Syncfusion prioritizes the security of your data and analytics. We implement encryption in transit and at rest, access controls, and authentication mechanisms to ensure data confidentiality. Secure coding practices, regular vulnerability assessments, and penetration testing strengthen our system’s security. Our robust monitoring tools, incident response plans, and compliance with standards like SOC 2® Type 2 help us maintain a high level of security. Below is a summary of our security practices followed across our products, Bold BI, BoldSign, BoldDesk, Bold Reports, and Essential Studio.
# Table of Contents

Security Management Report ................................................................. 1

Application Security: ........................................................................... 1
  Hosted-Scan security Tool................................................................. 1
  OWASP (Open Web Application Security Project): ........................... 1
  Burp Suite: ........................................................................................ 1
  Dependabot from GitHub: ................................................................. 1
  Soos.io for Dependency Scanning: .................................................... 1
  Security Scorecard (Third-party application): .................................... 2

Infrastructure Security ........................................................................... 2
  Microsoft 365 Defender..................................................................... 2
  Defender for Cloud ............................................................................ 2
  CrowdStrike ....................................................................................... 2
  Wazuh ............................................................................................... 2
  Nebula by Slack.................................................................................. 2
  Open VAS ......................................................................................... 2

Endpoint Security ................................................................................... 3
  Office 365 Defender for Endpoint.................................................... 3
  SonicWall ......................................................................................... 3

Dependency Management ...................................................................... 3
  Dependabot ....................................................................................... 3
  Soos.io ............................................................................................. 3

Email Security ....................................................................................... 3
  Office 365 phishing protection ........................................................ 3
  Safe attachments .............................................................................. 3
  Safe links .......................................................................................... 3
  Malware protection ......................................................................... 4

Identity Protection and Risk Management ............................................ 4

Security Awareness and Training ........................................................ 5
  365 attack simulation ...................................................................... 5
Security Management Report

Application Security:

Hosted-Scan security Tool:
- This tool is used to scan our web applications for known vulnerabilities and security weaknesses. It helps identify potential risks and vulnerabilities that could be exploited by malicious actors.
- The hosted scan security tool ensures that our applications are regularly checked for security issues and provides an added layer of protection against emerging threats.
- We are also checking open ports using the Nmap plugin.

OWASP (Open Web Application Security Project):
- OWASP is a widely recognized and respected community that provides guidelines, tools, and resources for improving web application security.
- Following OWASP guidelines ensures that applications are developed and maintained with best practices for security in mind, reducing the risk of common security vulnerabilities.

Burp Suite:
- Burp Suite is a popular web vulnerability scanner and testing tool used for manual and automated security testing of web applications.
- Burp Suite helps identify security vulnerabilities such as SQL injection, cross-site scripting (XSS), and other potential risks in the web applications.

Dependabot from GitHub:
- Dependabot is a tool that helps keep your project's dependencies up to date by automatically creating pull requests to update outdated dependencies.
- Keeping dependencies updated is crucial for maintaining the security and stability of applications, as vulnerabilities in outdated dependencies can be exploited by attackers.

Soos.io for Dependency Scanning:
- Soos.io is a tool used for identifying and managing security vulnerabilities in software's open-source dependencies.
- Soos.io helps users assess the security of third-party libraries and components, enabling us to remediate potential risks and vulnerabilities effectively.
Security Scorecard (Third-party application):

- Security-Scorecard provides an outside-in view of our security posture so we can take preventative action. Scoring is based on our trusted, transparent ratings methodology and data collected on millions of organizations.

**Infrastructure Security**

Our multi-layered infrastructure security approach includes the following.

**Microsoft 365 Defender**

A comprehensive security solution that gives us advanced threat protection across our digital ecosystem, safeguarding against a wide range of cyber threats.

**Defender for Cloud**

Extending our cloud security, this tool continuously monitors and protects our cloud-based resources and data.

**CrowdStrike**

A cloud-native endpoint security platform that provides us with threat intelligence, next-generation antivirus (NGAV), and endpoint detection and response (EDR) capabilities.

**Wazuh**

We use the Wazuh open-source security monitoring platform to detect, analyze, and respond to security incidents in real time both in the cloud and on premises.

**Nebula by Slack**

This tool enhances our infrastructure security by providing secure, seamless access to our systems for distributed and remote teams.

**OpenVAS**

The OpenVAS network vulnerability scanner scans our server for 50,000+ vulnerabilities (part of hosted scan).
Endpoint Security

Endpoint security remains a top priority.

Office 365 Defender for Endpoint

This solution offers advanced threat protection for endpoints, helping to safeguard against a variety of sophisticated attacks.

SonicWall

This on-premises security solution provides firewall protection and intrusion prevention, safeguarding the integrity of our internal network.

Dependency Management

Our approach to dependency management includes the following.

Dependabot

Automating the maintenance of secure and stable projects, Dependabot mitigates the risk of vulnerabilities associated with outdated dependencies.

Soos.io

Ensuring the security of open-source dependencies, Soos.io identifies and rectifies potential vulnerabilities in third-party libraries.

Email Security

Office 365 enhances our email security with the following features.

Office 365 phishing protection

Utilizing advanced threat intelligence and machine learning, this protection identifies and prevents suspicious emails from reaching users’ inboxes.

Safe attachments

This feature analyzes attachments in a virtualized environment to detect potential malware and malicious content before delivering them to users.

Safe links

URLs in emails are scanned in real time to ensure their safety before redirecting users to the intended destination.
Malware protection

Real-time scanning and heuristic analysis prevent the infiltration of malware through incoming emails and files.

Identity Protection and Risk Management

Office 365 Identity Protection and Risk Management offer robust tools and strategies to safeguard user identities and mitigate security risks within the Office 365 environment. This suite of features enhances overall security posture by focusing on user authentication, access control, and threat detection.

Identity Protection:

- Multi factor authentication (MFA): Users are required to provide multiple forms of authentication, bolstering login security.
- Conditional access: Enables administrators to define access policies based on user roles, locations, and device states, ensuring access control tailored to risk levels.
- Sign in risk policies: Leverages machine learning to assess sign-in risk and prompt additional verification steps for suspicious activities.

Threat Detection and Management:

- Identity threat detection: Monitors user activities and uses machine learning to detect anomalous behavior that could indicate compromised accounts.
- Suspicious activity reports: Provides insights into potentially harmful activities, empowering administrators to investigate and take action.
- Risk events dashboard: Offers a centralized view of risk events and insights into risk levels across the organization.

Risk-Based Conditional Access:

- Adaptive access policies: Dynamically adjusts access policies based on risk factors like location, device, or user behavior.
- Real time decision making: Assesses user risk before granting access, ensuring secure interactions based on up-to-date risk assessments.

Insider Risk Management:

- Insider risk policies: Identifies and mitigates internal security risks by monitoring user activities, data interactions, and communication patterns.
- Policy violation alerts: Alerts administrators to potential policy violations, facilitating timely intervention to prevent data breaches.
Security Awareness and Training

We foster employee awareness and knowledge.

365 attack simulation

This tool facilitates security awareness training by simulating real-world attacks, empowering our staff with valuable insights.