Battle Card

Protect Against Data-Driven Threats With the Safe-T Software Defined Access and Solebit SoleGATE Joint Solution

The Challenge

Your data is the lifeblood of your organization. Unfortunately, it's continuously at risk of getting stolen or compromised. By nature, your organization has countless methods of accessing files, and they are stored in numerous locations (on premise or in the cloud). This huge proliferation of data access methods and data storage solutions include: cloud storage solutions, S/FTP servers, network file storages, data vaults, document management applications, etc.

In addition, to providing your remote employees, customers and business partners access to files and data, you most likely utilize various solutions such as: email, file distribution applications, EFSS solutions, MFT solutions, etc.

Many businesses do not effectively control or monitor their sensitive and valuable data: when accessed, used or transferred. This creates a risk that your confidential information will fall into the wrong hands. Exposure of confidential data can result in a failure to meet regulatory standards (such as HIPAA, GDPR and PCI-DSS), legal action, fines, theft of intellectual property, bad publicity, and loss of strategic customers.

Key Benefits

- ✓ Control the flow of data in and out of the enterprise
- ✓ Unify all inbound data flows redirected to Solebit SoleGATE for advanced analysis
- ✓ Seamlessly secure all inbound data flows and data access
- ✓ Proactively protect in real-time against unknown threats contained in data entering the enterprise
- ✓ Prevent unauthorized access to data, services, networks, and APIs
- ✓ Block hackers from penetrating via your partners

Joint Solution: Safe-T Software Defined Access & Solebit SoleGATE

By deploying Safe-T's Software Defined Access integrated with Solebit SoleGATE Protection Platform organizations can now seamlessly and automatically analyze any file entering the organization from any source to any destination, including cloud, remote/local employees, customers, 3rd party business partners, remote applications using an API, SFTP, etc.

The joint solution works as follows:

1. Safe-T intercepts the stream of data, regardless of its source
2. Safe-T applies a workflow and policy on the data based on its source, destination, type, etc.
3. If required, the data is then streamed to SoleGATE, which in real-time, analyzes the data and alerts of any embedded malware
4. If the data is found clean by SoleGATE, it is then streamed on to the required destination

Safe-T Software Defined Access

Safe-T's unique Software Defined Access solution is built on the foundation that "if you can't be seen, you can't be hacked". It is designed to reduce your attack surface and mitigate data threats by protecting the perimeter on several levels:

- Prevents un-authorized access to data, services, networks, or APIs
- Protects against data-related threats, including data exfiltration, leakage, malware, and ransomware

By making your data invisible to the outside world, and by controlling the data access lifecycle, Safe-T protects you from cyber-attacks through a 3-step process:

- **Step 1 - Adaptive Access to Services and Data** - Safe-T's "on-demand Software Defined Perimeter" transparently grants access only to authorized users by separating the access layer from the authentication layer, and by segregating internal networks. It authenticates the user and verifies its device using fingerprinting, prior to providing access.

- **Step 2 - Control Usage of Data -** Once users have access to your applications and data, Safe-T ensures they only use the data according to their respective usage and access policies. The data residing inside your organization or being transferred in and out of the organization is completely controlled and protected from the inside out of the network – on premise or in the cloud.

- **Step 3 - Report on Data Usage -** Throughout the application access lifecycle, Safe-T monitors and audits all user actions for each access application or data repository. Granular real-time dashboards, historical reports and analysis on data usage and risks, ensures compliance to regulations and shortest time to breach discovery and remediation.

Solebit SoleGATE

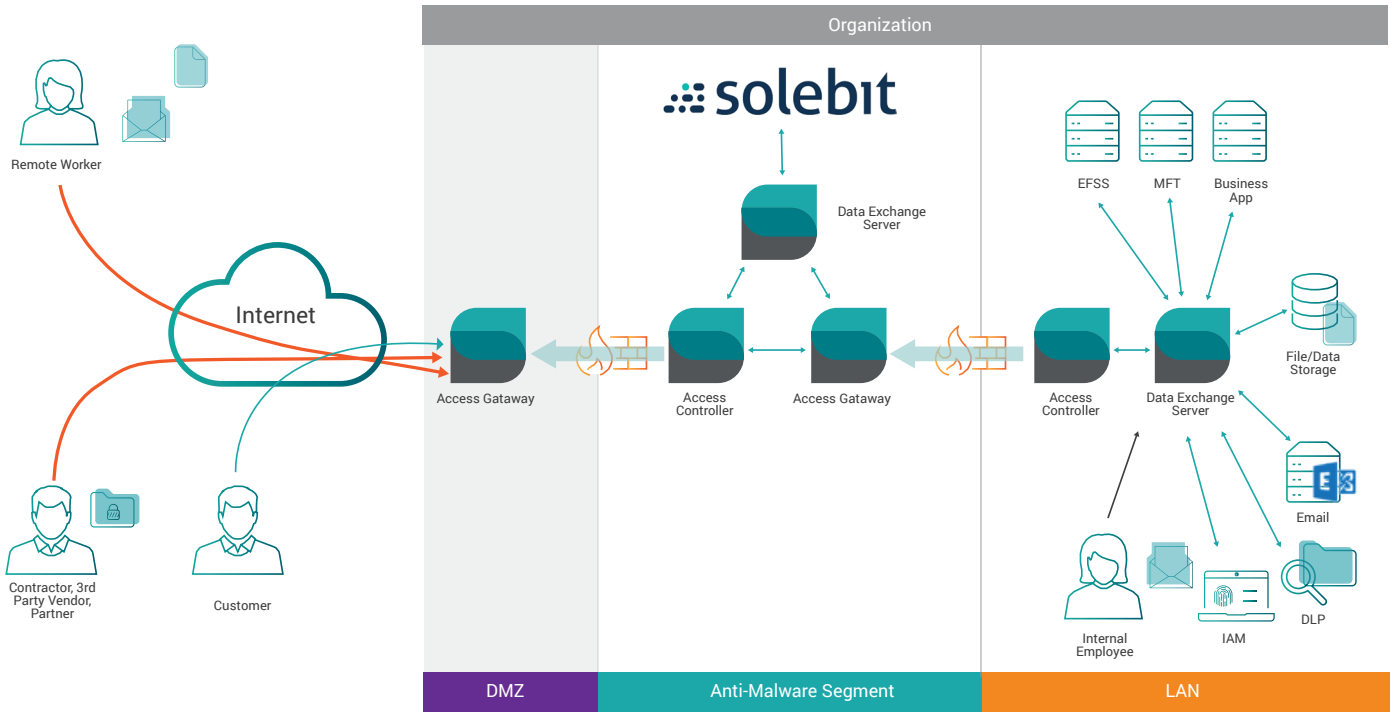
SoleGATE is an advanced threat protection platform, protecting organizations from unknown malware and zero-day attacks. SoleGATE introduces a new approach in malware protection by performing analysis at the data level, looking for hidden code which might have been injected by cyber criminals.

SoleGATE eliminates evasion techniques by systematically analyzing all code path and execution traversals to detect and block sophisticated macro/JavaScript attacks. This essentially eliminates all evasion opportunities.

SoleGATE uses a multi-tier protection schema to defend against attacks at different levels. This comprehensive approach is powerful, as evasion techniques may spread across different layers. The solution protects against advanced malware by using Solebit's patented deep inspection that analyzes commands from the CPU level, all the way up to the application level, analyzing macros and embedded JavaScripts in Microsoft office or any other data file types.

SoleGATE provides seamless prevention across all environments with no dependencies or customizations. The solution is agnostic to client applications and operating systems.

Joint Solution Diagram



- Full Zero Day protection - Signature-less, detects and prevents zero-day based attacks
- Provides conclusive results to enable real-time prevention without requiring user intervention to decide whether an item is truly malicious
- Extremely fast - Scales to meet customers throughput requirements
- Client-less file access
- Control usage of files
- End-to-end monitoring of file access flow

SAFE-T | solebit