**Microsoft Defender for Cloud Apps**

Microsoft's investment in a new approach to SaaS app protection is powered by security professionals’ need for extra protection within the SaaS App landscape. With an uptick in app usage and the breadth of applications being used combined with employees accessing company resources outside of corporate perimeters, protection is needed no matter where apps are hosted. Microsoft's unique approach helps security professionals easily start no matter where apps are accessed. With Microsoft Defender for Cloud Apps, organizations can gain visibility into dormant apps and having visibility into dormant apps is critical to their strategy to effectively protect against app-based threats. These new sets of capabilities, combined with fundamental app protection, encompass the entire app management lifecycle through a set of simple steps and guided to action. App-to-app Protection

**Sensitive data exposure**

Microsoft Defender for Cloud Apps connects to SaaS apps to scan for files protected no matter where it is being accessed. Defender for Cloud Apps integration with Microsoft Purview enables information protection: remediate risky third-party integrations, discover and remediate sensitive data exposure.

**Continuous threat detection and response**

Microsoft 365 Defender: The XDR technology correlates signals across endpoints, identities, email, and third-party integrations. Integrating Microsoft 365 Defender: Integrating Microsoft 365 Defender with Microsoft XDR Defense and signal integration with Microsoft XDR

**Best practices management (SSPM)**

SaaS Security Posture Management (SSPM) is a lightweight proxy for the health of your SaaS apps. With Microsoft’s SaaS security protection, you gain control of shadow IT by providing easy ways to identify, assess, and manage cloud apps beyond the traditional scope of security.

**Microsoft Defender for Cloud Apps**

Check out our tech community blog. Explore Protect your SaaS apps with Microsoft Defender for Cloud Apps... and more

**Microsoft © 2023**

Visit our Microsoft 365 Defender

Detect, investigate and respond to attacks with Microsoft 365 Defender:

- Detect
- Investigate
- Remediate
- Manage

**Sensitive data exposure**

55% of IT and security professionals report that the top three risks to their environment are cloud misconfigurations, cloud misconfigurations are a top risk in security. Cloud misconfigurations are a top risk in security. 59% of security professionals find the SaaS sprawl challenging to manage. The SaaS sprawl is a top risk in security. 55% of IT and security professionals report that the top three risks to their environment are cloud misconfigurations, cloud misconfigurations are a top risk in security. 59% of security professionals find the SaaS sprawl challenging to manage. The SaaS sprawl is a top risk in security. 55% of IT and security professionals report that the top three risks to their environment are cloud misconfigurations, cloud misconfigurations are a top risk in security. 59% of security professionals find the SaaS sprawl challenging to manage. The SaaS sprawl is a top risk in security.