FROST & SULLIVAN

RESEARCH & CONSULTING LTD

May 5, 2017

Initiation of Coverage - Excluding Valuation*

Safe-T: A Promising Entry Point to the Global Cybersecurity Technologies Industry

Stock Exchange: TASE

Symbol: SAFE

Sector: High-Tech

Sub-sector: Cybersecurity

As of March 30, 2017:

Closing Price: 6.65 NIS

Market Cap: 102.5 million NIS

# of Shares: 17 million

Stock Performance:** 67%

Price Range:** 3.99-7.67 NIS

Average Daily Trading Volume:** 113K NIS

** from June 21, 2016

Kobi Hazan - Lead Analyst

Analysts:

Jarad Carleton
Revital Rauchwerger
Dr. Tiran Rothman

Frost & Sullivan Research & Consulting Ltd.

Email: Equity.Research@frost.com
Tel.: +972-9-9502888
www.frost.com/EquityResearch

**Important Note: According to the Israel Securities Authority's regulation, an analysis can include a valuation only for companies that have been publicly traded for at least a year. A valuation will be added to the next quarterly analysis report.*

Company Overview

Safe-T Group Ltd. ("Safe-T"), listed on the Tel Aviv Stock Exchange (TASE: SAFE) since 2016, is a cybersecurity company that was founded in 2013 in Israel. The company develops and markets its High-risk Data Security (HDS™) Solution, which is designed to mitigate attacks on business-critical services and data for a wide range of industries, including financial, healthcare, government, and manufacturing organizations.

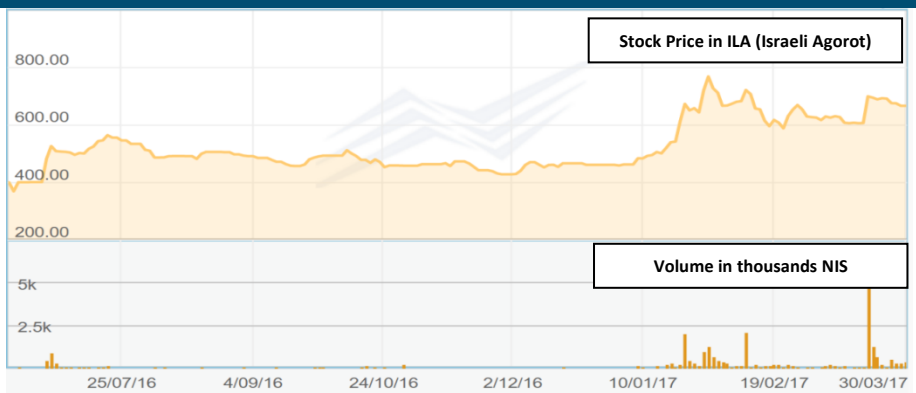
Deployed globally, HDS protects thousands of employees in enterprises and governments, securing their data, services, and networks from insider and external data threats. HDS mitigates data threats such as un-authorized access to data, services, and networks, as well as data-related threats that include data exfiltration, leakage, malware, ransomware, and fraud.

Headquartered in Israel, Safe-T is active in North America, APAC, Africa, and Europe.

Highlights

- Safe-T's activity was integrated into Matrat Mizug (as a reverse merger), a shelf corporation in 2016; the company commenced to be listed on TASE on June 21, 2016*
- Secure Data Exchange (SDE) and Secure Data Access (SDA), Safe-T's two flagship products, address large and growing markets. SDE's addressable market is valued at $3.4 billion in 2015, while SDA's was estimated at $992.8 million in 2016.
- However, Safe-T is active in a domain that generates intense competition. Smaller companies such as Safe-T are faced with the challenges of differentiating themselves, getting to market fast and first, and establishing a global presence
- Moreover, diverse regulatory and compliance requirements across various countries and regions increase the complexity for companies with a global presence.
- SDE comprises the features of three distinct products. Safe-T's management is convinced that no other vendor provides such breadth within one product.
- Within three years, Safe-T aims to become a significant player in the IoT and autonomous vehicles domains, both potential catalysts for substantial growth.
- We view the company as an attractive, but risky, investment in a small-size company in the fast-growing cybersecurity space. If the company successfully penetrates the North American and European markets, it may be acquired in the coming years as the consolidation trend surges.

Stock overview* YTD (Source: TASE website)



Executive Summary

Investment Thesis

Safe-T Group Ltd.[1], listed on the Tel Aviv Stock Exchange (TASE: SAFE) since 2016, is a cybersecurity company that was founded in 2013 by Amir Mizhar (32.88% holdings) in Israel. The company's solutions are designed to mitigate attacks on business-critical services and data for a wide range of industries, including financial, healthcare, government, and manufacturing organizations.

Safe-T is active in a domain that generates intense competition, wherein consolidation in the form of M&As is a growing trend. Smaller companies are faced with the challenges of differentiating themselves, getting to market fast and first, and establishing a global presence. Moreover, diverse regulatory and compliance requirements across various countries and regions increase the complexity for companies with a global presence.

Still, Secure Data Exchange (SDE) and Secure Data Access (SDA), Safe-T's two flagship products, address huge markets. SDE targets two primary markets: the Managed File Transfer (MFT) market that generated revenues of $1.15 billion in 2015, and the Cloud Access Security Broker (CASB) market that was valued at $3.4 billion in 2015. Moreover, the market for Safe-T's SDA, which targets the Software-Defined Perimeter (SDP) market, was estimated at $992.8 million in 2016.

Safe-T sells into a variety of vertical industries, including financial services, government, and healthcare. The three aforementioned verticals currently constitute 95% of their revenue stream:

- Financial Services customers include: Yelin Lapidot, Equiant, Banque Heritage, Temenos, LBG Austria, RLM Finsbury, one of the largest Israeli banks, and one of the largest Israeli insurance companies
- Government customers include: Gov.il, the Jewish Federation of Greater Vancouver, Netivei Israel (Israel's national transport infrastructure) and the Indiana Office of Technology
- Healthcare customers include: the Israeli Ministry of Health, Hadassah Medical Center (Israel), eviCore, and Kupat Holim Meuhedet (an Israeli HMO).

Within three years, Safe-T aims to become a significant player in the IoT and autonomous vehicles domains, both potential catalysts for substantial growth. Safe-T took a first step in the autonomous vehicles space through its recent announcement of an MOU with Foresight, for the establishment of a joint company to engage in cybersecurity for vehicles and railways.

We view the company as an attractive one, but believe that it entails the typical risks for a small-capitalization (cap) company in the fast-growing cybersecurity space. If the company successfully penetrates the North American and European markets, it may be acquired in the coming years, as the consolidation trend surges.

Vision

Safe-T is focused on high-risk data protection, and positions itself as "the only vendor today that provides a Cyber Dome for your high-risk security data needs." Safe-T's "Cyber Dome" refers to the company's High-risk Data Security (HDS™) Solution, which comprises its two flagship products: Secure Data Exchange (SDE) and Secure Data Access (SDA).

[1] Safe-T Group Ltd. has two private companies, which are wholly-owned subsidiaries: RSAccess Ltd. and Safe-T USA Inc. Additional information is available in the company's 2016 Financial Statements.

Furthermore, SDE comprises features of three distinct products in the market. SDE consolidates the functionality of Managed File Transfer (MFT), Enterprise File Sync and Share (EFSS) and Cloud Access Security Broker (CASB) into one cost-effective comprehensive product. Safe-T's management believes that no other vendor provides such breadth within one product, and that there is no other player in the secure data exchange market that unifies these three products into one unique value proposition.

Strategy

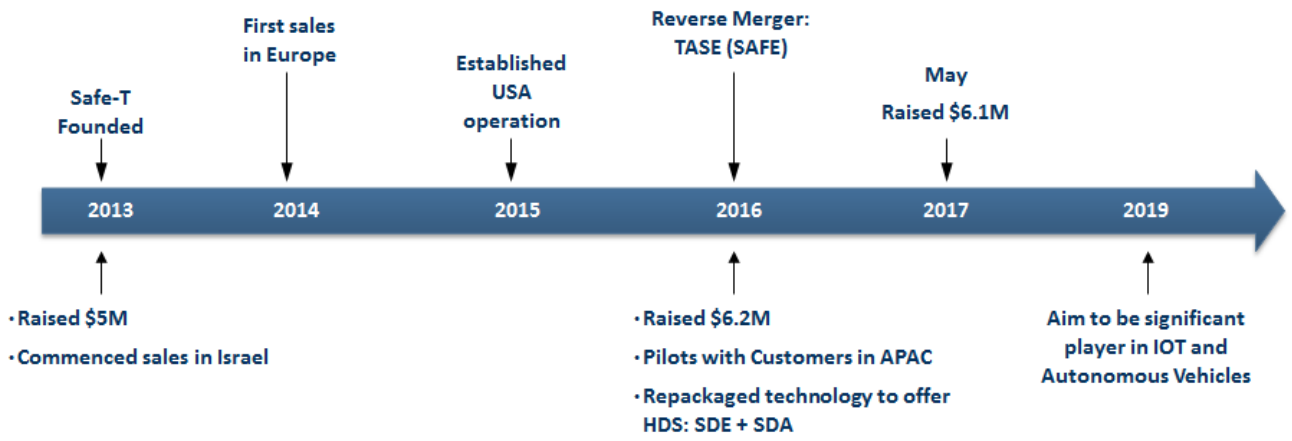
Safe-T positions itself as a "factory of technologies" offered to enterprises. During Q4 in 2016, the company repackaged their technology to offer one integrated comprehensive solution, and together their SDE and SDA products have evolved into their HDS. One reason for the change is that a high percentage of customers that purchased SDE also bought SDA to eliminate data from the demilitarized zone (DMZ), and use SDA to protect additional services and applications in addition to protecting SDE. An additional reason is due to the need to provide a single solution to address all high-risk data security requirements. Focused on enterprises, from SMBs to large global corporations, Safe-T is offering their HDS on-premises and as a Cloud-based as-a-service solution.

While the company is focused on promoting their HDS as a unique value proposition, we believe they will continue to sell their two flagship products individually, and bundled with their channel partners' complementary products.

Going forward, Safe-T's five-fold growth strategy comprises:

- Continued investment in R&D, improving existing products and developing new ones
- Recruiting additional OEM partners, resellers, distributors, and system integrators
- Opening new branches in key global locations
- Boosting marketing and sales activities, focused on enhancing their brand and reputation
- Establishing partnerships with industry leaders.

Roadmap



Scenarios

Upside Scenarios	Downside Scenarios
Safe-T is currently targeting very large addressable markets with fast-growing CAGRs, and planning to be a significant player in the IoT and autonomous vehicles' domains.	Safe-T is active in a domain with intense competition, including large companies.
SDE comprises features of three distinct products in the market - consolidated into one cost-effective comprehensive product. Safe-T believes that no other vendor provides such an offering. Safe-T's HDS is a comprehensive solution that comprises both SDE and SDA, based on real market need: 95% of enterprises that purchased SDE also bought SDA.	Regulatory and compliance requirements differ across countries and regions, and Safe-T may be obligated to comply with a complex variety of such specifications in order to remain competitive globally.
The M&A trend will pose an opportunity for Safe-T if it becomes an acquisition target, or alternatively, a threat if the company will have to deal with competitors that merged and became stronger as a result.	

Contents

Executive Summary **2**
Investment Thesis 2
Vision 2
Strategy 3
Roadmap 3
Scenarios 4
Market Analysis **6**
Market Overview 6
Market Need 6
Market Size & Growth Rate 7
Regulation 8
Trends & Drivers 8
Restraints 9
Technology **10**
Product / Service Offering **12**
Overview 12
Secure Data Access Solution (SDA) 12
Secure Data Exchange Broker Solution (SDE) 14
Marketing & Sales **16**
Target Markets & Customers 16
Marketing 17
Sales 17
Technology & Business Partners 19
Competitive Analysis **21**
Roadmap **23**
Financial Analysis **24**
P&L Analysis 24
Balance Sheet and Operational Cash Flow Analysis 24
Comparison to Similar Companies 24
Appendices **26**
Appendix A- Financial Reports 26
Appendix B – Management & Top Shareholders 27
Appendix C – Frost & Sullivan Analyst Team 28
Disclaimers & Disclosures **29**

Market Analysis

Market Overview

The cybersecurity market is vast and competition is intense. The majority of cybersecurity players are targeting enterprises, and these enterprise customers have a plethora of choices to secure their networks, computers, applications and data from attack, damage or unauthorized access.

This analysis will focus on Safe-T's four target markets:

1. **Software-defined Perimeter (SDP)** - secures connectivity between an enterprise's applications and data, and authorized end-point and/or users.
2. **Cloud Access Security Broker (CASB)** - software/service positioned between an enterprise's own infrastructure and that of a cloud provider, which allows enterprise to apply security policies on traffic destined for the cloud or arriving from the cloud
3. **Managed File Transfer (MFT)** - software/service that manages the secure transfer of data among devices through a network, for example, the Internet
4. **Enterprise File Sync and Share (EFSS)** - software/service that securely synchronizes and shares files and data among multiple devices

Market Need

Enterprises of all sizes face challenges in securing their data. They are seeking to mitigate data-related threats, including un-authorized access to data, services, networks, or APIs; unauthorized transfer of data from a computer; data breaches; malware; ransomware; and fraud.

The proliferation of legacy data exchange solutions, and the lack of integration with security solutions, exacerbates the existing potential for cyber-attacks as enterprise applications and data are oftentimes visible to the outside world.

Source: Safe-T Corporate Presentation, January 2017

Investment in cybersecurity for many regulated industries is a requirement for regulatory compliance and improved corporate governance. However, as new regulations are implemented, such as GDPR in Europe, the need to invest in strong cybersecurity solutions will increase in MNCs across all industries.

The exponential increase in high-risk data, the shift to cloud-based storage, BYOD ("bring your own device"), and distributed data centers connected via the Internet, are just some of the trends leading to an alarming growth in cybersecurity risks. Enterprises now, more than ever, are seeking strong next generation solutions to secure PII (personally identifiable information), trade secrets, and all other types of business critical data.

Market Size & Growth Rate

Safe-T's SDE addresses the Managed File Transfer (MFT), Enterprise File Sync and Share (EFSS), and Cloud Access Security Broker (CASB) markets, while the company's SDA addresses the logical segmentation, application access, and Software-defined Perimeter (SDP) markets.

Safe-T SDE Addressable Market

By basing market size on the amount of traffic that includes continual exponential growth of emails, documents, financial data, and medical images, the potential market size for solutions that secure high-risk data is substantial. Emails alone constitute an amount that is vast in itself. It has been forecast that 132 billion business emails are currently sent daily.[2]

Safe-T aims to secure high-risk enterprise data. As described previously, Safe-T SDE is a solution that unifies all data exchange flows, while addressing three cybersecurity market verticals simultaneously: MFT, CASB and EFSS.

1. **Managed File Transfer (MFT) -** The global MFT market is expected grow moderately during 2016-2025, from an estimated $1.23 billion in 2016 to $2.1 billion by the end of 2025. North America is expected to dominate with 40%+ market share by end-2025, followed by Western Europe with nearly 28%.[3]
2. **Cloud Access Security Broker (CASB) -** The CASB market was valued at $3.4 billion in 2015 and by 2024, is expected to reach $13.2 billion with a CAGR of 16.7% (2016 - 2023). SMBs have been the driving force behind the rapid adoption of CASB solutions.[4]
3. **Enterprise File Sync and Share (EFSS) -** In 2013, the market for EFSS was estimated at $0.5 billion. It is currently expected that by 2018, "70% of EFSS destination vendors will cease to exist, having been acquired or put out of business, and the remaining 30% will evolve to support the digital workplace or modernize corporate data infrastructures."[5]

Safe-T's SDE solution encompasses the functionality of MFT, EFSS and CASB solutions in one comprehensive solution. As the size of EFSS market is relatively negligible and diminishing in comparison to the MFT and CASB markets, we have not included it in our calculations. As such, the company's addressable market size is estimated to be approximately $5 billion.[6]

[2] The Radicati Group. *Email Statistics Report, 2016-2020.* March 2016.

[3] Future Market Insights (FMI). Managed File Transfer (MFT) Software and Service Market: North America Anticipated to Dominate the Global Market Through 2025: Global Industry Analysis and Opportunity Assessment, 2016-2025. February 2017.

[4] Transparency Market Research. *Cloud Access Security Brokers Market - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2016 - 2024*. April 2016.

[5] Gartner. *Magic Quadrant for Enterprise File Synchronization and Sharing*. July 2016.

[6] Although the $5 billion market size is based on data from different years (MFT from 2016, CASB from 2015, and EFSS from 2013), we believe that it provides a good estimate.

Safe-T SDA Addressable Market

SDA is primarily aimed at the Software-Defined Perimeter (SDP) market. It is estimated that the global SDP market will grow from $992.8 million in 2016 to $4.4 billion by 2021, at a CAGR of 34.7%.[7]

Trends shaping the market for Safe-T's SDA offering include:[8]

- *Through the end of 2017, at least 10% of enterprise organizations (up from less than 1% today) will leverage SDP technology to isolate sensitive environments.*
- *By 2021, 30% of enterprises will remove most digital business services from the visible public internet, up from less than 1% in 2016.*
- *By 2021, 60% of enterprises will phase out network VPNs for digital business communications in favor of software-defined perimeters, up from less than 1% in 2016.*
- *By 2020, 30% of enterprises will move consumer-facing services that require public internet access to IaaS providers and phase out legacy demilitarized zone (DMZs).*
- *Through 2021, organizations that isolate and remove digital business services from direct public internet access will experience 70% fewer successful attacks than organizations that didn't adopt isolation.*

Regulation

Safe-T's SDE is designed for Regulation Compliance, which will enable enterprises from various sectors including financial, healthcare and government, to comply with statutory requirements delineated in over a dozen regulations globally, with the objective of protecting sensitive data in transit and at rest.
The company plans to get certified for the US Federal Information Processing Standard (FIPS) 140-2.

Trends & Drivers

Key trends and drivers that support the need for Safe-T's solutions include:

- Increasing incidences of cyber- threats, cyber-attacks, spear phishing, ransomware, and advanced persistent threat (APT) attacks are on the rise, including via social media sites as well as compromised websites.
- BYOD to work has become the norm, bringing with it a host of mobile bots.
- Exposure of confidential information, unintentionally or otherwise, can result in failure to meet regulatory standards, leading to legal action, fines, theft of intellectual property, bad publicity, and loss of customers.
- 75% of businesses lack sufficient cybersecurity expertise, which increases opportunities for vendors.[9]
- Cloud-based storage and applications, such as Salesforce and Dropbox, across all verticals and industries, inevitably increase the need for cloud-based security services
- Software-defined perimeter (SDP) and other isolation technologies will go mainstream over the next five years and is expected to be adopted by over 30% of enterprises.[10]

[7] MarketsandMarkets. *Software-Defined Perimeter Market by Enforcement Point, Component, Deployment Mode, Organization Size, End User, and Region - Global Forecast to 2021*. November 2016.
[8] Gartner. *It's Time to Isolate Your Services from the Internet Cesspool*. September 2016.
[9] Seals, Tara. "75% of Orgs Lack Cybersecurity Expertise." Infosecurity, October 2016, www.infosecurity-magazine.com/news/75-of-orgs-lack-cybersecurity.
[10] Gartner. *It's Time to Isolate Your Services from the Internet Cesspool*. September 2016.

Restraints

Key restraints include:

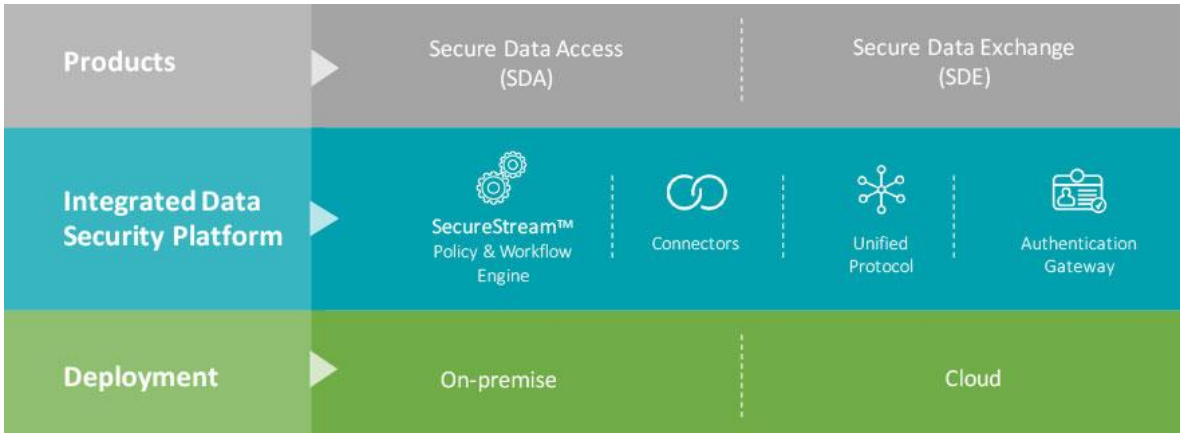
- The cybersecurity market is vast, competition intense, and consolidation in the form of mergers and acquisitions is a growing trend.
- Enterprise adoption for software-defined perimeter (SDP) technology and other isolation techniques is less than 1% today.[11]
- Regulatory and compliance requirements within various countries and regions increase the complexity for companies with a global presence.

[11] Ibid.

Technology

Safe-T's Integrated Data Security Platform:

Safe-T's High-risk Data Security (HDS) solution is built on the company's **Integrated Data Security Platform (IDSP)**. The IDSP integrates policies and workflows, data encryption, high availability, authentication, roles management, reporting, and detailed audit trails.



Source: Safe-T

- **SecureStream Policy and Workflow Engine:** enables enterprises to enforce security policies on any data exchange and data access workflow. Each workflow is fully controlled and monitored, providing complete auditing and tracking information.
- **Connectors:** enable integration with an enterprise's ecosystem, including its business applications, data storages, web sites, and security solutions. Safe-T's connectors' module exposes a multi-language standard API (including REST, SOAP, ICAP, and WS) that allows enterprise users and other 3rd parties to develop new connectors, modify existing ones, and integrate with new enterprise solutions.
- **Unified Protocol**: exposes a standard API, making data transfer processes transparent, regardless of the protocol or application used. Safe-T's IDSP supports native and SDK-based support for all common enterprise file transfer and business applications' protocols, including: HTTP/S, SSH, FTP/S, SFTP, ICAP, SMB, and REST.
- **Authentication Gateway:** allows implementing user authentication and authorization enforcement actions through multiple authentication engines, as part of any data exchange or access workflow.

Workflows are created through the integration of Safe-T's Connectors and Authentication Gateway with its SecureStream Policy and Workflow Engine, for example:

- Automatically enforce security policies on outgoing/incoming data exchange flows
- Create multi-factor authentication and authorization workflows
- Receive an uploaded file from a user and store it in a SFTP folder
- Store a file received from a document management system in an NTFS location
- Pass an email attachment to a DLP to be scanned and then to an encryption solution to be encrypted.

Safe-T's Connectors allow its products to be integrated with enterprise ecosystems, including with the latter's business applications, data storages, web sites, and security solutions.

SDE supports dozens of pre-built Safe-T Connectors, divided into three types:

Business Application	Data Storage	Security/Authentication Solution
SharePoint / SharePoint Online	SQL	IAM
Oracle	MySQL	IDP
MS Exchange	NFS	DLP
Documentum	NTFS	Anti-Malware
IBM AS400	SSH	Encryption
Outlook / Outlook 365	Cloud Storage (including DropBox, Box.com, and OneDrive)	Sandbox
SMS providers	SFTP	ActiveDirectory
		LDAP

Source: Safe-T

Customers can integrate their enterprise components with Safe-T's connectors via one of three methods:

1. **Out-of-the-box, designed specifically for enterprises**
   - "Plug and play" built-in connectors directly; or
   - Use Safe-T's API to implement an integration
2. **Professional Services**
   - Buy professional services, i.e., development hours for Safe-T to implement an integration
3. **DIY Integration**
   - Customize existing built-in connectors, for example, customize the SharePoint connector for an updated version of SharePoint

To develop connectors and integrate with SDE, 3rd parties are also provided with Safe-T's SDK.

Product / Service Offering

Overview

Safe-T's HDS is aimed at securing, managing and brokering enterprise customers' data and traffic patterns. HDS comprises two software-only products that can be deployed on-premises or in the cloud:

- Secure **Data Access** (SDA) - (*former product name: RSAccess*) software-defined perimeter (SDP) and logical segmentation solution, which creates a secure data center and protects all applications while enabling access.
  - Safe-T's patent for Reverse-Access™ method for securing front-end applications has been granted by the EPO, and in Austria, Switzerland, Germany, Spain, France, UK, and Italy. It is pending in China and Hong Kong, and in examination in the USA and Israel.
- Secure Data Exchange (SDE) - (former product name: Safe-T Box) data exchange broker, designed to modernize data infrastructure, control the flow of data in and out of the enterprise, and protect all applications while exchanging data.

SDE runs on Windows, and SDA on Linux. HDS client interfaces are available for iOS, Android, Windows, Linux and Outlook. Currently, nearly all HDS deployments are on-premises, but its cloud-based as-a-service solution targeted at SMBs is gaining traction globally.

To date, Safe-T's SDE constitutes the majority of sales to enterprises, as it allows for consolidation of all outbound and inbound scenarios on one platform. Case studies include a major Israeli bank that purchased SDE for protecting file upload capability for check scanning, and the Indiana Office of Technology that is using SDE to communicate with their partners, shareholders, and citizens.

Secure Data Access Solution (SDA)

SDA Secure Front End

Safe-T SDA is built on top of the Safe-T Integrated Data Security Platform (IDSP) and Safe-T's patented and secure reverse access technology. SDA is purpose-built to create a highly secure data center perimeter, protecting all applications while enabling access to them.

Safe-T's SDA is a software-only solution that secures access to data, applications, and the perimeter. It allows traffic to pass between two network segments, without the need to open ports within a firewall. This reverse-access solution is designed to overcome the challenges of current DMZ networks and network segmentation, prevent criminal application access, application hacking, and protect classified networks within the enterprise infrastructure.

A DMZ, defined as a screened sub-network that is placed between an internal network and the Internet, creates three distinct areas:

- **Public (Internet) area** - open to the general public and does not provide protection to systems located within it
- **DMZ Middle area** - comprises systems for providing data and application services to an enterprise's clients via the Internet, including: SharePoint, web mail services, ERP and CRM systems
- **Internal area** - corporate or trusted network comprising systems and hosts considered to be fully protected and secured.

DMZ architecture poses a number of challenges:

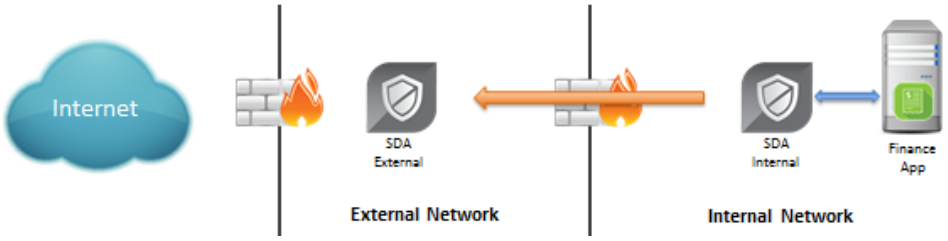
- To share information with external users, companies situate their applications and data in the DMZ, placing them at risk of being hacked or compromised

- Most DMZ implementations require opening firewall ports between the Internet and the DMZ to provide access to a service in the latter, which enables a potential attacker to take control of the service
- DMZ network configurations are costly when used to protect against external threats, as data and services in the internal network are sometimes duplicated in the DMZ (necessitating additional hardware and software licenses, as well as perpetual replication processes to ensure data synchronization).

Safe-T SDA eliminates the need to store sensitive data in the DMZ, and permits only authorized access to data, services, networks, and APIs. SDA is deployed on-premises or as a hybrid-cloud DMZ (DMZaaS).

How Safe-T's SDA works

1. An incoming request from a user/external application to an internal application arrives at the External Network node
2. The Internal Network node immediately pulls the request into the LAN over an outbound connection, and utilizes the SecureStream engine to apply policy and workflow to traffic
3. The request is sent to the internal application, and a reply is sent back to the user/external application



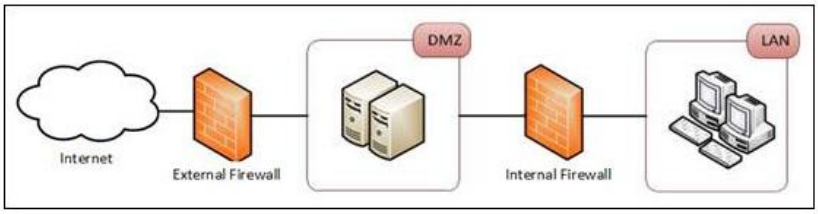
Source: Safe-T Corporate Presentation, January 2017

SDA Configurations

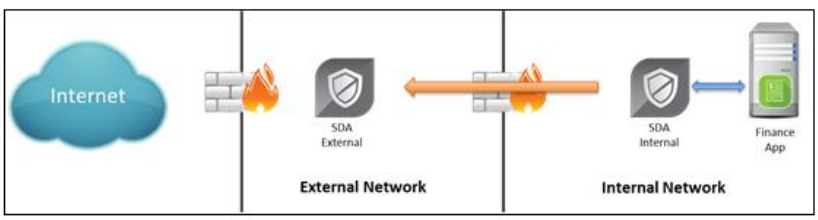
Configuration I: Securing the DMZ Front End

Most enterprises employ a DMZ sub-network that acts as a buffer between their internal networks and the Internet. Nevertheless, the DMZ does contain vulnerabilities as its network ports remain open to the Internet. Deployed in the DMZ, SDA reduces the former's hardware and software footprint, and eliminates the need for of data replication and synchronization.

Before SDA -



After SDA –



Source: Safe-T

Configuration II: Securing the Classified Network

In addition to separating the DMZ from the internal network, large enterprises also divide their internal networks into distinct sub-networks for greater security. Sub-networks avoid compromising the entire network if hackers gain unauthorized access to one of the internal sub-networks. Operating in conjunction with firewalls, SDA enables connectivity among sub-networks without exposing one sub-network to another.

Configuration III: Securing the Network Frontline Gateway

Many network gateways are protected by multiple layers of security mechanisms that require regular updates, including anti-virus, anti-spyware and anti-malware software. By closing open network ports and permitting only approved communications to access the network gateway, external security threats are minimized.

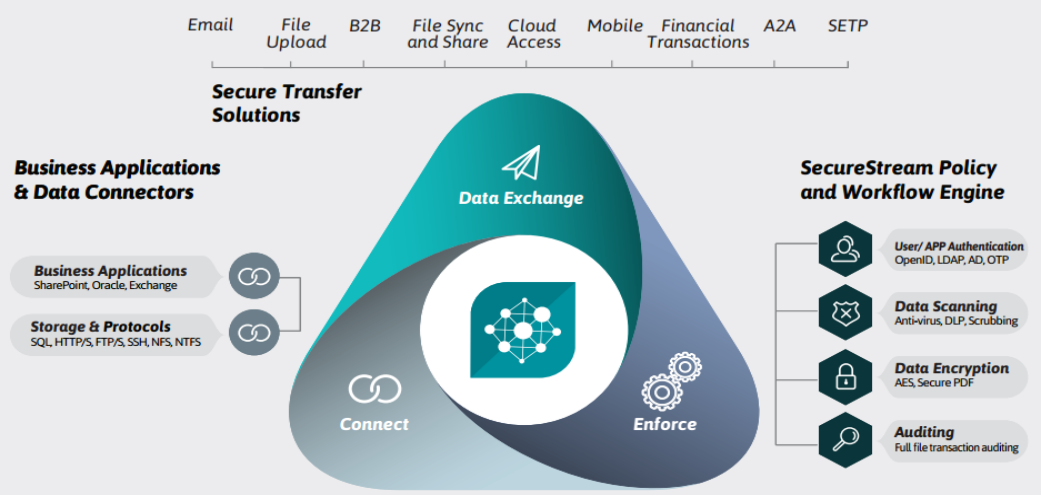
SDA use cases include:

- Software-defined Perimeter (SDP) – provides secure access to an entire organization's data center, as it conceals an organization's location and architecture
- Secure Partner Access – provides secure, authenticated, and scanned direct-access to any application for external partners and users, without opening ports in the firewall, or needing to provide VPN client-software
- Logical Network Segmentation – logically segments an enterprise's network, deploying a Zero Trust model, to reduce the risk of cyber-attacks from attaining access to, or moving through, internal network segments
- Secure Application Access - provides secure, authenticated, and scanned direct-access to any application, without opening any ports in the firewall.

Secure Data Exchange Broker Solution (SDE)

A major cause of cyber-attacks is the abundance of data exchange methods and data storage solutions within a given organization, including: emails, EFSS solutions, MFT solutions, S/FTP servers, network file storages, document management applications, human file upload portals, applications transferring data, and consumer cloud solutions.

Safe-T's Secure Data Exchange (SDE), a component of the company's Safe-T High-risk Data Security solution protects both inbound and outbound data exchange. It enables enterprises to broker, control and secure data exchange of any type and size between users, applications, cloud solutions, and businesses. SDE is based on a combination of Safe-T's IDSP and Secure Virtual Vaults (SVV) technology. SVV technology allows converting any type of storage to an encrypted digital vault, including: network file storage, FTP/SFTP site, cloud storage, databases, and document management systems.



Source: Safe-T Secure Data Exchange Brochure, 2017

The combined technologies create a Secure Data Exchange Broker solution that integrates an enterprise's data exchange and data storage solutions; prevents data exfiltration, leakage, malware, and fraud; secures data exchange with customers, partners, applications, and the cloud; and stores the data secured and encrypted. As to encryption, Safe-T supports two options: encrypt at rest and transfer decrypted over a secure channel to the user; and encrypt both at rest and in transit.

Deployed on-premises or in the cloud, **SDE comprises three separate, yet interconnected modules**:

- ***Connect*** – connectors to integrate with business applications, local and network storages, protocols, and cloud storage
- ***Enforce*** - policy enforcement engine to create and enforce automated security policy workflows
- ***Data Exchange*** - secure transfer solutions support a variety of outbound and inbound secure data exchange methods.

Safe-T Secure Transfer Solutions for Enterprises includes the following components:

- **Cloud Access Security Broker (CASB) -** connects to consumer cloud storage and cloud SaaS solutions (such as DropBox, Box.com, Google Drive, Microsoft SharePoint Online, and Microsoft Azure), while maintaining full visibility, governance, and control of all data and files uploaded and downloaded from the cloud
- **Secure Managed File Transfer (MFT)** - securely transfers sensitive data and uploads files. Adds security layers to standard file share and file upload solutions including authentication, data scanning and data encryption (supports a basic DLP and integrating with 3rd party DLPs). Integrates seamlessly with business applications, legacy systems and proprietary tools
- **Safe-T Secure File Sync and Share (EFSS)** - secures enterprise file and data collaboration solution that enables data access from any device (web, desktop, mobile) without the need for a VPN
- **Safe-T Secure Email** - sends sensitive emails securely between applications and users, without requiring recipients to install software or exchange cryptographic keys
- **Safe-T Secure Data Exchange Network** - creates a secure 'internal' network for the transfer of files.

Safe-T's SecureStream Policy and Workflow Engine

- Automatically enforces security policies on outgoing/incoming data exchange flows
- Provides multi-factor authentication and authorization, and data exchange workflows
- Brokers traffic to 3rd party security (DLP, AV, and Anti-malware) and AWS Identity and Access Management (IAM) products

SDE Use Cases include:

- **Human Data Exchange** – control, manage, and secure human data exchange scenarios, including: incoming/outgoing email, S/FTP, consumer cloud access, file uploads, mobile data exchange, employee collaboration (EFSS), and digital vaults
- **Application Data Exchange** – control, manage, and secure application data exchange scenarios, including: business to business file transfers, application to application file transfers, and financial transactions
- **Anti-Financial Fraud** – deploy a highly secured and authenticated end-to-end solution for digital check deposits, ATM withdrawals, wire transfer, and emails requests.
- **Prevent Ransomware Attacks** – prevent ransomware attacks from encrypting NTFS located files, by controlling the allowed file encryption type, verifying file integrity, preventing copying un-allowed files, preventing modifying file types and format, tracking and logging all file based actions, and ensuring that any file manipulation is implemented solely by SDE.

Marketing & Sales

Safe-T uses the following logo:

SAFE-T
Accelerating Safe Business

Target Markets & Customers

Safe-T is positioned as a cybersecurity company that can sell into any vertical industry, including: financial services, government, healthcare, education, defense, law firms and manufacturing. The company cites financial services, government, and healthcare as their "sweet spots," and these currently constitute 95% of their revenue stream. Safe-T expects that the bulk of their revenue will continue to be generated from these three industries.

The Financial Services Industry (FSI) includes banks, investment houses, credit cards, fintech, insurance, and mortgage origination companies. Safe-T's current FSI customers include: Yelin Lapidot, Equiant, Banque Heritage, Temenos (banking software), LBG Austria, RLM Finsbury, one of the largest Israeli banks, and one of the largest Israeli insurance companies.

The Healthcare industry includes hospitals, HMOs, labs, and health insurance (preauthorization) companies. Safe-T's current customers include: the Israeli Ministry of Health, Hadassah Medical Center (Israel), eviCore, and Kupat Holim Meuhedet (an Israeli HMO).

The Government sector includes Government Ministries, Defense and HLS, and Law Enforcement.
Safe-T's current customers include: Gov.il, the Jewish Federation of Greater Vancouver, Netivei Israel (Israel's national transport infrastructure) and the Indiana Office of Technology.

Safe-T's roster of customers also includes large corporations in the ***manufacturing, utilities, and law*** sectors such as: Groupe Minoteries, Rollomatic SA, ECI Telecom, Boegli-Gravures S.A., and one of the largest industrial companies in Israel. In addition, Safe-T has attracted interest from the ***Education*** sector, and counts the Weizmann Institute of Science and University of Haifa among its customers.

Geographies

Safe-T has a strong presence in Israel, is expanding its sales efforts in the USA, and gaining traction in Eastern Europe and Singapore. Sales in the USA will be their primary focus over the next three years, and are expected to constitute 25% of their revenues in the future. Safe-T has a marketing, pre-sales, and sales presence in the USA, with feet on the ground in Connecticut, Arizona, New Jersey, Ohio, and California.

The difference in type of sales in the USA and Europe are marked. Whereas Europe presents the potential to close a large number of deals with small- and medium-size enterprises, the USA provides more potential deals with large enterprises (1,000+ employees). Notwithstanding the smaller number of deals, the USA is strategic to Safe-T in terms of building their brand and reputation due to the size of the market.

With respect to Central and Western Europe, Safe-T is currently establishing an operational infrastructure for indirect sales through re-sellers and distributors in Germany, France, Italy, and the UK. However, as an Israeli company developing cybersecurity technology, Safe-T faces challenges in countries such as Switzerland and Germany. In contrast, countries such as Serbia and Turkey look favorably upon Israeli technology.

Shachar Daniel, Safe-T's CEO considers it crucial to the company's success that they remain highly focused on specific geographies. As he stated during a call with us: "If we go all over, we can lose all over."

Marketing

Safe-T's current marketing efforts are aimed at public relations in Israel (via the Israeli firm Kav Yashir) and the USA (via the Israeli firm SpiceTree); investor relations in Israel; participation in conferences globally; and social media activities such as LinkedIn, Twitter, Facebook, and blogs.

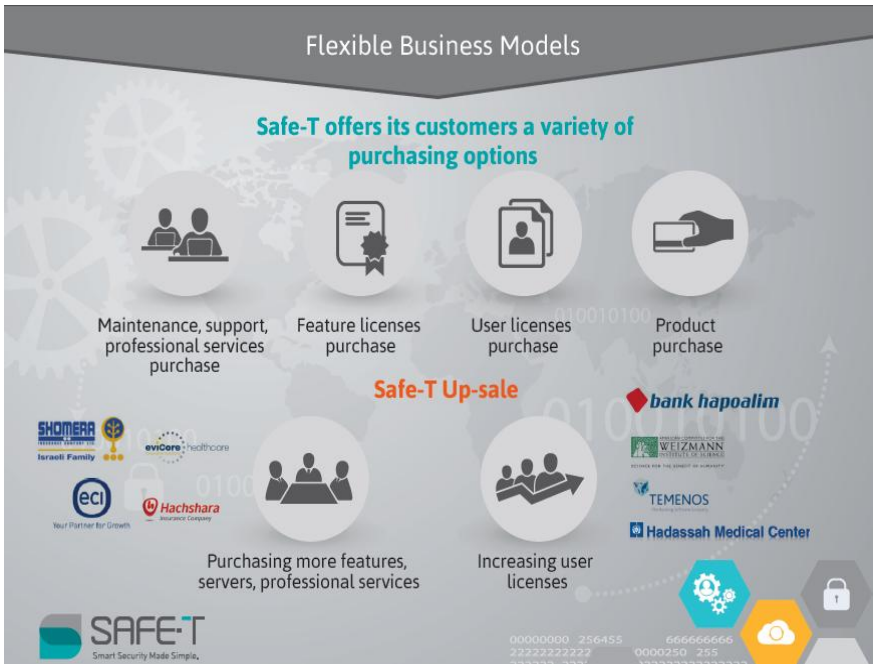
Their current marketing budget is in the range of a few hundreds of thousands of dollars, primarily to cover fixed costs for consultants and contractors of digital marketing and public relations, and maintaining investor relations with analysts. Safe-T's marketing budget also covers events (such as exhibitions, customer events, and partner events), corporate videos, press releases, advertisements, and marketing communication that include giveaways and printed materials. The company's resellers and distributors participate primarily in local events in their regions.

Going forward, and subject to financial considerations, Safe-T intends to extend and increase their marketing budget, with a focus on strengthening their brand globally.

Sales

Safe-T sells directly in Israel and the USA. The company sells indirectly in Israel, USA (i.e., SecureAuth), Europe, and APAC, through OEM partners, resellers, distributors and system integrators.

As the company does not possess adequate local presence for deployment and support activities (which also result in lower margins), it aims to increase sales via channels and OEMs. Going forward, direct sales are expected to provide 30% of revenues. Currently, Safe-T's gross margin stands at approximately 37%, due to the need to provide customer support. As revenues grow, and the number of its resellers (that handle support issues) increase, the company expects gross margins to level out at 90% within two years.



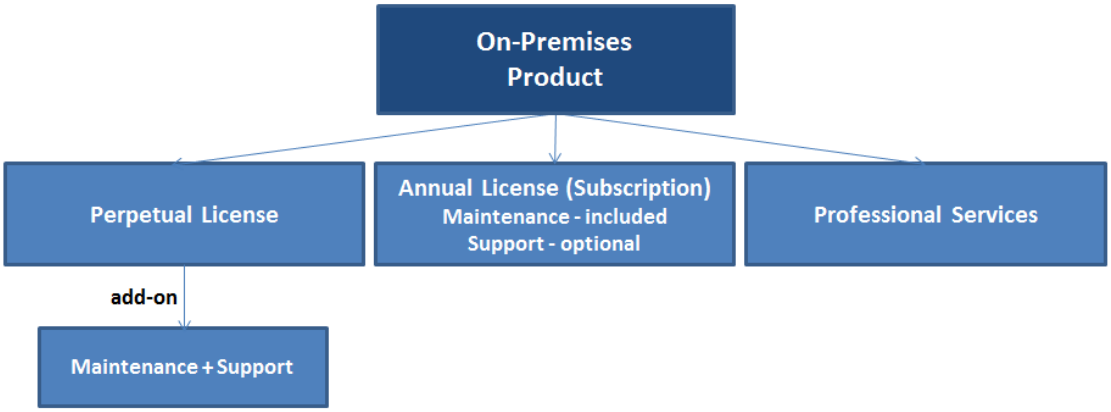
Source: Safe-T Investor Presentation, 2016

Sales Strategy

Safe-T sells its products on-premises, as-a-service, and via OEM agreements.

- **On-premises solutions** are sold directly and indirectly, for which Safe-T provides a virtual machine and end-user licenses, and the end-customer provides the server hardware.
- **Cloud-based "as-a-service" solutions** are sold indirectly through Safe-T's channel partners, for example, Shield4uc sells a hosted service to Canadian SMBs. The average price for as-a-service subscriptions is $100/user annually.
- **OEM agreements** are made for SDA sales only, for which Safe-T white labels their product.
    - **Case Study**: Safe-T white labeled their SDA through SecureAuth, a Safe-T partner and Identify Provider (IdP). **SecureAuth** sells on-premises SDA as SAAG (SecureAuth Access Gateway), one node in the DMZ and one in the LAN. To date, SecureAuth has implemented SDA at the largest healthcare clinic for women on the US East Coast, and at one of the largest global biotechnology companies.

On-Premises Sales



- Whether direct or through channels, on-premises sales of Safe-T's products generate recurring revenues based on perpetual and annual licenses. With respect to "perpetual license" versus "annual license" sales: on the first sale, perpetual license sales are approximately 2.5 - 3 greater than annual license sales, but as of the second year, revenues generated from maintenance amount to only 20% of the first sale, while "annual license" (subscription) sales remain constant.
- Perpetual licenses are sold as a one-time fee, based on the number of users; maintenance (20% of cost) and support are add-ons. Level 1 and Level 2 support cost an additional 3% and 7%, respectively. Maintenance costs serve as the basis, and thus support cannot be purchased without maintenance. Software updates are provided through maintenance payments.
- Annual licenses include maintenance and support, and are usually sold as 3-year contracts and amortized over that period of time.
- Safe-T sells professional services to their customers and resellers, which includes proof-of-concept, pre-deployment support, customization, and deployment services.

Of the company's 40 customers, six have not renewed their maintenance period, which represents an approximately 15% churn rate. At least three of these customers left during Safe-T's first or second year of operations, when solutions were less comprehensive and less stable. As Safe-T's products and processes mature, and as their understanding of the market improves, the company expect no more than 10% churn going forward.

Technology & Business Partners

Source: Safe-T Investor Presentation, 2017

Safe-T has partnered with a number of technology companies:

- **FICO**: analytics software company that provides a range of vertical solutions, include credit scoring in the USA. Their cloud-based analytics solution is integrated with Safe-T's SDA
- **ECI Telecom**: ECI's cyber division sells racks integrated with SDA to telecoms
- **Check Point**: joint partnership, integrating SDE and Check Point's Sandblast solution. SDE transmits data to be scanned by Sandblast
- **ODI**: like Check Point, Safe-T's SDE is integrated with ODI's scrubbing solution
- **RE-SEC**: like Check Point, Safe-T's SDE is integrated with RE-SEC's scrubbing solution
- **OPSWAT**: like Check Point, Safe-T's SDE is integrated with OPSWAT's scrubbing solution
- **SecureAuth**: OEM partnership with Safe-T; SecureAuth sells SDA, which is deployed as a proxy, bundled with their Secure Access Gateways as on-premises servers.
- **Microsoft**: Safe-T develops connectors for Microsoft offerings such as SharePoint and Outlook
- **Foresight**: During April 2017, Safe-T and **Foresight** announced a Memorandum of Understanding (MOU) for the establishment of a joint company to engage in cyber security activity in the domain of vehicles and railways. Based on the MOU, the two companies reached an understanding regarding their holdings in the joint company, and have agreed that Safe-T will provide the joint company with a license (in return for payment) to use its SDA product.
    - Safe-T will provide (in return for payment to be determined in a service agreement to be signed between Safe-T and the joint company): customization services to adapt its products for the transportation domain; development services; and technical support.
    - Foresight and Rail Vision (which develops an automated early warning system for train safety, and is a partner in the joint company as Foresight currently owns 32% of Rail Vision), will leverage their knowledge and business relationships in the areas of autonomous vehicles and trains to provide the joint company with consulting and sales services (in return for payment as stipulated in the agreement), in addition to other business services.
    - A fourth party, Shrem-Silberman Group, will provide the initial financial resources through direct investment and will be responsible for future financing of the joint company's operations.

Safe-T's channel partners include resellers, distributors, and system integrators.
They include, but are not limited to:
USA - Resellers, Distributors and System Integrators

- **Shield4uc** - sells cybersecurity services including fax and email transmission
- **SYNNEX** - business process services
- **Escalade IT** - cloud security services provider and IT consultancy and implementation firm.
- **Corporate Computer Solution**s - provides professional services
- **Software Licensing Advisors** - Microsoft product licensing advisors
- **Insight** - IT services

Europe - System Integrators

- **COMING** - Computer Engineering - *Serbia*
- **Newtech Security** - *Italy*
- **Creative Consulting GmbH** - *Germany*
- **TR & MA Information Technology** - *France*
- **InfoNet** - *Turkey*
- **E-Secure** - *Switzerland*

Israel - System Integrators

- **Taldor**
- **Smart-X Professional Services**
- **2Bsecure**

APAC

- **Cyber Armor** - exclusive system integrator - *Singapore, Hong Kong, Korea, Thailand, Taiwan, and other countries in APAC*

Competitive Analysis

Safe-T's competition is diverse and abundant. Competing vendors are divided across four products:

- Secure Data Access (SDA)
    - **Software-defined Perimeter (SDP)**
- Secure Data Exchange (SDE)
    - **Managed File Transfer (MFT)**
    - **Cloud Access Security Broker (CASB)**
    - **Enterprise File Sync and Share (EFSS)**

Safe-T's SDA

SDA is positioned within the Software-defined Perimeter (SDP) space, as it secures the connectivity among enterprise applications and data, and authorized end-points and/or users. Competing vendors include: Vidder and SOHA, which was acquired by Akamai. Although these vendors are strong players, Safe-T's SDA offers competitive advantages, including:

- No need to open inbound firewall ports
- Ability to broker traffic to 3rd party solutions
- Support for any TCP based application, including HTTP/S, RDP, and SSH
- Bi-directional traffic flow
- Application front-end deployment
- Cloud-based deployment
- Authentication gateway
- Built-in application firewall

Safe-T's SDE

SDE competes across three products: MFT, CASB, and EFSS. As Safe-T's management is convinced that there is no other single player in the secure data exchange market that unifies these three products into one unique value proposition, this analysis will address the overall competition in terms of features, but will provide representative competing vendors per product. The majority of Safe-T's SDE competitors provide only one data exchange capability, for example secure email; enterprise grade cloud-based storage; web, desktop, and mobile clients; support for all major file types and sizes; some level of document security; and an API for developers.

However, Safe-T's SDE provides competitive advantages that few if any of its competitors do, including:

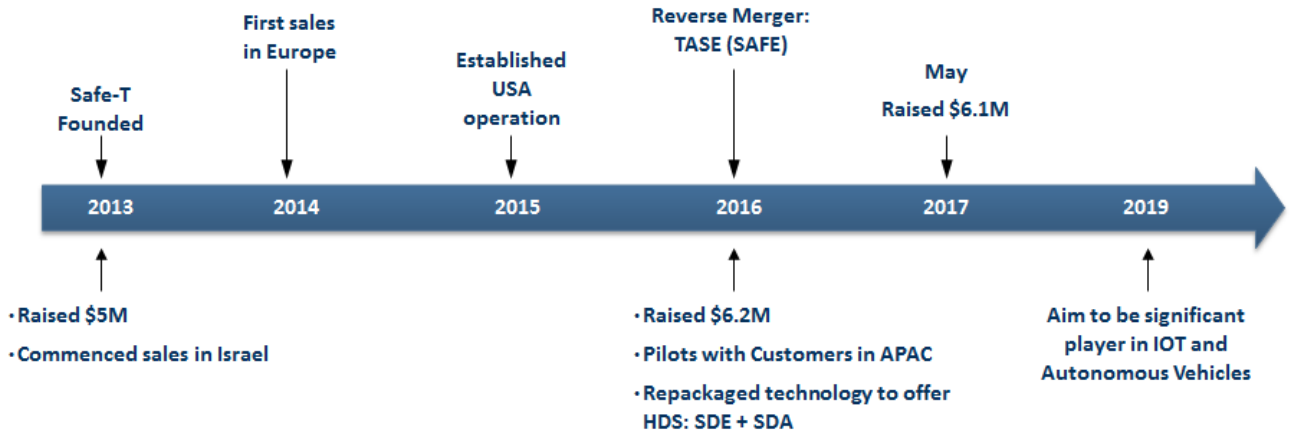
- Storage and access to files in a LAN without opening a firewall
- Connectors
    - Cloud-based storage and applications, including SAP, Salesforce, Dropbox, and Google Drive
    - Out-of-the-box connectors to business storage
    - Out-of-the-box connectors to business applications
    - Out-of-the-box connectors to security solutions
- Vault-to-vault data exchange network
- Secure Cloud Enablement / Cloud Access Security Broker (CASB)
- Ability to define policies for users, groups, and folders
- Integration of work flows
- Outbound and inbound file transfer

Managed File Transfer (MFT) is software/service that manages the secure transfer of data between devices through a network, for example, the Internet. Representative vendors include: Axway, IPSwitch - MOVEit, Seeburger, Attunity, Biscom, Cleo, Egress Software Technologies, Globalscape, Litéra, Infobay, DataMotion, CargoServer, and CyberArk.

Cloud Access Security Broker (CASB) is software/service positioned between an enterprise's infrastructure and that of a cloud provider, and allows the enterprise to apply their security policies to infrastructure that is not on-premises. Representative vendors include: Bitglass, CensorNet, CipherCloud, Cisco CloudLock, FireLayers, Microsoft (Adallom), Netskope, and Skyhigh Networks.

Enterprise File Sync and Share (EFSS) is software/service that securely synchronizes and shares files and data among multiple devices. The EFSS domain is crowded, with more than 100 vendors vying for a share of the revenue. Representative vendors include: Totemo, LeapFile, Brainloop, FileCatalyst, LiquidFiles, Varonis, Citrix, Box, Intralinks, Dropbox, Egnyte, Accellion, Huddle, Microsoft OneDrive for Business, Syncplicity, WatchDox, OpenText, ownCloud, Aspera, and Signiant.

Roadmap



- **During 2015-2016** - Safe-T validated its business model in Israel by securing large customers in the financial, government and health industries
- **During 2016** - established the infrastructure for future sales, focused on indirect sales
- **End-2016** - met with their customers to brainstorm a future strategy, the result leading to the combining and integration of their SDA and SDE offerings
    - Safe-T positions itself as a "factory of technologies" offered to enterprises.
    - During 4Q16, the company repackaged their product to offer one integrated comprehensive solution, and together their SDE and SDA products have evolved into their HDS. Core technology remains unchanged.
- **3-year forward-looking perspective**: aiming to be significant players in these verticals:
    - IoT and associated sensors, as SDA technology can protect this type of communication for example, in smart homes
    - Autonomous vehicles

Financial Analysis

Safe-T's activity was integrated into a shelf corporation in 2016. The company commenced operations in its current legal status on June 15, 2016, and as such its 2016 financial data is incomplete. Safe-T is focused on high-risk data protection with Secure Data Exchange (SDE) and Secure Data Access (SDA), its two primary products, and a third that is a combination of these two products.

The company sells its products on-premises, as-a-service, and via OEM agreements.

- **On-premises solutions** are sold both directly and indirectly. Safe-T provides a virtual machine and end-user licenses, and the end-customer provides the server hardware.
- **Cloud-based "as-a-service" solutions** are sold indirectly through Safe-T's channel partners.
- **OEM agreements** are based on sales of SDA only, for which Safe-T white labels their product.

P&L Analysis

Safe-T's revenues were $177K in 2013, $531K in 2014, $715K in 2015, and $843K in 2016. This growth in revenue is attributed primarily to its USA customers. To date, their main income has been generated in Israel via on-premises solutions (sold as perpetual licenses) to customers that include Haifa University.

Gross margins were similar in 2015 and 2016, 37% and 39%, respectively. This relatively low GM is due to Safe-T being a young company that depends on direct channels to sell their products. Research and Development (R&D) expenses were $177K in 2013, in the range $740K-$800K during 2014-2015, and $1.1 million in 2016, a growth representing Safe-T's investment in its future activity. In our view, General and Administrative (G&A) expenses in 2015-2016 represent a steady state, although marketing expenses are higher in 2016 ($600K higher than in 2015) as the company expands into regions such as Europe and the USA.

Operational loss was $7.3 million in 2016, which includes Reverse Merger and Offering expenses, and non-cash costs resulting from the merger event.

Balance Sheet and Operational Cash Flow Analysis

Safe-T's accountant has provided a warning disclosure, which is currently an on-going concern. The company's cash, as of December 31, 2016, is $1.4 million, and fully funded by its shareholders. As of May 3, 2017, the company has succeeded in raising a total of $4.1 million from private investors, and $2 million from the exercise of warrants. Safe-T equity, as of December 31, 2016, is $1.2 million, similar to 2015. The company's operational cash flow needs are $3.3 million for 2016, an increase from 2015 ($2.4 million) due to higher marketing and R&D expenses.

Comparison to Similar Companies

Safe-T primarily targets the following markets: Managed File Transfer (MFT), Cloud Access Security Broker (CASB), and Software-Defined Perimeter (SDP).

The following publicly-traded companies are operating in Safe-T's markets:

- Axway Software SA (Euronext: AXW.PA) - a France-based company engaged in software development. AMPLIFY, its core product, is a cloud-enabled data integration and engagement platform, which enables businesses to manage their customer experience networks.

- Attunity (NASDAQ: ATTU) - provides Big Data management software solutions that enable access, management, sharing and distribution of data across heterogeneous enterprise platforms, organizations and the cloud. The Company's software solutions include: data replication and distribution (Attunity Replicate, Change Data Capture (CDC), and Attunity Gold Client Solutions), test data management (Attunity Gold Client Solutions), data connectivity (Attunity Connect), enterprise file replication (Attunity RepliWeb), managed-file-transfer (Attunity MFT), data warehouse automation (Attunity Compose), data usage analytics (Attunity Visibility) and cloud data delivery (AttunityCloudBeam).

- Globalscape (NYSE: GSB) - provides secure information exchange capabilities for enterprises and consumers through the development and distribution of software, delivery of managed and hosted solutions, and provisioning of associated services. The Company's primary product is Enhance File Transfer (EFT). Its software products and services include Managed File Transfer Solutions (MFT), Secure Content Mobility Solutions, Wide Area File Services (WAFS), Managed E-Mail Attachment Solution, Consumer-Based File Transfer Solution, and professional services. Its solution portfolio facilitates transmission of critical information, such as financial data, medical records, customer files, vendor files, personnel files, transaction activity and other similar documents.

- CyberArk Software Ltd. (NASDAQ: CYBR) - provides information technology (IT) security solutions that protect organizations from cyber-attacks. The Company's products include Privileged Account Security Solution and Sensitive Information Management Solution. Its Privileged Account Security Solution enables its customers to secure, manage and monitor privileged account access and activities. The Company's Privileged Account Security Solution consists of its Enterprise Password Vault, SSH Key Manager, Privileged Session Manager, Privileged Threat Analytics, Application Identity Manager, Viewfinity and On-Demand Privileges Manager.

Ticker	Market Cap ($M)	Revenues ($M)	R&D expenses ($M)	Employees	Revenues per employee ($K)	R&D expenses per employee ($K)
EPA: AXW	636	284.61	48.162	1,930	147	25
NASDAQ: ATTU	101	54.49	11.139	235	232	47
NYSE: GSB	87	33.34	2.562	854	39	3
NASDAQ: CYBR	1,558	216.61	14.4	644	336	22
Average					**189**	**24**
TASE: SAFE	21	0.8	1.085	34	**25**	**32**

(Data as of December 31, 2016)

The comparison above provides a glance into the company`s operational activity. Safe-T's "revenues per employee" were $23K as of the end of 2016, whereas the average for the four above-mentioned companies is $189K. However, as Safe-T is a young firm, its R&D expenses per employee ($32K), which represent the company's investment in future operations, is higher than the $24K average of these four publicly-traded companies.

According to Israeli regulations, only companies that have been publicly traded for at least a year can be valued by analysts.

Appendices

Appendix A- Financial Reports

P&L	Audited	Audited	Audited	Audited
	$, 000	$, 000	$, 000	$, 000
$, 000	2013	2014	2015	2016
Revenues	177	531	715	843
Cost of revenues	368	503	453	512
Gross profit (loss)	-191	28	262	331
% of Revenues	*-108%*	*5%*	*37%*	*39%*
Research and development expenses	338	742	795	1,085
General and administrative expenses	315	685	2,252	2,123
Marketing expenses	1,220	1,460	2,295	2,892
IPO expenses	0	0	14,012	1,579
Total operating expenses	1,873	2,887	19,354	7,679
Operating loss	-2,064	-2,859	-19,092	-7,348
Financial expenses	-	833	312	1,854
Other financial expenses (income), net	77	-	1,206	282
Total loss	-1,987	-3,692	-18,198	-8,920

Balance Sheet	Audited	Audited
	$, 000	$, 000
Current Assets:	2015	2016
Cash and cash equivalents	62	1,311
Restricted deposits	44	44
Account receivable	633	251
Total current assets	739	1,606
Non-Current Assets:		
PPE, net	60	70
Restricted deposits		13
Goodwill	523	523
Intangible assets	1,266	1,015
Total non-current assets	1,849	1,621
Total Assets	2,588	3,227
Current Liabilities:		
Loans	314	63
Accounts payables and others	967	891
Total current liabilities	1,281	954
Non-Current Liabilites:		
Warrants	0	1,038
Loans to Chief scientist (Israel)	24	63
Total Liabilities	1,305	2,055
Equity	1,283	1,172

Appendix B – Management & Top Shareholders

Safe-T's top shareholders are Amir Mizhar with 32.88% and Kibbutz Sasa with 21.49%. 54.37% are public holdings.

Amir Mizhar - Founder and Chairman: prior to founding Safe-T, Amir founded and led eTouchware. As founder and CEO of M-Technologies, Amir led the vision and creation of online collaboration tools, and online merchandising systems for retail markets. Developing commercial software programs since the age of 13, Amir is an expert ethical hacker and currently holds multiple patents in the area of data transfer over communication networks.

Shachar Daniel - Co-Founder and CEO: responsible for Safe-T's overall vision, company strategy, daily operations, and growing the company's business and presence around the world. Shachar brings over 10 years of managerial experience in in operations and project management. Prior to joining Safe-T, he was Program Manager at Prime-sense, Head of Operations Project Managers at Logic, and Project Manager at Elbit systems.

Derek Schwartz - CEO Safe-T North America: over 25 years of leadership experience in global organizations delivering solutions to Enterprises. Derek brings executive experience with Mission Critical Secure Data Transmissions at Cyclone Commerce, Axway and SEEBURGER as well as merging in acquisitions such as Tumbleweed. Derek's networks stems from living, working and building businesses in Canada, United Kingdom, Europe, USA, Asia and South Africa.

Shai Avnit - CFO: leads Safe-T's financials affairs including taxation, accounting, budgeting, cash flows and financing. He has extensive experience in managing financial, operational, administrative and legal affairs in companies within the medical device, consumer electronics and software fields. He served as a CFO at both public and private hi-tech companies, including Card Guard Scientific Survival (currently LifeWatch), Valor Computerized Systems, ProSight, and BriefCam.

Eitan Bremler - Co-founder and Vice President, Marketing and Product Management: responsible for Safe-T's global marketing and product management activities, including product strategy and roadmap, product marketing, positioning, go-to-market strategy, and corporate marketing. Eitan has over 15 years' experience in marketing, product marketing and product management roles, including at Radware and Radvision (an Avaya company). Prior to working for the RAD group, he served as an officer in Unit 8200, an Israeli Intelligence Corps unit.

Jorge Gerber - Vice President of Sales, Rest of the World: an experienced Networking and Cyber Security solutions sales executive, he has been a key player in successful technology endeavors for over 25 years. Prior to joining Safe-T, Jorge led the Virtualization & Security Business at Hewlett-Packard Israel. He was also Founder and Managing Director of Sweetspot, a consulting firm that matches technology startups with investors and strategic alliances, and a founding member of Radware, in the roles of VP Sales EMEA and VP Strategic Alliances.

Yossi Carmon- Vice President of Sales, Middle East and Africa: over 20 years' experience in developing and selling application, networking and cybersecurity solutions to the healthcare, finance and overmanned markets. Prior to joining Safe-T, Yossi held multiple R&D, sales, and project management positions in global companies including IBM Israel. Yossi is a veteran of the Israel Defense Forces Cyber Unit.

Appendix C – Frost & Sullivan Analyst Team

Kobi Hazan is the Lead Analyst at Frost & Sullivan Research & Consulting Ltd., a subsidiary of Frost & Sullivan in Israel. He has over 14 years of experience in capital markets, including research, analysis, investment advisory, and management. Mr. Hazan served as a Fund Manager for provident and mutual funds at Analyst Ltd. and, since 2012, he owns and manages the Amida Israel Fund, a hedge fund specializing in Israeli equities. Kobi holds an Economics and Management degree from The College of Management Academic Studies. He is licensed as an Investment Advisor in Israel.

Jarad Carleton is a Principal Consultant and Analyst at Frost & Sullivan, with over 16 years of strategy consulting for the Fortune 500 and Global 1000 in North America, Latin America, Europe, and Asia Pacific. Jarad has led high profile strategic projects with leading firms including: Intel Security Group, CTIA Cyber Security Working Group, NRI Secure Technologies, and (ISC)². He earned his MBA in International Management from Thunderbird, School of Global Management, in Arizona.

Revital Rauchwerger is an Analyst and Consultant at Frost & Sullivan in Israel, and part of the Global Information and Communication Technologies team. Her professional experience spans Venture Capital investments to executive positions in Corporate Strategy, Product Management, and Product Marketing. Throughout the years, she has volunteered as a mentor and advisor to entrepreneurs and start-ups. Revital earned her MBA from Tel Aviv University.

Dr. Tiran Rothman is an Analyst and Consultant at Frost & Sullivan Research & Consulting Ltd., a subsidiary of Frost & Sullivan in Israel. He has over 10 years' experience in research and economic analysis of capital and private markets, obtained through positions at a boutique office for economic valuations, as chief economist at the AMPAL group, and as co-founder and analyst at Bioassociate Biotech Consulting. Dr. Rothman also serves as the Economics & Management School Head at Wizo Academic College (Haifa). Tiran holds a PhD in Economics, MBA (finance), and was a visiting scholar at Stern Business School, NYU.

Disclaimers & Disclosures

Definitions: **"Frost & Sullivan**" – a company registered in California, USA with branches and subsidiaries in other regions, including in Israel, which includes any other relevant Frost & Sullivan entities, such as Frost & Sullivan Research & Consulting Ltd. **"The Company"** or "**Participant"** – the company that is analyzed in the Report (as defined herein) and participates in the TASE Program. **"Report"**, "**Research Note"** or **"Analysis"** – the contents and any part thereof where applicable, contained in a document such as the Research Note and/or any other previous or subsequent document the author of which is Frost & Sullivan, regardless as to whether or not it has been authored within the framework of the "Analysis Program", if included in the database set out in www.frost.com and regardless of the Analysis format-online, whether a digital file or hard copy **;**
"Invest", "**Investment**" or "**Investment Decision"** – any decision and/or a recommendation to Buy, Hold or Sell any security of the Company .

General: The purpose of this Report is to enable its reader to make a more informed Investment Decision. However, nothing in the Report shall constitute a recommendation or solicitation to make any Investment Decision, and accordingly, Frost & Sullivan assumes no responsibility and shall not be deemed responsible for any specific decision, including an Investment Decision, and will not be liable for any actual, consequential, or punitive damages, whether directly or indirectly relating to the Report. Without derogating from the generality of the above, you shall consider the following clarifications, disclosure recommendations and disclaimers. The Report does not include any personal advice or advice of a personalized nature, given that it cannot consider the particular investment criteria, needs, preferences, priorities, limitations, financial situation, risk aversion, and any other particular circumstances and factors that shall impact an investment decision. Frost & Sullivan neither provides any warranty nor makes any representation, express or implied, as to the completeness and accuracy of the Report at the time of any investment decision, and no liability shall attach thereto, in view of the following, among other reasons**: the Report may not include the most updated and relevant information from all relevant sources**, including subsequent Reports, if any, at the time of the investment decision. **Accordingly, any investment decision shall take this into account**; The Analysis considers data, information and assessments provided by the Company and from sources that were published by third parties (however, even reliable sources contain, from time to time, unknown errors); The aim of the methodology set out in the Analysis is to focus on major known products, activities and target markets of the Company that may have a significant impact on its performance based upon our discretion. It should be noted that the methodology may ignore other elements, including the fact that the Company was not allowed to share any inside information; Any investment decision must be based on a clear understanding of the technologies, products, business environments, and any other drivers and restraints of the Company's performance, regardless as to whether or not such information is mentioned in the Report. In this regard, an investment decision shall consider any relevant updated information, such as the Company's website and reports on ISA's website ("**Magna**"). Information and assessments contained in the Report are obtained from sources believed by us to be reliable (however, it should be noted that any source may contain unknown errors). All expressions of opinions, forecasts or estimates reflect the judgment at the time of writing, based on the Company's latest financial report, and some additional information (which are subject to change without any notice). Accordingly, you shall consider the entire analysis contained in the Report. No specific part of the Report, including any summary that is provided for convenience only, shall serve as a basis for any investment decision. In case you perceive a contradiction between any parts of the Report, you shall avoid any investment decision until such contradiction is resolved .

Risks, valuation and projections: Any stock price or equity value referred to in the Report may fluctuate. Past performance is not indicative of future performance, future returns are not guaranteed, and a loss of original capital may occur. Nothing contained in the Report is, or should be relied on as a promise or representation as to the future. The projected financial information is prepared expressly for use herein and is based upon the stated assumptions and Frost &Sullivan's analysis of information available at the time at which this Report was prepared. There is no representation, warranty, or other assurance that any of the projections will be realized. The Report contains forward-looking statements, such as" anticipate", "continue", "estimate", "expect", "may", "will", "project". "should", "believe", and similar expressions. Undue reliance should not be placed on the forward-looking statements given that that there is no assurance that they will prove to be correct. Since forward-looking statements address future events and conditions, they involve inherent risks and uncertainties. Forward-looking information or statements contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results to be materially different from current projections. Macro level factors that are not directly analyzed in the Report, such as interest rates and exchange rates, any events related to the eco-system, clients, suppliers, competitors, regulators and others may fluctuate at any time. An investment decision must consider the risks implied or **described in the Report** and any other relevant Reports, if any, including the latest financial reports of the Company. R&D activities shall be considered as high risk, even if such risks are not specifically discussed in the Report. Any investment decision shall consider the impact of negative and even worst case scenarios.

Agreement with the Tel Aviv Stock Exchange: The Report was authored by Frost & Sullivan Research & Consulting Ltd. (**"Frost Consulting"**) within the framework of an Agreement between Frost Consulting and the Tel Aviv Stock Exchange (the **"Agreement"** and "**TASE",** respectively**)**. The Agreement was signed as part the TASE analysis Program. The Agreement with the Tel-Aviv Stock Exchange Ltd. regarding participation in the Program for research analysis of public companies does not and shall not constitute an agreement on the part of the Tel-Aviv Stock Exchange Ltd. or the Israel Securities Authority to the content of the Research Notes. The purpose of the Program is for the activity of Technology and Biomed (Healthcare) companies, which are registered on the TASE, to be made known to investors in Israel and outside of Israel, by means of the analysis performed, *inter alia*, by Frost Consulting [more and updated information regarding the Program can be found at www.tase.co.il . Such analyses will be in respect of the Participants. According to the Agreement, Frost Consulting Ltd. is entitled to an annual fee to be paid directly by the TASE. The fee shall be in the range of USD 35 to 50 thousand for each participant. Each Participant shall pay the fee for its participation in the Program directly to the TASE. A summary of the Report shall also be published in Hebrew. The Report shall include a description of the Participant and its business activities, which shall inter alia relate to matters such as: shareholders; management; products; relevant intellectual property; the business environment in which the Participant operates; the Participant's standing in such an environment including current and forecasted trends; a description of past and current financial positions of the Participant; a forecast regarding future developments; and any other matter which, in the professional, view of Frost & Sullivan (as defined below) should be addressed in a research Report (of the nature published) and which may affect the decision of a reasonable investor contemplating an investment in the Participant's securities. To the extent it is relevant, the Analysis shall include a schedule of scientific analysis by an expert in the field of life sciences. An equity research abstract shall accompany each Equity Research Report, describing the main points addressed. A thorough analysis and discussion will be included in Reports where the investment case has materially changed. Short update notes, in which the investment case has not materially changed, will include a summary valuation discussion. The Equity Research Reports shall be distributed through various channels.

Company Details: Name of the Licensed Company: Frost & Sullivan Research & Consulting Ltd.; Address: Abba Eban 1, Herzliya, PO Box 12495; Phone Number: +972 (0) 9-9502888

Disclosure Paragraph pursuant to the addendum to the Directive: I, Kobi Hazan, in whose name license number 6097 is registered, certify that the views expressed in the Report accurately reflect my personal views about the Company and its securities, and that no part of my compensation was, is, or will be directly or indirectly related to the specific recommendation or view contained in the Report. Neither the analyst nor Frost & Sullivan trade or directly own any securities in the Company.