Prevoty

Solution Brief

Security for Microsoft SharePoint Applications

SharePoint and Prevoty: Enabling Secure Collaboration

The Microsoft SharePoint platform has seen an increased adoption for both Intranet and web applications. Prevoty Runtime Application Security provides visibility into attacks and protects against data leakage and exfiltration.

Both legacy and modern enterprise applications are rife with vulnerability backlogs. Security and development are at odds as business imperatives to quickly push applications to production overpower the risks. Furthermore, as SharePoint applications migrate to the cloud, physical server security is lost. Applications must protect themselves. Prevoty Runtime Security protects from within the application itself, providing the last line of defense irrespective of deployment.

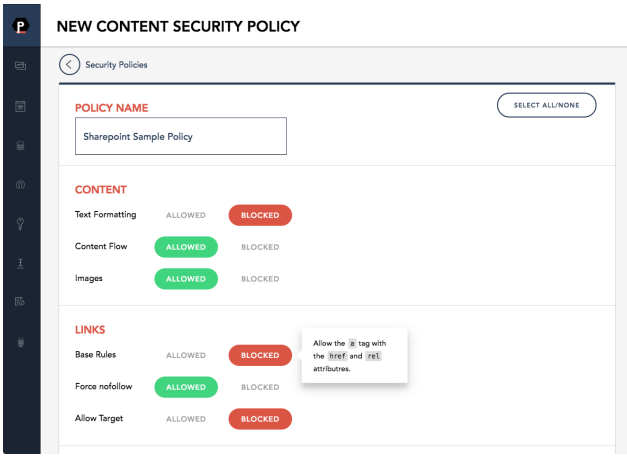
Top 6 SharePoint Use Cases	
1 - Reduce vulnerability backlog	Scanning and testing of SharePoint applications results in increased vulnerability backlogs that slow down production.
2. Protect sensitive data	Increased access and collaboration leads to the risk of data leakage.
3 - Visibility into attacks in production	Implementing runtime security in monitoring mode allows for full visibility into real-time attacks (as opposed to theoretical or potential vulnerabilities).
4 - Push applications into production faster	Release applications more quickly without worrying about security vulnerabilities.
5 - Protect legacy applications	Legacy apps often drive critical revenue, but can be written in older languages and do not have active development or support.
6 - Optimize the DevSecOps Lifecycle	Runtime security Plug-ins and SDKs can be an effective part of proactively training developers, reducing vulnerabilities introduced during coding.

Common SharePoint Attack Vectors

- **SQL Injections (SQLi) to compromise sensitive data tied to SharePoint -** attacker manipulates an application to submit a malicious SQL command and expose the back-end database.
- **Cross-site scripting (XSS) against websites hosted by SharePoint -** attacker injects client-side scripts into web pages viewed by other users, bypassing access controls such as the same-origin policy. Hackers often use fuzzing/obfuscation to bypass perimeter protections.
- **Cross-site request forgery (CSRF) behind the scenes to orchestrate unwanted actions -** allows a malicious website, email, blog, instant message, or program to run, causing a user's Web browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

Prevoty Offers Seamless Protection for SharePoint Applications

Prevoty's runtime solution seamlessly integrates with SharePoint when installed on Internet Information Services (IIS) and prevents against SQLi, XSS, and CSRF zero-day attacks. Through Prevoty, all incoming data is instantly examined and threats are automatically neutralized, safeguarding applications. Users can create individual security policies to enhance SharePoint operations, allowing or disallowing content parameters that generate html tags. This ability to create and customize specific policies enables organizations to optimize Prevoty for use with SharePoint as well as other third-party software.



Zero-touch Prevoty

Prevoty is self-contained for .NET Environments.
No application changes required.

Learn More

Further details on the installation and deployment of Prevoty Runtime Application Security solutions for Microsoft SharePoint are available by demo. Please email info@prevoty.com.