ABB Ability™ Cyber Security Application Allowlisting
Fortify your industrial control system
Advanced threats make it increasingly difficult to protect your industrial control system.

Advanced threats need advanced cyber security solutions to protect your systems without compromising reliability. Outsmart cybercriminals and keep your organization secure and productive.
ABB Ability™ Cyber Security Application Allowlisting
A trust-centric approach

ABB Ability™ Cyber Security Application Allowlisting brings a trust-centric approach to cyber security, safeguarding your processes from never-before-seen attacks.

This solution is valuable to a wide range of organization types, whether you are looking to take the next step in your cyber journey, have long production cycles, or have a planned upgrade with a classic DCS system.

How it works: Application Allowlisting is a proactive solution that works by only allowing users to take actions on a device that a system administrator has explicitly allowed in advance. Instead of staying one step ahead of cyber threats to identify and block malware, security personnel compile a list of approved applications called an allowlist that users have access to.

What threats does allowlisting protect against?
Application allowlisting is most effective against advanced malware. Stopping zero-day threats, unknown malware, or otherwise unauthorized software from executing. Allowlisting can also act as a “shadow OT” tool to protect against end-users who may try to install insecure and unlicensed software.

Did you know?
"X-Force observed a 49% year-over-year increase in ICS vulnerabilities in 2020" - IBM

Adversaries are evolving faster than endpoint protection. Traditional protection from cyber attacks is based on malware detection that checks applications against databases of known malware before it is executed. In the ABB Ability™ Cyber Security product, this basic layer of threat protection is represented by ABB Ability Cyber Security Malware Protection. While antimalware software does a great job of blocking known cyber threats, it’s practically impossible to keep up-to-date on all new threats that are unknown and have yet to be discovered.
Advantages
Maintain cyber resiliency without compromising on your digital transformation

In-depth Threat Protection
Application Allowlisting protects against zero-day and advanced malware attacks by blocking the execution of unknown applications preventing them from opening up and spreading within an environment.

Protection against yourself
Often employees attempt to install unverified or unsigned applications to their workstation creating security vulnerabilities. Application Allowlisting will block those unverified applications from being installed by the operator and notify the appropriate security personnel about the attempt.

Long-production Cycle Protection
Delaying security patches is a considerable risk to production facilities as they are known exploits that attackers are searching for. Application Allowlisting will limit the risk of exposure for the duration of the patch implementation delay.

Optimized Management
Ensure production uptime and maximum security with less resources through ABB expertise.

Protect Legacy Systems
Need to protect older System 800xA running Windows 7 without Microsoft offered security support? ABB has you covered. Application Allowlisting will protect your legacy systems while you prepare for your next upgrade.

Incident Response Insights
Security personnel responding to an incident can identify the characteristics of malicious files on the host and use the Application Allowlisting solution to compare that file to the files on other systems to see what other hosts are compromised.

How Application Allowlisting could have lessened the impact

Major Energy Utility Company

- Ransomware attack Shut down power and operations
- 6,000 Computers and 1,200 servers affected
- Estimated cost $45 Million

Threat Vector: Ransomware via 3rd party software

Application Allowlisting: Prevents unauthorized applications from running which would block the malicious software and prevent the attack.
Features

Streamlined Security
Centrally manage application related files. Pinpoint vulnerabilities and validate internal and external compliance.

Joint Solution Management
ABB cyber experts joint manage your allowlist, ensuring only necessary applications are running to promote production uptime.

System Intelligence Reports
Monthly improvement reports identifying threats averted and solution improvement suggestions.

Vendor Validated Allowlist
A vendor validated allowlist built for each machine in your control system environment.
Flexible deployment in 4 simple steps

1. Design the solution
   An ABB Cyber Engineer will work with your security personnel to:
   • Identify current and future needs for the Application Allowlisting Solution
   • Specify requirements for performance, functionality, and security
   • Define relevant systems and architect the deployment

2. Implement and test
   The next phase involves implementing and testing a prototype of the designed solution.

3. Deploy and tune
   Once testing is completed, the Application Allowlisting solution will be deployed across your industrial control system and tuned to match the performance, functionality, and security requirements defined in step 1.

4. Manage the solution
   After the solution is deployed, ABB Cyber Engineers will support you throughout the lifecycle of the solution. This includes:
   • Support in modifications to allowlist
   • Quarterly performance reports and review
   • Software training, updates, and support
Why ABB
ABB delivers superior technology and proven domain expertise

---

**People**

ABB pioneered the development of electrical and automation technologies and has years of experience helping customers protect control systems and other automation assets.

**Process**

ABB’s control systems are present globally across many industries. We know the type of cyber threats our customers face and what needs to be done to mitigate risks. We stay ahead of threats by investing heavily in research and development to continuously improve our security offerings.

**Technology**

ABB can support our customers throughout the lifecycle of their assets through our products, services and expert operations by making technology relevant to customers in industrial sector.