ARCTIC WOLF

BRIEF

A Cybersecurity Checklist for Monitoring SaaS Applications

Software-as-a-service (SaaS) applications enable businesses to reach unseen levels of productivity, but they bring significant cybersecurity challenges.

Today's digital perimeters grant authorized users anytime/anywhere access to sensitive business data. Because of this, SaaS-heavy IT environments introduce a higher complexity to threat detection and response efforts. User activity on SaaS accounts can be quite varied, occurring on multiple endpoints and from a variety of locations. Businesses must distinguish between legitimate and potentially illicit user activity on busy networks. What's more, the onus isn't on the SaaS provider to secure user data should an account compromise occur. In light of these and other challenges, SaaS applications require continuous, carefully calibrated monitoring.

Continuous Monitoring for SaaS Applications

Most SaaS applications generate large volumes of event data from user, administrator, and application back-end activities. These activity logs need to be monitored around the clock for potential indicators of compromise.

The following checklist identifies some of the core security-related SaaS activities that must be continuously monitored and associates them to the types of incidents that may be detected.

✓ User and Administrator Access

To detect credential theft and user and administrator account compromises, companies must monitor:

- Login successes and failures
- Logins by time and location
- Logins by device type and attributes
- Repeated login failures followed by login success
- SSO activity, AD activity

✓ Administrator Behavior

Once cybercriminals obtain administrator credentials, they can cause vast damage to an organization in terms of data loss, primarily from hackers carrying out data exfiltration or data destruction activities. Security experts, therefore, must monitor:

- Repeated user and/or data deletions
- Addition of privileged users
- Changes to network permissions
- Changes to audit logging configuration
- Changes to policy controls

✓ User Behavior

Organizations also need to keep a sharp eye on user activities as well to detect malicious insiders, data exfiltration attempts, use of unapproved shadow IT applications, and more. They must monitor:

- User file activity (download, delete, print, copy, move)
- Sharing files with external collaborators
- Creating open/shared links (public access)
- Unauthorized/untrusted mobile device activity
- Network traffic activity

✓ Third-Party API Access

Application program interfaces (APIs) enable third-party software to interact with SaaS apps, but are often abused and used in "Man-in-the-Middle" (MITM) attacks. To detect such abuse, cybersecurity personnel must monitor:

- Changes to API access permissions
- OAuth certificate activity
- OAuth token activity

Secure Your Organization with Arctic Wolf's Cloud-Based AWN CyberSOC™ Service

Arctic Wolf provides organizations using SaaS applications with a predictably-priced, comprehensive and fully-staffed security operations center (SOC)-as-a-service, the AWN CyberSOC. We aggregate log data from on-premises and cloud-based resources in real time, giving our security analysts 24/7 centralized visibility into activity across all of your attack surfaces. Arctic Wolf's Concierge Security™ team detects and responds to potential security incidents such as unauthorized access, data loss, and API abuse to help ensure your SaaS applications remain safe and secure.

Detecting bad actors in today's complex, hybrid IT environments isn't easy. But with 24/7 security monitoring and incident response, Arctic Wolf helps effectively defend your organization against increasingly sophisticated cyberthreats targeting your critical SaaS applications and on-premises IT resources.

ARCTIC WOLF

AICPA SOC

SOC2 Type II Certified

Contact us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com