



Zscaler Collaborates with IBM and Red Hat to Protect Private Applications from Frontier AI-Powered Threats

October 5, 2026

New collaboration combines Zscaler Autonomous Application Shield with Lightwell from IBM and Red Hat to help organizations reduce exposure between vulnerability disclosure and patch deployment through inline protection and validated remediation

SAN JOSE, Calif., Oct. 05, 2026 (GLOBE NEWSWIRE) -- [Zscaler, Inc.](#) (NASDAQ: ZS), the cybersecurity platform for the AI era, today announced a collaboration with IBM and Red Hat to help organizations protect private applications during the period between vulnerability disclosure and patch deployment. The collaboration combines [Zscaler Autonomous Application Shield](#), delivered through the Zscaler Zero Trust Exchange™ security platform, with [Lightwell](#) from IBM and Red Hat to deliver adaptive, application-specific protection with validated software remediation in a single coordinated response.

The economics of exploitation have shifted. Capabilities that once required elite skills and weeks of manual effort are now widely available, and attackers are weaponizing newly disclosed vulnerabilities faster than enterprise patch cycles can respond. According to Mandiant's M-Trends 2026 report, the mean time to exploit a vulnerability has fallen below zero, meaning vulnerabilities are increasingly exploited before a public patch exists. Patching remains necessary, but on its own it can no longer keep pace. Organizations need protection that can be applied at machine speed while remediation is prepared and deployed.

This collaboration extends Zscaler's [protection-first operating model for private applications](#), which assumes a remediation window will always exist and builds resilience around it: hide applications with [Zscaler Private Access™ \(ZPA™\)](#) so they are harder to discover and target, segment access with [Autonomous User-to-App Segmentation](#) so a foothold does not become broad reachability, and shield reachable applications with [Autonomous Application Shield](#) so exploit attempts are stopped inline while the root cause is fixed. By uniting Zscaler Autonomous App Shield with Lightwell, the collaboration provides customers a coordinated path from immediate protection to durable fix.

Operating through the Zero Trust Exchange, Zscaler App Connectors continuously perform safe assessments of each private application's exposure points and vulnerabilities. The Zscaler cloud individually evaluates each application, ensuring only necessary protections are applied. When a new vulnerability emerges, adaptive protections can be applied inline and in real time, without waiting for a patch. Through this collaboration, Lightwell helps Zscaler defend its customers from potential cyber threats, with Zscaler blocking exploit attempts immediately at the network level. Lightwell then provides validated remediations for affected open source software, enabling customers to fix the underlying flaw at the source.

"As attackers weaponize newly disclosed vulnerabilities faster than enterprises can respond, organizations need a way to protect private applications immediately while fixes are being prepared and deployed," said Joby Menon, Senior Vice President of Product Management at Zscaler. "Our collaboration with IBM and Red Hat brings together inline, application-specific protection and validated remediation to help customers reduce risk during that gap."

Through this collaboration, Zscaler, IBM, and Red Hat will deliver integrated capabilities across the application security lifecycle, addressing critical needs including:

- **Exposure Discovery:** Providing a current understanding of a private application's actual risk profile, updated as fast as applications change, rather than relying on periodic scans.
- **Preemptive, Application-Specific Protection:** Bridging the gap between vulnerability and patching. Applying only the protections a given application needs during the gap between disclosure and patching, reducing exposure while remediation is underway and avoiding one-size-fits-all policy noise.
- **Machine-Speed Response:** Deploying protections inline and in real time when a new vulnerability emerges, informed by global threat intelligence from across Zscaler's worldwide customer base.
- **Validated Source-Level Remediation:** Delivering tested software fixes through Lightwell so organizations can resolve the underlying vulnerability, with advisory and deployment support to prioritize and validate protections across complex environments.

"AI is shrinking the window between vulnerability discovery and vulnerability exploitation. A window that was months or weeks is now hours and minutes," said Gunnar Hellekson, vice president and general manager, Lightwell, Red Hat. "Lightwell helps keep open source safe by patching and fixing these vulnerabilities at machine speed. Collaborating with partners like Zscaler brings Lightwell's capabilities to the forefront of enterprise networks, mitigating potential vulnerabilities head-on while patches are applied to critical systems."

Autonomous Application Shield is currently available through an Early Access Program. Availability, capabilities, and timing of the collaboration described herein are subject to change.

For a deeper dive into how Zscaler is helping protect against AI threats, please visit [this blog](#).

Forward-Looking Statements

This press release contains forward-looking statements that are based on our management's beliefs and assumptions and on information currently available to our management. These forward-looking statements include the expected performance and benefits of Zscaler Autonomous Application

Shield and its collaboration with IBM and Red Hat, including the delivery of adaptive, machine-speed protection for private applications. These forward-looking statements are subject to the safe harbor provisions created by the Private Securities Litigation Reform Act of 1995. A significant number of factors could cause actual results to differ materially from statements made in this press release, including those factors related to Zscaler's ability to achieve partner and customer adoption of Autonomous Application Shield and the collaboration described herein. Additional risks and uncertainties are set forth in our most recent Annual Report on Form 10-K filed with the Securities and Exchange Commission ("SEC") on September 3, 2026, which is available on our website at ir.zscaler.com and on the SEC's website at www.sec.gov. Any forward-looking statements in this release are based on the limited information currently available to Zscaler as of the date hereof, which is subject to change, and Zscaler will not necessarily update the information, even if new information becomes available in the future.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across 200+ public data centers globally and thousands of private sites at the edge, the SASE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Media Contacts

Nick Gonzalez, Director of Public Relations, press@zscaler.com