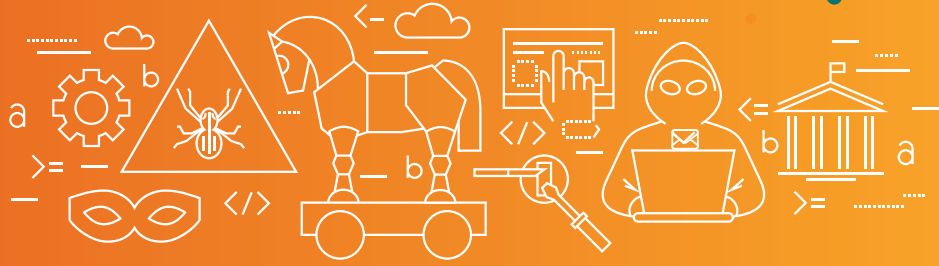


## Software Defined Access Connectors for Security Solutions



Software Defined Access enables organizations to control and secure data exchange of any type and size between people, applications, cloud solutions, and businesses. Built on the industry's widest range of pre-configured application connectors and powered by an automated security policy enforcement engine, Safe-T Software Defined Access is designed to rapidly add security and control across a wide variety of data exchange scenarios for enterprises of all types and to the cloud.

Safe-T Software Defined Access enables organizations to quickly and easily add security layers to existing business processes, thereby strengthening the control of and reducing the costs of sensitive data sharing. Safe-T's Software Defined Access unique modular architecture and integration capabilities ensure that it seamlessly integrates into existing data exchange scenarios in the enterprise and cloud, providing policy enforcement and secure data transfer.

**Safe-T Software Defined Access Security Connectors allow enterprises' IT to add security layers on top of their existing incoming and outgoing data exchange workflows, thus ensuring any data entering and leaving the organization is scanned and potential virus outbreaks are mitigated.**

Safe-T Software Defined Access offers unmatched integration between the enterprise eco-system and its security solutions, through the use of its Safe-T Connectors, allowing organizations to connect to the leading anti-virus, scrubbing, sandbox, data leak prevention, and sanitizing solutions such as McAfee, Symantec, Check Point, etc.

Safe-T Connectors offer a variety of scanning operations which can be done on data exchanged through Safe-T Software Defined Access, including the following scenarios:

- ✓ Scanning the body and attachment of incoming and outgoing emails
- ✓ Scanning files uploaded into the organization's portal
- ✓ Scanning files downloaded from the cloud
- ✓ Scanning files uploaded to the cloud

