

EXPOSING YOUR IT ASSETS TO RISK CAN ENDANGER YOUR ENTERPRISE REPUTATION

SummitAI Asset Controller
ensures robust endpoint
security and compliance
for your IT assets



Asset utilization, securing data & enforcing compliance – all integrated into one

As organizations worldwide continue to depend on applications for their everyday operations, data is increasingly forming the core of business processes. Multitudes of information get accessed and stored on numerous web-based and cloud-based applications, exposing organizations to various security breaches and threats. According to **Risk-based Security**, data breaches exposed 4.1 billion records in the first half of 2019 alone.¹

These recent trends are increasingly making organizations vulnerable to data breaches, which lead to business loss. While the ways of accessing and protecting data continue to evolve, monitoring and controlling data security threats while operating efficiently and productively remains a challenge.

Companies are becoming aware of cybersecurity and making prevention and security best practices a part of their culture. However, only whitelisting and blacklisting doesn't help eliminate the risks posed by malicious, illegal, and unauthorized software and network access. You need a next-generation solution, powered by AI, to put new controls and processes to manage hardware and software assets effectively. An integrated solution that helps you manage assets, control applications, and provide endpoint compliance.



Leverage SummitAI Asset Controller to reduce risk and ensure compliance

SummitAI Asset Controller is a comprehensive and proactive compliance solution consisting of 3 components, namely: **Application Control**, **Endpoint Compliance**, and **Dynamic Local Admin Password Management Solution**. Together, these components help improve your endpoint security posture.



Application Control - It's a security practice that blocks or restricts unauthorized applications from executing in ways that put data at risk. It ensures the privacy and security of data used and transmitted between various applications.



Endpoint Compliance sub-system - It's a plug-in that can be used to monitor the security compliance of the computing devices in an organization's network, based on the security policies configured. The Endpoint Compliance covers over 170 out-of-the-box security compliance monitoring capabilities. Moreover, the security administrator can create additional security compliance parameter checks. These customized parameters can be configured based on registry entries, the value of WMI class, VB scripts, PowerShell, Batch Command, and so on.





Dynamic Local Admin Password Management - The local administrator account is one of the most vulnerable areas for security breaches.

Therefore, controlling it becomes a crucial business activity. SummitAI Asset Controller provides an effective way to manage the local administrator accounts. It creates a unique password for every local administrator account across the organization. These passwords are managed centrally in the Password Vault and are available on request by selected IT administrators through which the transactions are controlled and tracked.



Application Control

Rule-based software entitlement mapping

Reduces the risk of running malware

Effective privilege management

Reduces inventory loss



Endpoint Compliance

Proactive and real-time endpoint compliance engine

Supports 170+ out-of-the-box security parameters

Allows configuring of dynamic controls for monitoring



Dynamic Local Admin Password Management

Secures shared and Service account passwords

Controls duration of password life dynamically

Tracks users who have requested super-user passwords



Organizations have come across challenges of not being able to control their assets and protect confidential data. With 'work from home' becoming a norm post COVID-19, organizations are at a higher risk of data breaches and data loss.

With SummitAI Asset Controller, you can ensure optimized asset utilization while enforcing compliance and save costs. You can also prevent malware and zero-day attacks, block unauthorized applications, protect networks from intrusion, alleviate chances of system damage or data loss – all as an extension of SummitAI Asset Management Suite.

To know more or request a quick demo,
write to us at summit.sales@symphonysummit.com



Summit Software Inc.,
4 Main St Suite 100, Los Altos,
CA 94022, USA

Call: (866) 209-2066 (Toll Free)
Email: summit@symphonysummit.com
Visit: www.symphonysummit.com