreed: “If access to those servers had been limited to pre-authorized internal processes through controlled tunnels, the attack surface could have been effectively eliminated.”

However businesses with strict access controls could have limited the exploit’s reach, environments that permit external sharing would have challenges enforcing such restrictions.

Multiple controls working together reduce risk significantly, Maurer said. "A comprehensive security posture incorporating zero-trust models, intrusion detection, and data diodes for air-gapped networks is essential,” he said.

Lessons for Enterprise Software Security

The breach serves as a stark reminder of the need for risk-based security planning. Relying on assumptions or perceptions can leave dangerous gaps in defense. Sound risk assessment and mitigation planning must form the foundation of any security strategy, warned de Magalhaes, cautioning against trust in perception alone.

In today's hybrid cloud and data-sharing environments, proactive security hygiene is indispensable. Reiter urged organizations to act decisively, whether they were affected or not. "It is time to take proactive steps to ensure your data security posture and hygiene (no matter where your data resides) and institute continuous threat and suspect activity monitoring," he said. Traditional perimeter-based defenses are no longer enough.

Strengthening the security posture means reducing breach likelihood by enforcing strict access boundaries. However, technical debt continues to accelerate exposure to modern threats. As attackers become more agile and sophisticated, the risk compounds.

"Threat actors today are faster, smarter and chained exploits like ToolShell prove just how quickly technical debt can become an open door," warned dope.security founder and CEO Kunal Agarwal.

Ultimately, data-centric security must remain at the core. Clyde Williamson of Protegrity summed it up succinctly: "If someone gets in, they should walk away with nothing. SharePoint houses the crown jewels: contracts, records, IP. A patch buys time, not safety."

Editor's Note: Read more about security questions below:

About the Author

David is a European-based journalist of 35 years who has spent the last 15 following the development of workplace technologies, from the early days of document management, enterprise content management and content services. Now, with the development of new remote and hybrid work models, he covers the evolution of technologies that enable collaboration, communications and work and has recently spent a great deal of time exploring the far reaches of AI, generative AI and General AI.

Our mission is to advance the careers of top workplace practitioners and forward thinking leadership via high impact knowledge, networking and recognition (awards).

Today the Reworked community consists of over 2 million influential employee experience, digital workplace and talent development professionals, the majority of whom are based in North America and employed by medium to large organizations. Our sister community, CMSWire gathers the world's leading customer experience, voice of the customer, digital experience and customer service professionals. And our newest community, VKTR, is home for artificial intelligence professionals focused on the business of enterprise AI.

JOIN THE COMMUNITY

Email address

JOIN US

GET THE REWORKED MOBILE APP

Download on the App Store

GET IT ON Google Play