safe-t
Masters of Access

Safe-T Secure Application Access

Competitive Analysis
February 2020

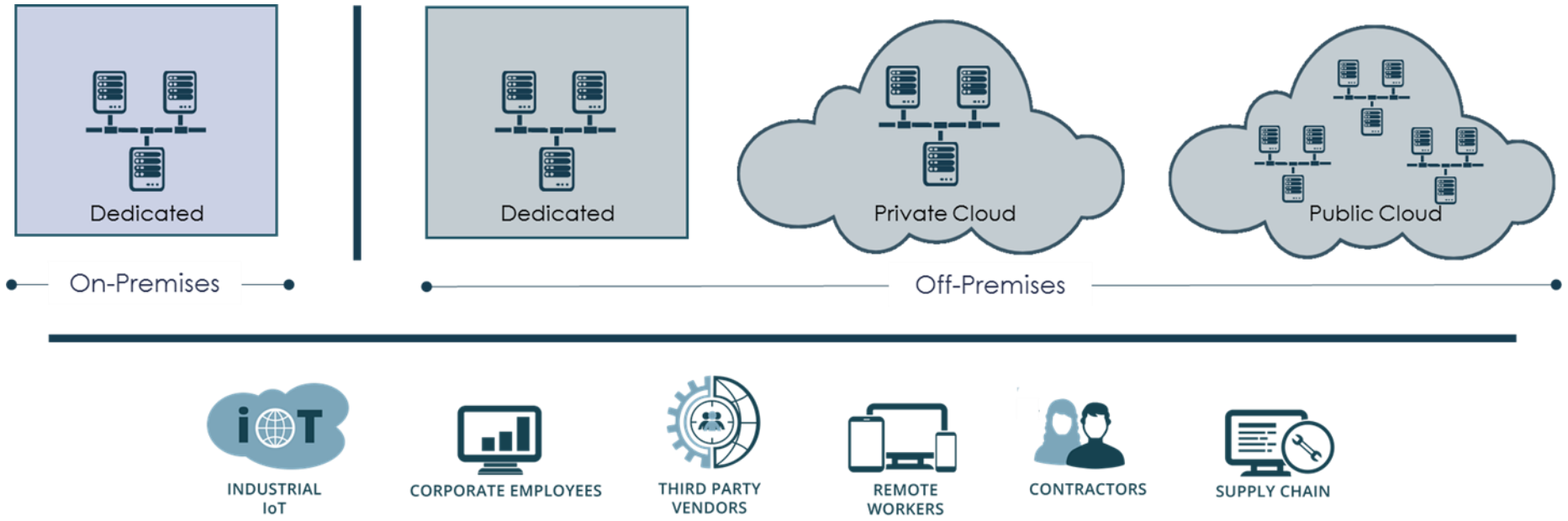
Name of presenter | Position

Our Main Software Define Perimeter (SDP) Competitors

- Zscaler
- Akamai
- Appgate (was Cyxtera)
- Symantec (was Luminate)
- Meta Networks
- Perimeter 81
- Pulse Secure

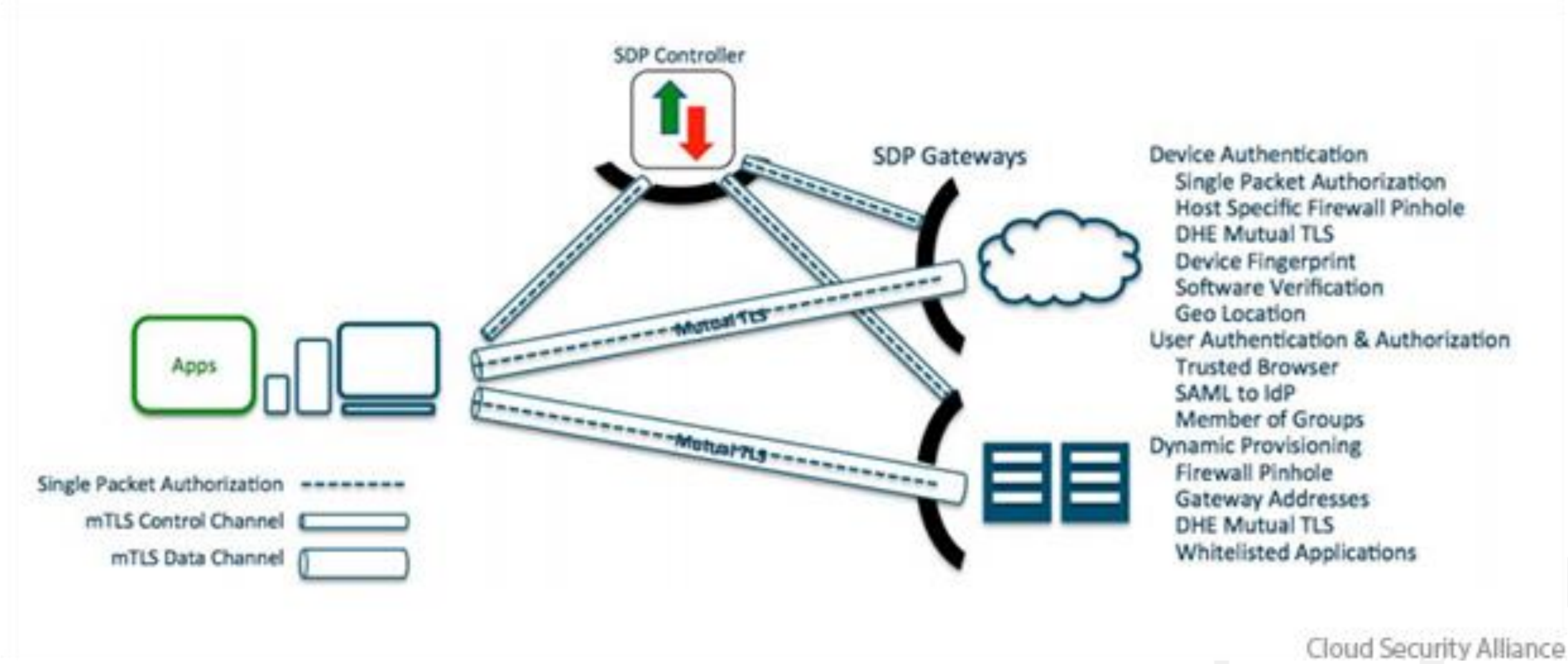
IT in the World of Digital Transformation

Services are widely distributed among cloud and data center infrastructures



- Multiple platforms, tools, teams, users
- No single policy, view, or enforcement point
- End result: Complexity

Software Defined Perimeter Architecture



Competition

CLIENT

Positives
- Strong authentication and encryption
- Device authentication, mitigates credential theft

Negatives
- Precludes some 3rd party's devices
- Prevents App-App and IoT use-cases

CLIENTLESS

Positives
- Enables 3rd party access where a client can't be added to device
- Easy to deploy
- Supports App-App and IoT use-cases

Negatives
- Prevents end-point posture checks**
- May cause shared IP access issues

**** Safe-T utilizes built-in OS L2TP client***

***** Can be achieved by 3rd party***

SaaS	On-premises solution	AWS solution
Positives • Easy to deploy • Lower cost • Remote access to cloud apps without local net access **Negatives** • Local users must access web to uses local apps • Access to local identity solution requires opening the FW	**Positives** • Local users don't leave network to access local apps • No networking considerations • Fits regulated organizations **Negatives** • Cloud access is routed via on-premise solution • More complicated to deploy than SaaS	**Positives** • Easy deployment in AWS • Fits cloud-based organizations **Negatives** • Cloud access is routed via AWS • More complicated to deploy than SaaS
Zscaler AppGate (Cyxtera) Symantec Proofpoint Perimeter81 Odo **Safe-T (Hybrid-service)***	AppGate (Cyxtera) Pulse Secure **Safe-T***	Zscaler AppGate (Cyxtera) Perimeter81 Pulse Secure **Safe-T***
Zscaler Akamai Symantec Proofpoint Perimeter81 Odo **Safe-T (Hybrid-service)**	Pulse Secure **Safe-T**	Zscaler Cyxtera Perimeter81 Pulse Secure **Safe-T**

Market Activity

- Strong messaging, aggressive sales and marketing
- Strong channel program
- Focus on market education: Webinars, strong content and web site

Strategic Considerations

Strategy is to enable secure migration to the cloud with the vision "the internet is the new network." Traditionally focused on secure web access, secure access to application in the cloud is a natural extension. Zscaler Private Access is a strategic component of the corporate growthy strategy.

Positioning

Secure Remote Access to the Cloud Positioned relative to legacy VPN

- A better experience for remote users
- Less complexity for administrators/Simplicity
- Easy to implement and administer
- Secure remote access to internal apps – More Secure
- Increased business value – Acquisition and operating cost
- Accelerated adoption of cloud initiatives

zscaler

safe-t

Deployment:
Saas

Who deploys:
Customer and SaaS (have excellent online documentation)

Competitive Strength
- Sales and marketing engine
- Channel
- Strong brand
- Financial resources
- Large installed base of web access clients
- 3rd party product integrations
- Management console for configuration and policy management, monitoring and reporting

Product Strengths
- Maturity: product deployed by customers today
- Management console for creating and maintaining policy, entitlements, filters, and monitoring usage. Flexibility and configurability.
- Can allow administrative and command line access to network services
- Easy to deploy

Product Limitations
- User centric, not applicable to app-app, connected devices
- Ability to deploy in data center. They say they can do it, but this is not where they play
- IdP integration. They've integrated OKTA. Others limited, maybe on roadmap
- No user behavior analysis
- Client and Client-less options

Feature	Safe-T Secure Application Access	Zscaler Private Access
Client / Client-less	Client-less, IPSEC tunnel	Client-based and Client-less
Deployment	Solution, MSSP, Hybrid-service	SaaS
Outbound connections	Yes, Safe-T has reverse-access patent	Yes, but not a true reverse access
Supported user type	Human, application, API, IOT device	Human only
Supported applications	Web, RDP, Any TCP, Webdav (CIFS replacement), SSH	Web, RDP
Authentication workflow	Yes	No
Support external IdP	Yes	Yes
Support On-premises Active Directory	Yes	Yes, but requires opening the firewall for Zscaler to connect
Full L7 Proxy	Yes	No
SSL Offload done on-premises	Yes	No, keys are provided to Zscaler
User Behavior Analysis and Anomaly Detection	Yes	No
Application discovery	No	Yes
End-user machine posture checks	No	No

Market Activity

- Favor selling over Marketing
- Outbound - little marketing promotion beyond events
- Limited SEO and outside published content

Strategic Considerations

Akamai's core media delivery business is declining; enterprise security is the growth driver. Within enterprise security Akamai is expanding its portfolio from protecting websites from DDoS attacks to securing assets, both endpoints and applications. Their focus in the cloud, not on on-premise.

Positioning

DMZ-as-a-Service Positioned against VPN, RDP, and proxies

- Increased security – secure access delivery
- Exceptional User Experience
- East to deploy – deploy once, protect everywhere
- Lower TCO - zero CapEx, low OpEx model

safe-t

Akamai

Deployment: Saas **Who deploys:** Customer and SaaS (have excellent online documentation)	**Competitive Strength** ✚ Financially, technically strong ✚ Broader portfolio of cloud security solutions ✚ Large, established customer relationship for CDM ✚ Audit and monitoring ✚ Large, in place sales organization ✚ Free trail demo ✚ Strong brand ✚ Financial resources ✚ Management console for monitoring, alerting, and reporting
Product Strengths ✚ Client-less ✚ Maturity: product deployed by customers today ✚ Management console for and monitoring, alerting, and usage. ✚ Easy to deploy: Deploy once, protect anywhere ✚ Direct to cloud without entering corporate network	**Product Limitations** ✚ User centric, not suited to app-app, connected devices ✚ Ability to deploy in data center. They say they can do it, but this is not where they play ✚ IdP integration. They've integrated OKTA, DUO. Others limited, maybe on roadmap ✚ No user behavior analysis

Feature	Safe-T Secure Application Access	Akamai Enterprise Application Access
Client / Client-less	Client-less, IPSEC tunnel	Client-less
Deployment	Solution, MSSP, Hybrid-service	SaaS
Outbound connections	Yes, Safe-T has reverse-access patent	Yes, but not a true reverse access
Supported user type	Human, application, API, IOT device	Human only
Supported applications	Web, RDP, Any TCP, Webdav (CIFS replacement), SSH	Web only
Authentication workflow	Yes	No
Support external IdP	Yes	Yes
Support On-premises Active Directory	Yes	Yes, but requires opening the firewall for Akamai to connect
Full L7 Proxy	Yes	No
SSL Offload done on-premises	Yes	No, keys are provided to Akamai
User Behavior Analysis and Anomaly Detection	Yes	No
Application discovery	No	No
End-user machine posture checks	No	No

APPGATE

Market Activity

- Strong messaging, aggressive sales and marketing
- Focus on thought leadership, market education
  - Speaking, webinars, social, content
  - Strong spokespeople

Strategic Considerations

Focused on hybrid cloud. AppGate bridges public cloud and private cloud. Corporate strategy: sell clients AppGate for public cloud, then use as the bridge to sell the Cyxtera as a private cloud solution. Their focus is on cloud deployments, not on-premise

Positioning

A Software Defined Perimeter positioned against VPN, firewall, and NAC

- A solution for complex hybrid IT environment (with a focus on cloud and migration to cloud)
- Better secure access
- Simplifies network configuration and reduced operational effort (Lower TCO)
- Consistent access policy across environment
- Human and IOT use cases

APPGATE

Deployment:
Infrastructure Deployed
VM or appliance on-premise, VM in cloud, SaaS

Who deploys:
Customer deployed

Competitive Strength

- Sales and marketing engine
- Tie to Cyxtera private cloud strategy
- Management console: Flexibility and configurability at the cost of complexity
- Session allows simultaneous multi-service access – once authenticated, can be simultaneously connected to multiple services/applications
- Developer, administrator, and user level access
- Transparent MFA
- Strong encryption
- Enables migration of IT to the cloud
- FREE trial demo
- Tied to AWS and Azure

Product Strengths

- Maturity: product deployed by customers today
- Management console for creating and maintaining policy, entitlements, filters, and monitoring usage. Flexibility and configurability.
- Can allow administrative and command line access to network services
- Human and IOT use cases

Product Limitations

- Gateway installed behind network firewall, not deployable deeper in a network (i.e., within nested VLANs)
- Establishes connection by opening/ closing INBOUND firewall pin holes. AppGate may not be compatible with some legacy firewalls, requiring the customer to uplift their infrastructure
- Not suited to app-app
- No user behavior analysis

Symantec.

Market Activity

- Strong messaging, aggressive sales and marketing
- Focus on thought leadership, market education
  - Speaking, webinars, social, content
  - Strong spokespeople

Strategic Considerations

Focused on human access to corporate resources in the cloud or on-premises.

Positioning

A Software Defined Perimeter positioned for the following use cases:

- VPN replacement - Replace traditional VPNs and DMZ with cloud-native point-to-point access
- 3rd party and BYOD - Connect any user, from any device to the corporate applications in a secure and easy to manage manner
- DevOps access - Enable the engineering teams to securely leverage the agility and speed of the cloud

Symantec

Deployment:
SaaS

Who deploys:
Customer and SaaS

Competitive Strength
- Symantec back for financing, sales and marketing
- Easily deployed
- Transparent MFA
- Enables migration of IT to the cloud
- Connection to corporate messaging systems for reporting within IT
- Tied to AWS and Azure
- Very nice reporting

Product Strengths
- Client-less and Client-based
- Cloud solution, deployed very fast
- Integration with AWS, Azure, GCP
- Can track user actions
- Full L7 proxy in the cloud

Product Limitations
- No support for native RDP, SFTP, NTFS
- Complex support for native TCP
- User-centric. Not suited to app-app, connected devices
- No user behavior analysis
- Not sold stand-alone, only as part of cloud

Feature	Safe-T Secure Application Access	Symantec Secure Access Cloud
Client / Client-less	Client-less, IPSEC tunnel	Client-less, Client-based
Deployment	Solution, MSSP, Hybrid-service	SaaS, Versions for AWS and Azure
Outbound connections	Yes, Safe-T has reverse-access patent	Yes
Supported user type	Human, application, API, IOT device	Human only
Supported applications	Web, RDP, Any TCP, Webdav (CIFS replacement), SSH	Web, SSH
Authentication workflow	Yes	No
Support external IdP	Yes	Yes
Support On-premises Active Directory	Yes	Yes
Full L7 Proxy	Yes	Yes
SSL Offload done on-premises	Yes	NA
User Behavior Analysis and Anomaly Detection	Yes	No
Application discovery	No	Yes
End-user machine posture checks	443, IPSEC	443, 22

Meta Networks

safe-t

Market Activity

- Strong messaging and marketing
- Focus on thought NaaS and SDP leadership, market education

Strategic Considerations

- Focused on human access to corporate resources in the cloud or on-premises.
- Targeting to become a complete cloud based network providing quick access to corporate resources from anywhere in the globe.

Positioning

A Software Defined Perimeter positioned for the following use cases:

- Secure Remote Access
- Always-on VPN alternative
- Beyondcorp for Enterprise
- Zero-Trust Network Access
- Cloud-Delivered Network Security and Access
- Multi Cloud Connectivity and Security

Meta Networks

safe-t

Deployment:
SaaS

Who deploys:
Customer and SaaS

Competitive Strength
- Proofpoint back for financing, sales and marketing
- Easily deployed
- Large number of locations world wide
- Very nice reporting

Product Strengths
- Client, Client-less
- Cloud solution, deployed very fast
- 30 pops around the world
- MetaNetworks service works like a SD-WAN, capable of routing user traffic within the service's network to reach closest exit point to customer network

Product Limitations
- No support for native NTFS
- Native protocols require a client
- Requires synchronizing user credentials with MetaNetworks cloud
- No user behavior analysis

Meta Networks

safe-t

Feature	Safe-T Secure Application Access	Meta Networks Meta NaaS
Client / Client-less	Client-less, IPSEC tunnel	Client, Client-less
Deployment	Solution, MSSP, Hybrid-service	SaaS
Outbound connections	Yes, Safe-T has reverse-access patent	Yes
Supported user type	Human, application, API, IOT device	Human, application
Supported applications	Web, RDP, Any TCP, Webdav (CIFS replacement), SSH	Web, RDP, Any TCP, SSH
Authentication workflow	Yes	No
Support external IdP	Yes	Yes
Support On-premises Active Directory	Yes	Yes
Full L7 Proxy	Yes	No
SSL Offload done on-premises	Yes	NA
User Behavior Analysis and Anomaly Detection	Yes	No
Application discovery	No	No
End-user machine posture checks	443, IPSEC	443, IPSEC

perimeter 81

safe-t

Market Activity

- Strong messaging and marketing, especially re-marketing and social
- Gartner cool vendor

Strategic Considerations

- Perimeter81 service works like a cloud VPN, connecting the user into the corporate network
- Solution is client based, designed for humans.

Positioning

A Software Defined Perimeter positioned for the following use cases:

- Secure Remote Access
- Always-on VPN alternative
- Beyondcorp for Enterprise
- Zero-Trust Network Access
- Cloud-Delivered Network Security and Access
- Multi Cloud Connectivity and Security

perimeter 81

safe-t

Deployment:
SaaS

Who deploys:
Customer and SaaS

Competitive Strength
- Easily deployed
- Large number of locations world wide
- Very nice reporting

Product Strengths
- Client, client-less is on roadmap
- Cloud solution, deployed very fast
- Multiple cloud locations

Product Limitations
- No support for native NTFS
- User-centric. Not suited to app-app, connected devices
- No user behavior analysis
- User is connected to the network

Feature	Safe-T Secure Application Access	Perimeter81
Client / Client-less	Client-less, IPSEC tunnel	Client, Client-less in roadmap
Deployment	Solution, MSSP, Hybrid-service	SaaS
Outbound connections	Yes, Safe-T has reverse-access patent	Yes
Supported user type	Human, application, API, IOT device	Human, application
Supported applications	Web, RDP, Any TCP, Webdav (CIFS replacement), SSH	Web, RDP, Any TCP, SSH
Authentication workflow	Yes	No
Support external IdP	Yes	Yes
Support On-premises Active Directory	Yes	Yes
Full L7 Proxy	Yes	No
SSL Offload done on-premises	Yes	NA
User Behavior Analysis and Anomaly Detection	Yes	No
Application discovery	No	No
End-user machine posture checks	443, IPSEC	443, IPSEC

Market Activity

- Strong messaging and marketing
- Pushing hard on up-sale to existing customers

Strategic Considerations

- Designed to add SDP capabilities to existing VPN deployments
- Provides PulseSecure a Zero Trust play
- Solution is client based, designed for humans.

Positioning

A Software Defined Perimeter positioned for the following use cases:

- Per-application Segmentation in Data Center & Private Cloud
- Privileged and 3rd Party Access to Applications from Anywhere
- Direct, Secure Access to Public Cloud Applications

Pulse Secure

safe-t

Deployment:
On-premises, AWS/Azure Market place

Who deploys:
Customer

Competitive Strength
- Fully integrated with Pulse Secure VPN
- Large number of locations world wide
- Large number of existing VPN customers

Product Strengths
- Client and client-less
- Fast deployment side-by-side Pulse Secure VPN

Product Limitations
- Requires client for native RDP, SSH, SFTP, NTFS, TCP
- User-centric. Not suited to app-app, connected devices
- No user behavior analysis
- Requires opening the firewall
- Cannot work with existing VPN

Feature	Safe-T Secure Application Access	Pulse Secure
Client / Client-less	Client-less, IPSEC tunnel	Client, Client-less
Deployment	Solution, MSSP, Hybrid-service	Solution, AWS/Azure Market place
Outbound connections	Yes, Safe-T has reverse-access patent	No, requires opening the firewall
Supported user type	Human, application, API, IOT device	Human
Supported applications	Web, RDP, Any TCP, Webdav (CIFS replacement), SSH	Client-less – Web, RDP over HTTP Client - RDP, Any TCP, SSH, SFTP, etc
Authentication workflow	Yes	No
Support external IdP	Yes	Yes
Support On-premises Active Directory	Yes	Yes
Full L7 Proxy	Yes	No
SSL Offload done on-premises	Yes	Yes
User Behavior Analysis and Anomaly Detection	Yes	No
Application discovery	No	No
End-user machine posture checks	443, IPSEC	443, IPSEC

Stated Target Use Cases

	zscaler	Akamai	APPGATE	Symantec.	Meta Networks	perimeter 81	Pulse Secure	safe-t
Secure Access: Cloud and On-Premise	X	X	X	X	X	X	X	X
Cloud Migration	X	X	X	X	X	X		X
Secure Access: Server			X				X	X
3rd Party / Privileged User Access	X	X	X	X	X	X	X	X
VPN Replacement	X		X	X	X	X		X
M & A / IT Integration	X			X				X
App - App					X	X		X
Connected devices			X					X

Thank you

safe-t