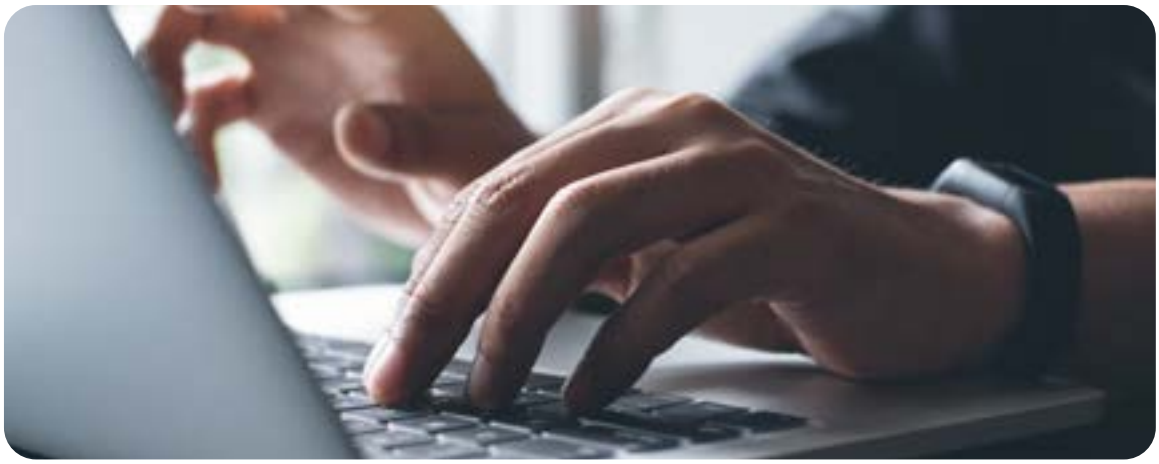
PROMON

How to secure your desktop applications

2022 • www.promon.co

PROMON

Content



Executive summary

This guide is intended for organizations interested in learning more about how Promon SHIELD™ can protect desktop applications. It will help you understand:

- ✓ Remote working security threats
- ✓ How Promon SHIELD™ protects your applications
- ✓ How Promon SHIELD™ works

Technology overview

Promon SHIELD™ for desktop can be integrated with applications that commonly handle sensitive information. Through blocking unwanted interactions with applications initiated by possible malware residing on the system, a secure process (a secure execution environment for the application) is created.

- ✓ Protection against both known and unknown threats
- ✓ End-to-end security control for service providers
- ✓ Transparent countermeasures for the end-user

Self-defending applications become crucial as modern architectures migrate software logic to the client side

Gartner

PROMON

Remote working increases cyber security risks

Malware threats

The workplace is changing fast. A study by International Workplace Group, which operates serviced offices and co-working spaces, found that 50 per cent of employees globally work away from their office at least two and a half days a week. Some analysts predict that up to half of the workforce will be freelance within 10 years, as short-term work becomes more common.

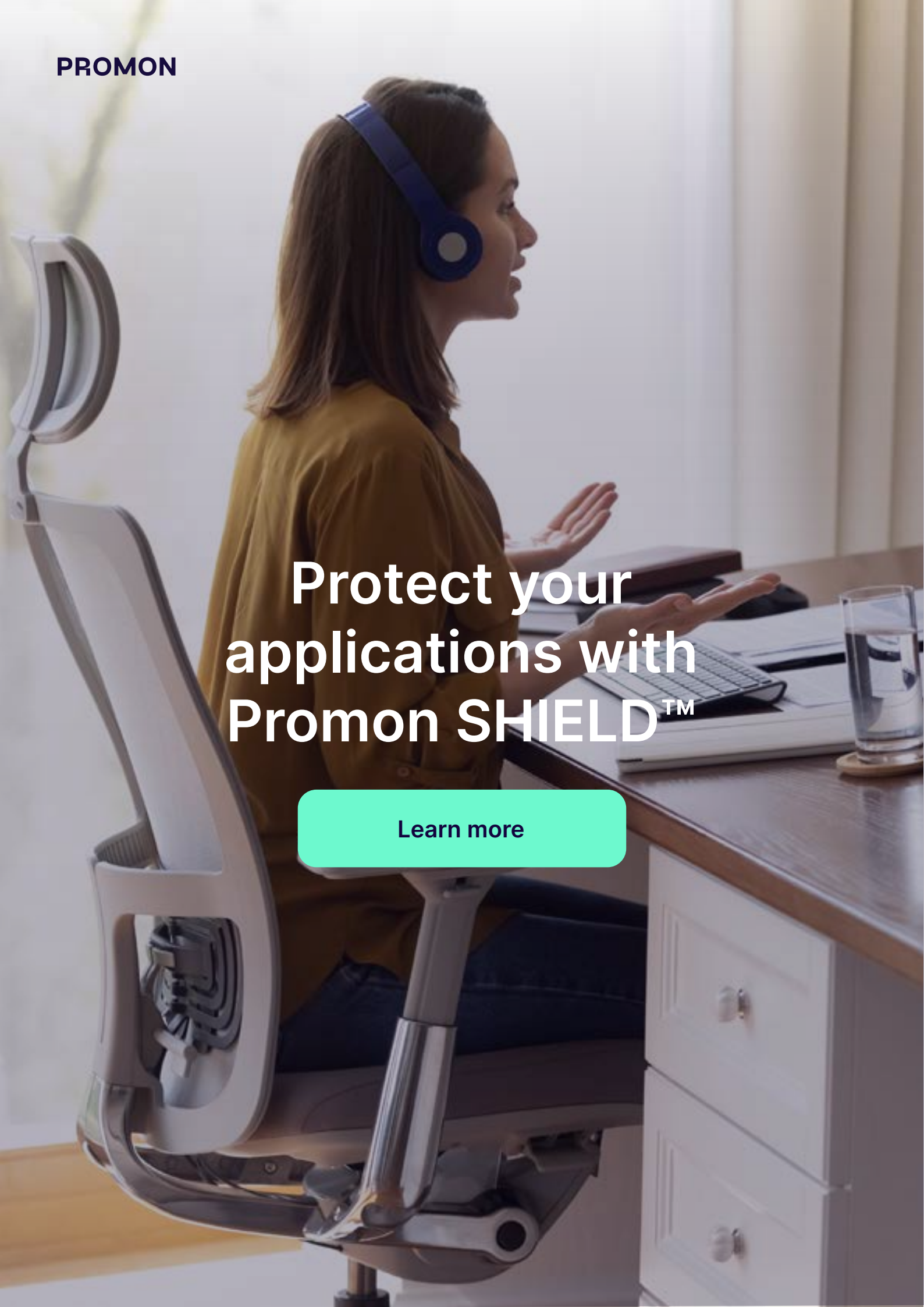
A dispersed workforce gives rise to a variety of security challenges. Employees are accessing company information remotely at home, causing issues that are not mitigated by anti-virus, authentication and encryption alone. Key security threats include app-hijacking, man-in-the-middle attacks and spyware.

App-hijacking
Malware on infected endpoints can steal, spy on or manipulate sensitive information being used or accessed from the client side.

Man-in-the-middle attacks
By controlling the application from the inside, malware can easily operate as a man-in-the-middle copying or changing data.

Spyware
On an infected endpoint, keyloggers or screenshot scrapers can harvest sensitive information.

PROMON



Protect your applications with Promon SHIELD™

Learn more

Comprehensive desktop protection

- In-process attacks
- Out-of-process attacks
- Information disclosure
- Network attacks
- Reverse engineering

In-process attacks

In-process attack mechanisms, including code injection and code execution, are used by malware to inject malicious code into a target process. Once the malware is inside the process, it can intercept, spy on or manipulate your applications.

Promon SHIELD™ offers multi-layered protection against in-process attacks. The first layer prevents malicious code from being loaded, inserted or executed in the protected process. This is performed through different mechanisms including remote thread execution blocking, remote code injection blocking, DLL validation and hook cleaning.

Out-of-process attacks

Desktop operating systems and applications include mechanisms that enable malicious code to be loaded into the process or methods used to spy on the user. Loaded malicious code can be done through manipulated files such as DLLs. Keyboard logging and screens-hot scraping can be done out-of-process using standard system APIs with normal user access rights.

Promon SHIELD™ uses special mechanisms to counter out-of-process code manipulation and snooping. DLLs can be checked against valid certificates or SHA256 hash values at run-time before being allowed to load into the process. To prevent spying, the technology artificially generates extra random keyboard input that renders logged information useless, and protects the application against screenshots.

Information disclosure

Corporate information may also require copy protection from the person using the program. Promon SHIELD™ includes options for information disclosure, such as blocking or limiting clipboard access and printing.

Network communication attacks

Network communication attacks, frequently referred to as Man-in-the-Middle (MitM) attacks, include malicious proxy servers, DNS spoofing or cache poisoning, HTTPS spoofing or SSL/TLS certificate theft.

Promon SHIELD™ has multiple layers of protection against network communication attacks, manipulation or spoofing. The extension of the s ecure and protected zone from the protected process to the endpoint server is an important part of our solution. You may configure Promon SHIELD™ to do SSL/TLS certificate pinning, but you may also configure client SSL/TLS certificates that allow Promon SHIELD™ to negotiate the sessions.

Reverse engineering

In addition to protecting the software against malware attacks, it is equally important to protect applications against hackers contemplating attacks.

Promon SHIELD™ uses several techniques to block reverse engineering attempts, including blocking any debugger from attaching to the process. Promon SHIELD™ also detects and blocks other mechanisms such as debugger breakpoints, and other techniques used to access and analyze the process at runtime.

How to use Promon SHIELD™

- ✓ Remote access
- ✓ OEM
- ✓ Windows applications
- ✓ Team collaboration
- ✓ Videoconferencing

Remote access

> Remote desktop
> Virtual desktop infrastructure

Original Equipment Manufacturer (OEM)

> Application to manage security products

Windows applications

> Banking and payment
> Government
> Healthcare
> Supervisory control and data acquisition
> Smart lock industry and hotels

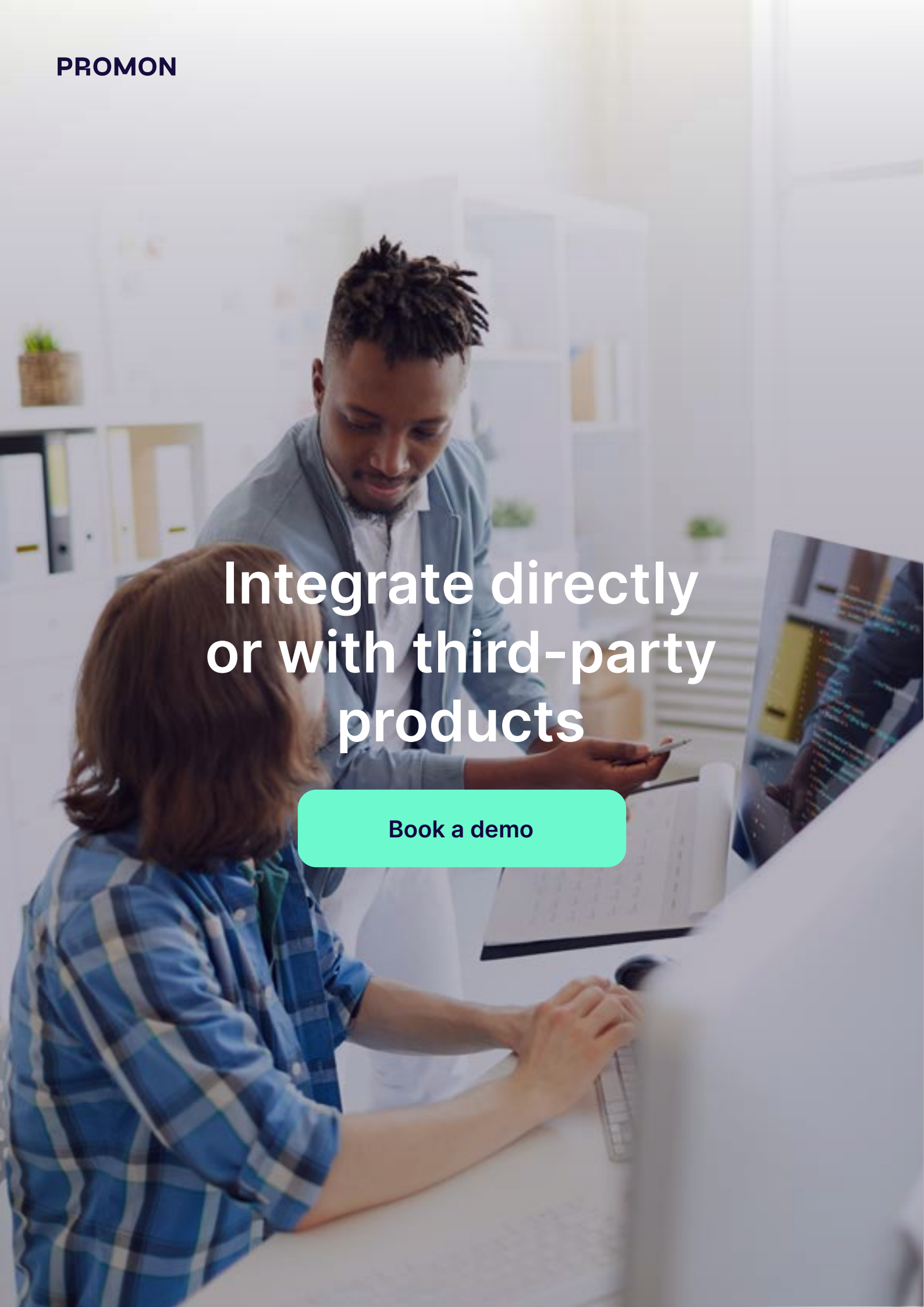
Team collaboration and videoconferencing

> Unified communication and collaboration platforms including Microsoft Teams

Windows communication agents

> Promon SHIELD™ is also designed to protect all kinds of communication agents, like VPN, and vendor specific communication clients or agents

PROMON



Integrate directly or with third-party products

Book a demo

Implementation

Promon SHIELD™ for desktop provides two different methods for launching a protected process for developers:

> SDK
> Shielder

The first allows the developer to build and manage their own Promon SHIELD™ launcher. The Shielder method is a tool that wraps the developer's main program .exe into a self-contained Promon SHIELD™ launcher.

SDK

The Promon SHIELD™ for desktop SDK offers an API to the developer. The SDK can be configured through a programmable C/C++ interface, allowing a protected application to be launched in response to commands or user events. The SDK identifies the platform, and then uses the necessary code to launch a new and protected process. If required, Promon can provide assistance with integrating the launcher code in an existing code base.

Shielder

The Shielder is an application wrapper. The output is a dedicated launcher .exe binary that contains the original application binary and the Promon SHIELD™ protection module. When the new Shielder wrapped .exe is executed, it launches the original application as a protected process.

PROMON

Why should you consider us?

Our app shielding software requires minimal security knowledge and takes care of the complexities of app security. Promon SHIELD™ dramatically accelerates your apps time-to-market and works smoothly with your dev team's favorite CI/CD tools.

- Protecting more than 500 million end-users
- Ease of use and integration
- Multi-layered protection
- Best in class app shielding
- Cross-platform availability

Book a demo >