Anti-malware policy

Abstract

SalesTim is not storing nor uploading any document to your Microsoft 365 environment. SalesTim was designed with this requirement in mind. We're not accessing, storing nor processing any document from or to your environment, therefore antimalware requirement doesn't really apply to us.

The only files we're storing (as a volatile cache) is the templates pictures, the one you see in each template from your template catalog. These images are generated from the team logo, and stored in Azure Blob Storage.

How are we protecting these files?

Our entire Azure environment is protected by Azure Defender, and as part of Azure Defender, we're monitoring all our Storage Accounts. These storage account resources are monitored by the Azure Defender for Storage service.

> Azure Defender for Storage provides: - Azure-native security - With 1-click enablement, Defender for Storage protects data stored in Azure Blob, Azure Files, and Data Lakes. As an Azure-native service, Defender for Storage provides centralized security across all data assets managed by Azure and is integrated with other Azure security services such as Azure Sentinel. - Rich detection suite - Powered by Microsoft Threat Intelligence, the detections in Defender for Storage cover the top storage threats such as anonymous access, compromised credentials, social engineering, privilege abuse, and malicious content. - Response at scale - Security Center's automation tools make it easier to prevent and respond to identified threats. Learn more in Automate responses to Security Center triggers.
>
> What kind of alerts does Azure Defender for Storage provide? Security alerts are triggered when there's: - Suspicious access patterns - such as successful access from a Tor exit node or from an IP considered suspicious by Microsoft Threat Intelligence - Suspicious activities - such as anomalous data extraction or unusual change of access permissions - Upload of malicious content - such as potential malware files (based on hash reputation analysis) or hosting of phishing content

Learn more about Azure Defender for Storage.

Integration with our SIEM

As this anti-malware protection is managed by Azure Defender, it is natively connected to our Azure Sentinel SIEM, which aggregates all the logs and alerts from our entire platform.