Zscaler™ and ServiceNow:
Protect More, Work Smarter
The risk to your SaaS data is rising

Although SaaS services, such as ServiceNow, are popular because of their ubiquity, scalability, and ease of use, the accelerated migration to the cloud and the adoption of SaaS applications mean enterprises are facing increased security threats to their most precious asset—data.

As data leaves your data center for cloud apps, it becomes increasingly distributed and more at risk, especially as users access it directly over the internet. Because it’s impossible to train every employee to always apply security best practices with SaaS applications, your company faces the risk of accidental data exposure, configuration mistakes, and compliance violations. As these incidents rise in numbers, IT security teams have difficulty keeping up with triage, resulting in slower response times and increasingly complex workflows.

Zscaler + ServiceNow: better data protection and threat workflows

Protect data with Zscaler CASB and DLP

The Zscaler platform offers a range of data protection services that provide immediate visibility into sensitive data residing in your ServiceNow data stores. By scanning new and existing ServiceNow data, Zscaler helps you easily identify sensitive data based on DLP policies. You’ll get a clear picture of data exposure and risky access violations, so you can accelerate compliance and protection efforts. In addition, any outbound upload of sensitive data files will be blocked in real time by Zscaler DLP policies.

Remove the risk of BYOD and unmanaged devices with zero trust

Through Zscaler Zero Trust Exchange integrations with ServiceNow, you can prevent unauthorized BYOD access to your sensitive ServiceNow data. By leveraging Zscaler as your identity proxy, devices can only connect to ServiceNow through Zscaler. By adding Zscaler Cloud Browser Isolation to the equation, you can safely deliver data to authorized devices in the form of pixels only.

Improve security workflows

Accelerate workflows by adding Zscaler Cloud Sandbox threat intelligence to ServiceNow security incidents. Stop emerging threats faster by enforcing inline blocking within Zscaler directly from ServiceNow. Also, with Zscaler Cloud Security Posture Management (CSPM), you can scan your public clouds for dangerous misconfigurations. RemEDIATE incidents instantly or create alert tickets in ServiceNow as artifacts for streamlined workflows.

Benefits

With Zscaler and ServiceNow integrations, you can:

- Improve data protection and compliance within ServiceNow
- Scan and discover sensitive data and malicious content across your deployment
- Block direct access into ServiceNow by BYOD and securely enable B2B access to data
- Respond quickly to threats with ServiceNow Security Incidents & Response workflows
- Enrich incident context and speed triage by adding Zscaler threat intelligence to ServiceNow incidents
- Enforce Zscaler blocking directly with more intelligence from ServiceNow Security Incident Response
- Prevent cloud breaches quicker by logging discovered misconfigurations from Zscaler CSPM directly into ServiceNow as tickets
How integrations protect your data

Secure ServiceNow data inline and out-of-band
By leveraging Zscaler CASB out-of-band capabilities, ServiceNow customers can quickly scan the attachments in their platform and understand where sensitive files reside, if the files are benign or malicious, who is accessing them, and what data violations need to be fixed to restore security and compliance. The Zscaler inline DLP capabilities can also inspect the uploading of files and attachments and block sensitive data from leaking in real time.

Control BYOD access to ServiceNow with Zscaler
When an unmanaged or BYOD device attempts to access a ServiceNow cloud instance, it is redirected to Zscaler, via the Zscaler Identity Proxy. As a result, users and devices can only access ServiceNow through the Zscaler Zero Trust Exchange, so that all traffic is inspected and access to sensitive data is controlled by Zscaler security policies. Alternatively, devices that remain unmanaged, and are therefore risky, are prevented from accessing the ServiceNow instance directly or indirectly. As an option, additional protections can be enabled using Zscaler Cloud Browser Isolation to stream data to devices in the form of screen pixels, enabling access while preventing downloading, cutting, pasting, or printing.
**Improve ServiceNow SecOps workflows with Zscaler**

By leveraging Zscaler threat intelligence, Cloud Sandbox reports, and cloud misconfiguration information to enrich incident tickets, you can respond more quickly via automated workflows. By retrieving additional context automatically from Zscaler, ServiceNow Security Incident Response can orchestrate response actions, including updating Zscaler’s tenant-specific Custom Block List. Risky IPs, domains, and URLs can be blocked without manual intervention, while cloud misconfigurations can be closed to help reduce the risk of a breach. These automated workflows reduce response time by minimizing manual triage tasks, increasing the IT team’s speed and productivity.

**Use cases**

With Zscaler and ServiceNow integrations, you can:

- **Restore data protection and compliance**: improve data visibility and prevent exfiltration by scanning the Now Platform for sensitive data and violations. Quickly understand how data is being used and who is accessing it.
- **Securely enable WFA**: prevent BYOD and other risky, unmanaged devices from accessing both the Now Platform and sensitive data to enable a more secure work-from-anywhere experience.
- **Streamline incident response**: respond quicker to emerging threats by adding Zscaler threat intelligence to incident response workflows within the ServiceNow Security Operations platform. Get better fidelity across emerging incidents and easily orchestrate blocking directly from ServiceNow back into Zscaler.

Visit the Zscaler website to learn more about ServiceNow integrations →

**About Zscaler**

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world’s largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.