

Versatility 2024

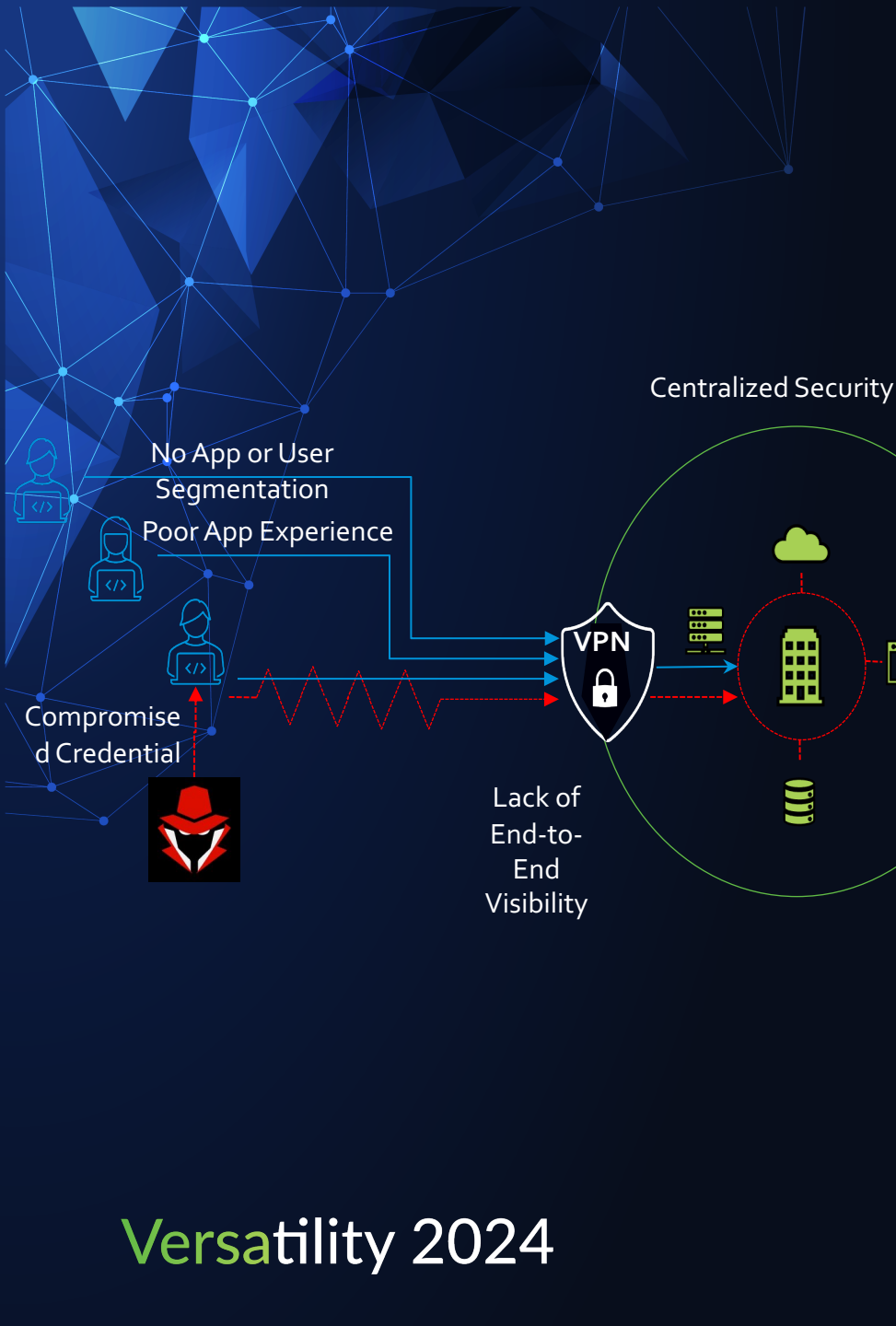
Stopping Cyber Threats with Zero Trust Network Access



Agenda

- Legacy VPN challenges
- Zero Trust framework
- Versa ZTNA
- Components of Versa ZTNA
- Use Cases
- Industry validation – Cyberratings
- One more thing

The diagram illustrates the limitations of Centralized Security and the need for Versatility 2024. It features a dark blue background with a network of white lines and dots. On the left, three user icons (labeled 'No App or User Segmentation' and 'Poor App Experience') are connected to a central shield icon labeled 'VPN'. A red dashed line with a jagged waveform, labeled 'Compromised Credential', points to the VPN shield. Below this, a red and black icon of a person with a red mask is shown. To the right, a large green circle labeled 'Centralized Security' contains a building icon, a cloud icon, and a server rack icon. A red dashed line connects the VPN shield to the building icon. Below the VPN shield, the text 'Lack of End-to-End Visibility' is displayed. At the bottom, the text 'Versatility 2024' is written in a large, bold, white font.



-
- The diagram illustrates the limitations of Centralized Security and the need for Versatility 2024. It features a dark blue background with a network of white lines and dots. On the left, three user icons (labeled 'No App or User Segmentation' and 'Poor App Experience') are connected to a central shield icon labeled 'VPN'. A red dashed line with a jagged waveform, labeled 'Compromised Credential', points to the VPN shield. Below this, a red and black icon of a person with a red mask is shown. To the right, a large green circle labeled 'Centralized Security' contains a building icon, a cloud icon, and a server rack icon. A red dashed line connects the VPN shield to the building icon. Below the VPN shield, the text 'Lack of End-to-End Visibility' is displayed. At the bottom, the text 'Versatility 2024' is written in a large, bold, white font.

Digital Transformation Requires Modernization of Legacy VPN Infrastructure

Anywhere, Anytime Access is the New Normal

- **Post Pandemic, hybrid work is the future**
 - No specific office or geographical location

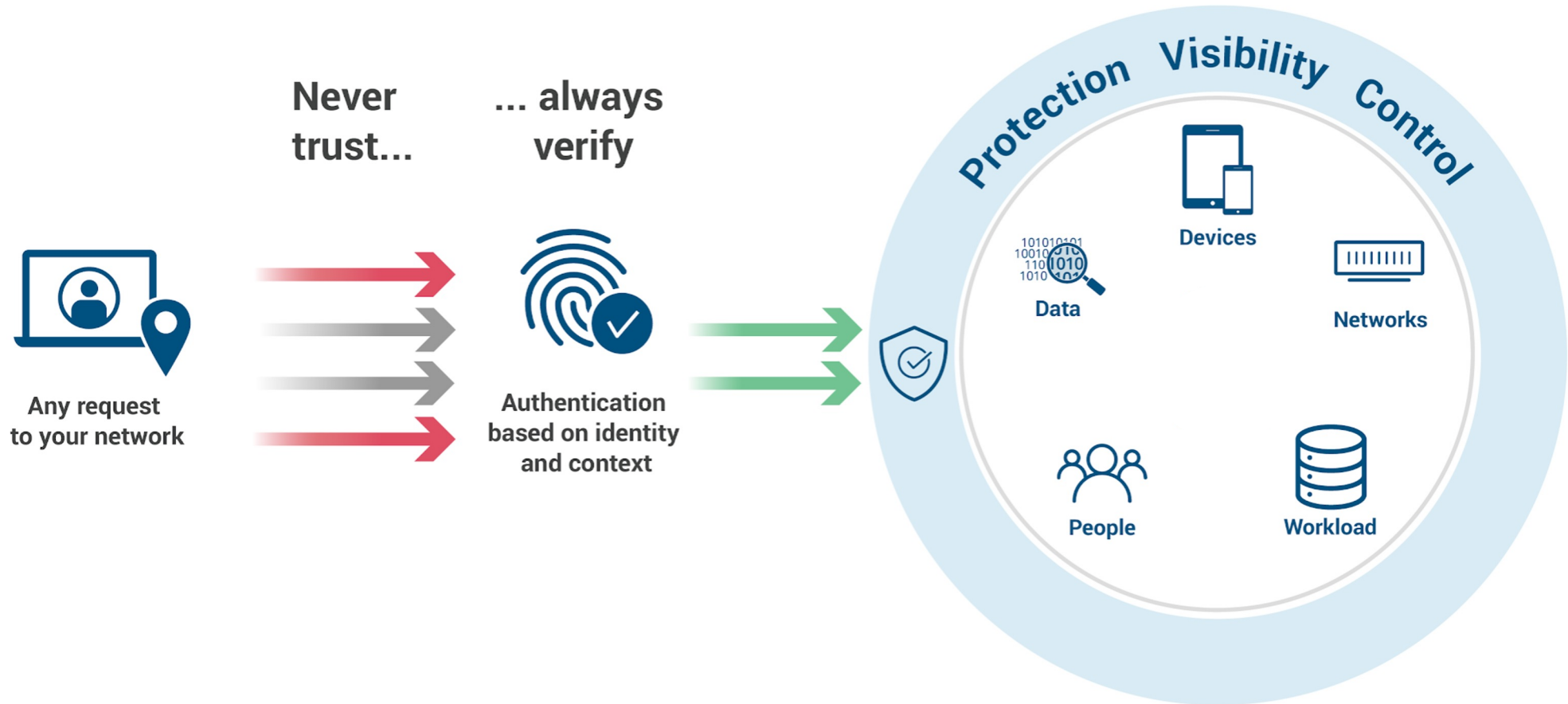
- **Users want fast, seamless access from anywhere**
 - Flawless connectivity experience to corporate applications, on-prem or cloud

- **Enterprise IT wants to manage hybrid access without impacting user experience**
 - Authenticate and control user access to applications, regardless of device or location
 - Increase operational efficiency, reduce complexity and costs

- **Legacy Firewalls/VPNs not built to support modern business models**
 - Increased cybersecurity risk with expanded attack surface
 - Lost productivity and poor user experience due to latency/backhauling of traffic

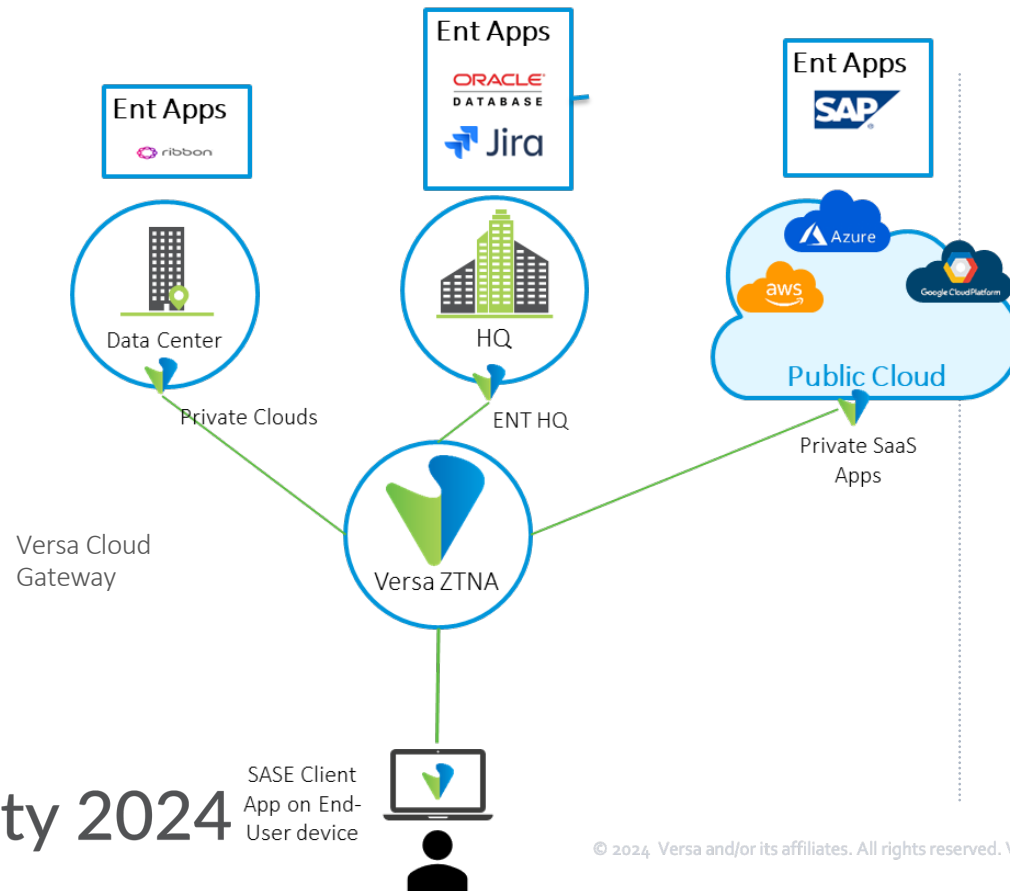


Zero Trust Framework for a Hybrid Workforce



Versa Zero Trust Network Access

Versa ZTNA is an easy to deploy, Zero Trust based secure access solution that fits into your existing environment



Versa ZTNA Highlights

- Direct, secure per-application access to enterprise applications
- Zero Trust framework for user and device authentication and verification, with granular least privilege access policies
- Continuous security posture assessment with adaptive access control and remediation
- Reduced attack surface with “dark cloud”
- Data loss and malware prevention
- Exceptional user experiences for employees

Versatility 2024

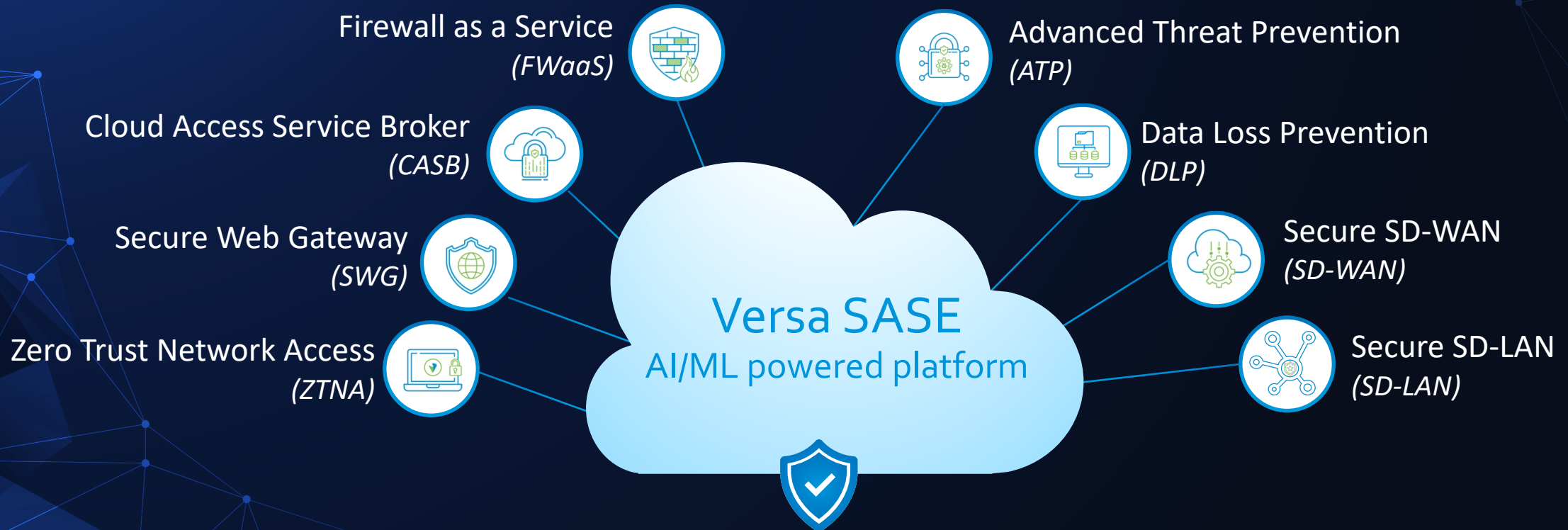
SASE Client
App on End-
User device

© 2024 Versa and/or its affiliates. All rights reserved. Versa Networks Confidential



Versa Unified SASE

AI/ML powered platform



Versatility 2024

Users

Users

Branches

Private Cloud

Public Cloud

© 2024 Versa and/or its affiliates. All rights reserved. Versa Networks Confidential
Industry leading VOS™ multi-tenant software



Components of Versa ZTNA Solution



Self Management Portal

- Visibility & control of users, apps and more for enterprise IT and security teams



Versa Cloud Gateway

- Cloud based ZTNA gateway securely connects to enterprise network and Cloud/SaaS



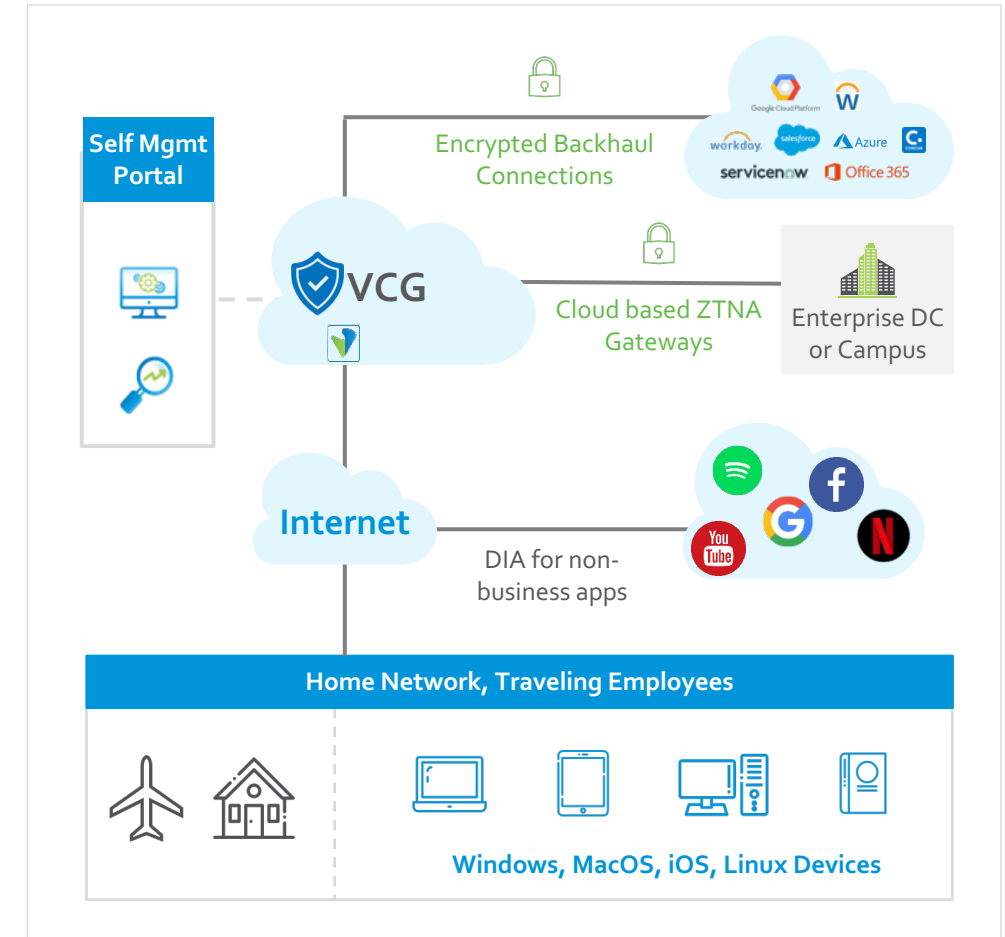
Fast Internet connectivity for remote workforce and intranet connection for in-campus access

- Wired, Wireless, Cellular



Universal SASE Client

- For Windows, MacOS, iOS and Android devices
- Clientless connectivity option

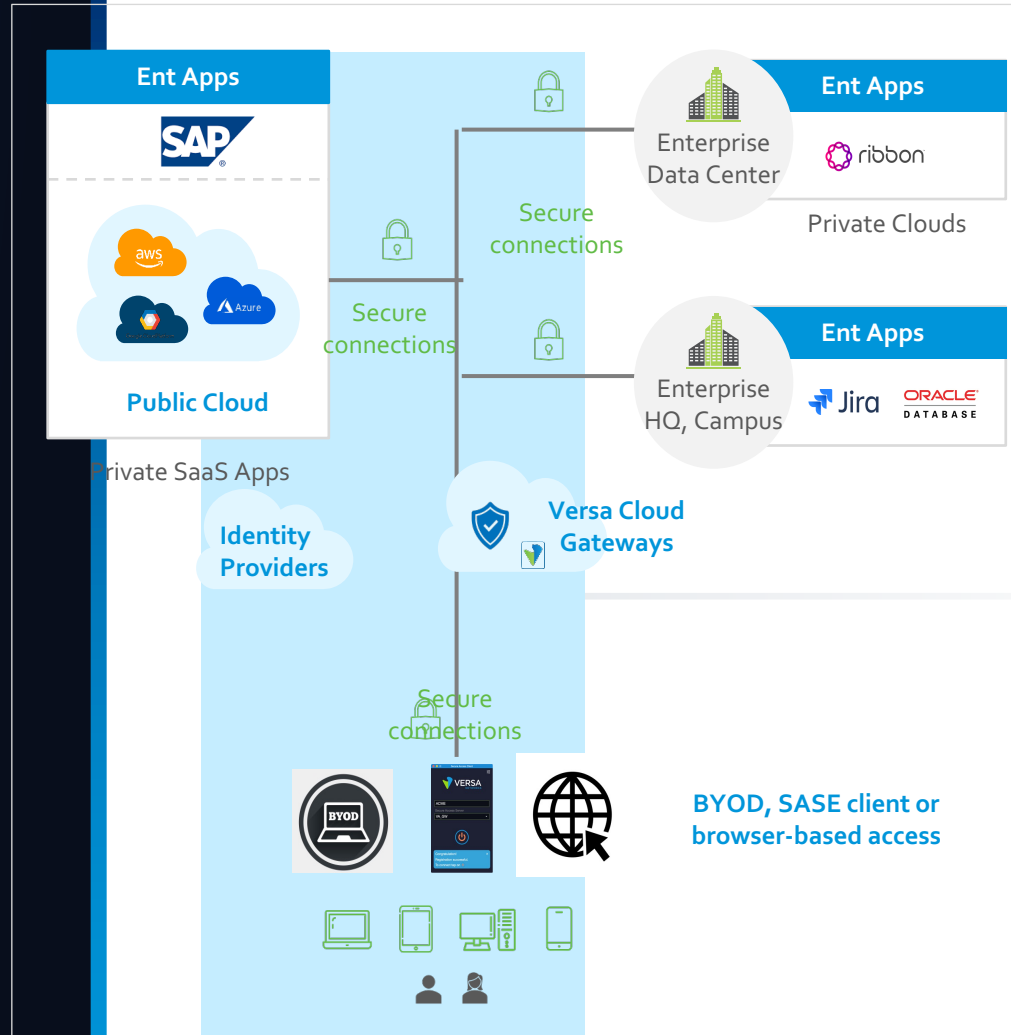


Use Case

Secure Remote Access

*Objective:
Secure end-to-end access for
hybrid, distributed workforce*

Versatility 2024



Capabilities

- Secures corporate devices with the SASE client, BYOD, browser-based access, IoT devices
- Zero Trust access to enterprise applications in datacenters, private or public clouds



Benefits

- Universal ZTNA policies connecting any user to application

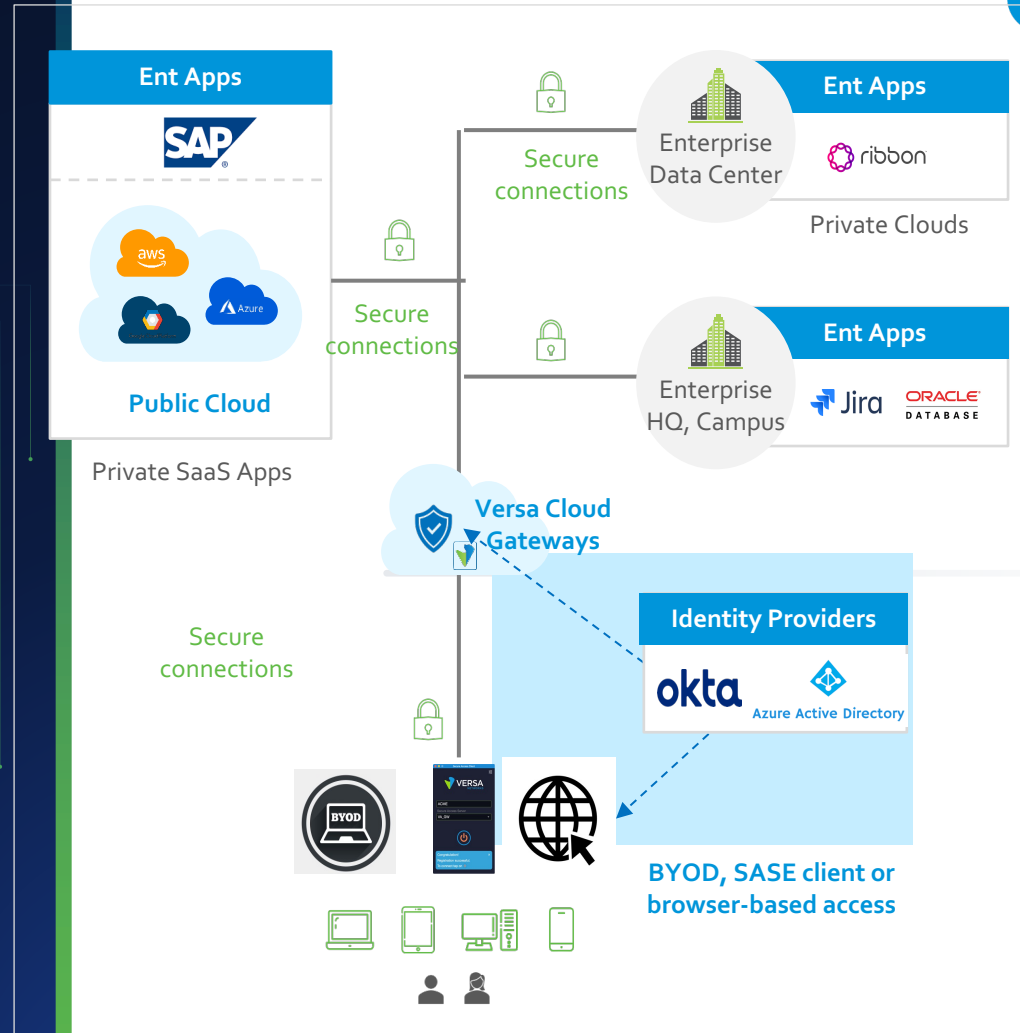


Use Case

Identity-based Access

*Objective:
Identity-based zero-trust
access for all users and devices*

Versatility 2024



Capabilities & Benefits

- Contextual access based on user identity, role, application, geo-location
- Adheres to zero-trust principles of always verify
- Integrate with Identity providers – Okta, Azure AD, Ping Identity, Google Identity
- Multi-Factor Authentication, Single-sign on to Identity providers
- Identity mgmt. - SAML, LDAP

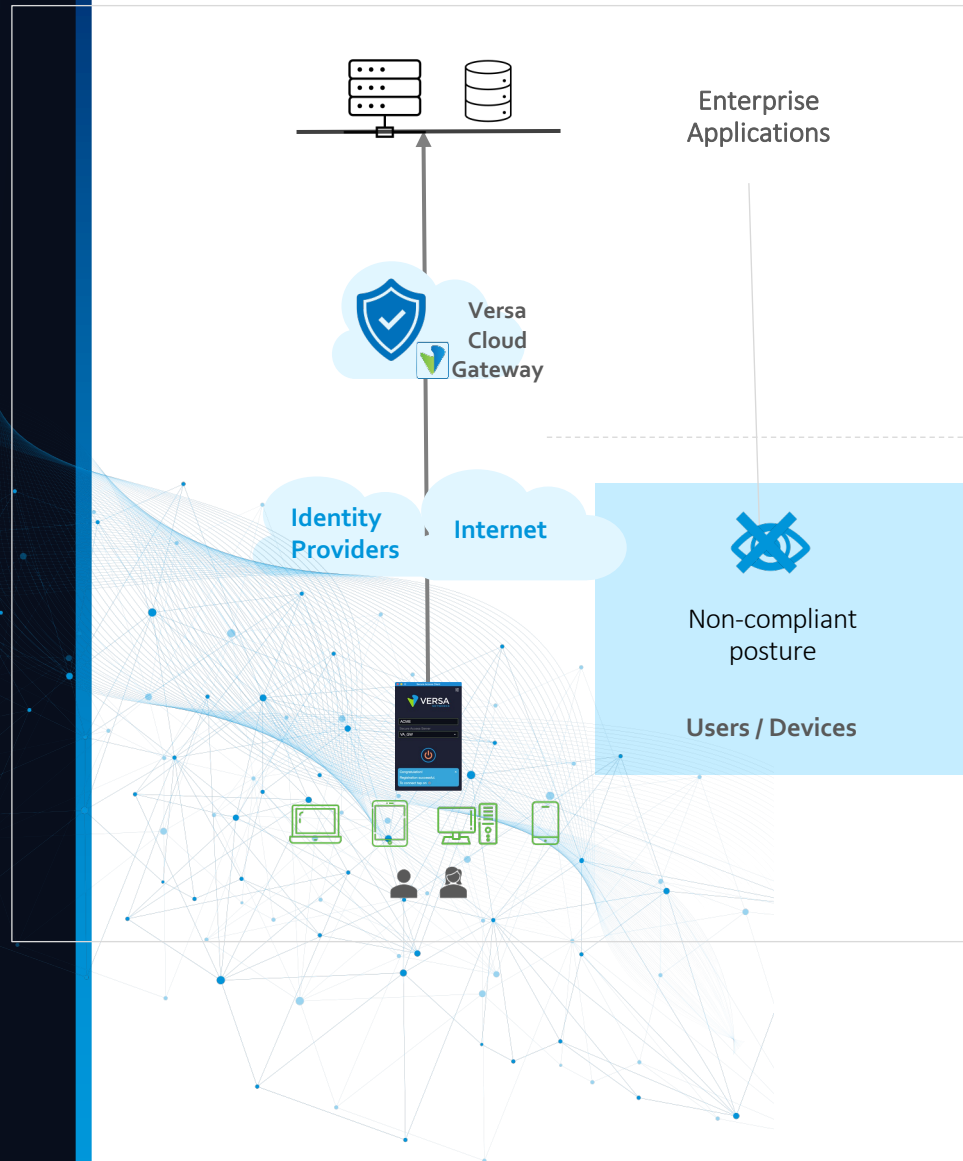


Use Case

Evaluate Endpoint Posture Checks

*Objective:
Continuously evaluate endpoint
posture and enforce ZTNA*

Versatility 2024



✓ Capabilities

- Endpoint posture checks
- Check on connection initiation and continue to evaluate
- Attributes – Host certificate, firewall, endpoint platform, disk encryption, domain joined and more..

✓ Benefits

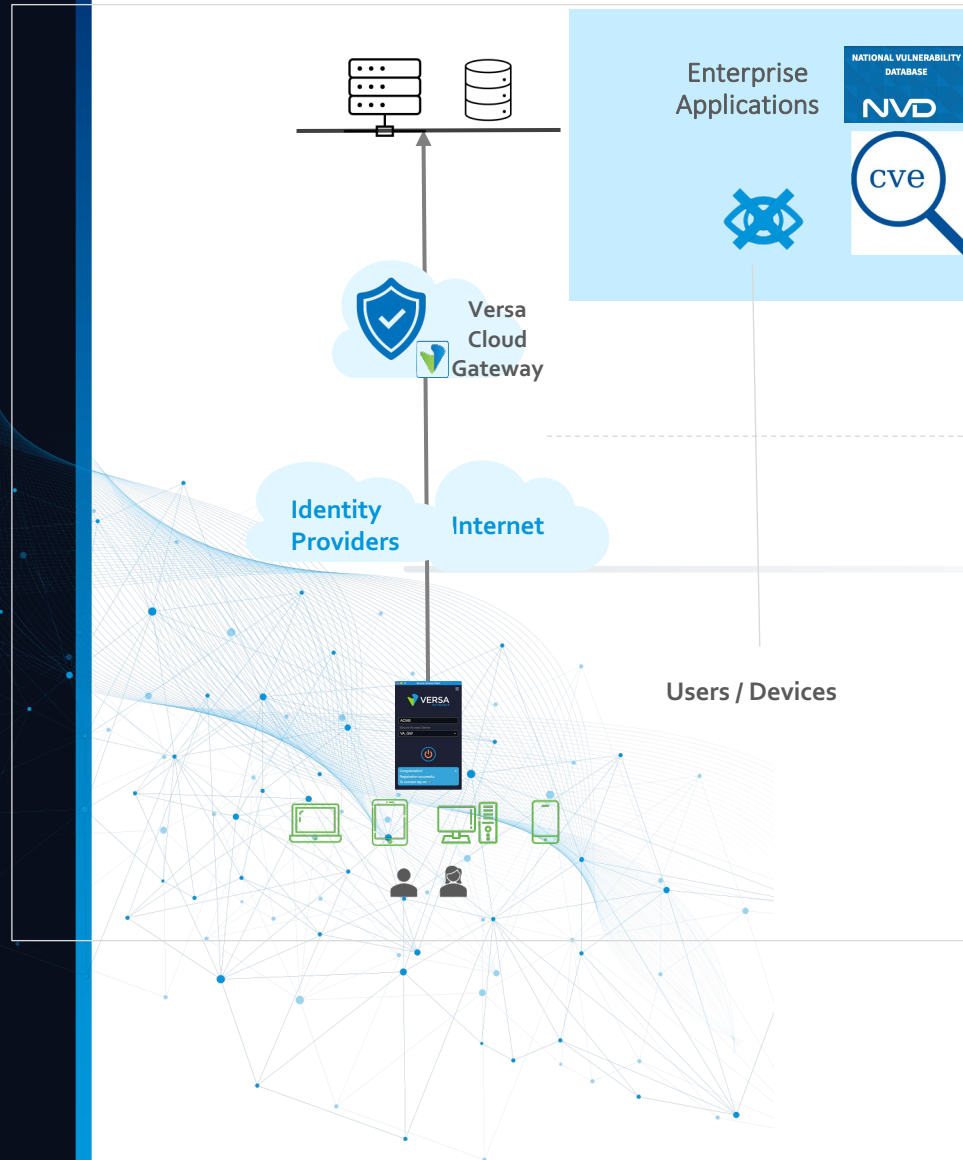
- Continuous compliance and enforcement of ZTNA

Use Case

Protect against Vulnerabilities

*Objective:
Protect users and enterprise
networks from application
vulnerabilities*

Versatility 2024



✓ Capabilities

- ZTNA with IPS protection
- More than OWASP top 10 issues
- Continuous protection from newer vulnerabilities in any application software e.g. Apache, Microsoft Exchange Server, NGINX, Wordpress, freerdp

✓ Benefits

- Vulnerability protection along with zero trust access

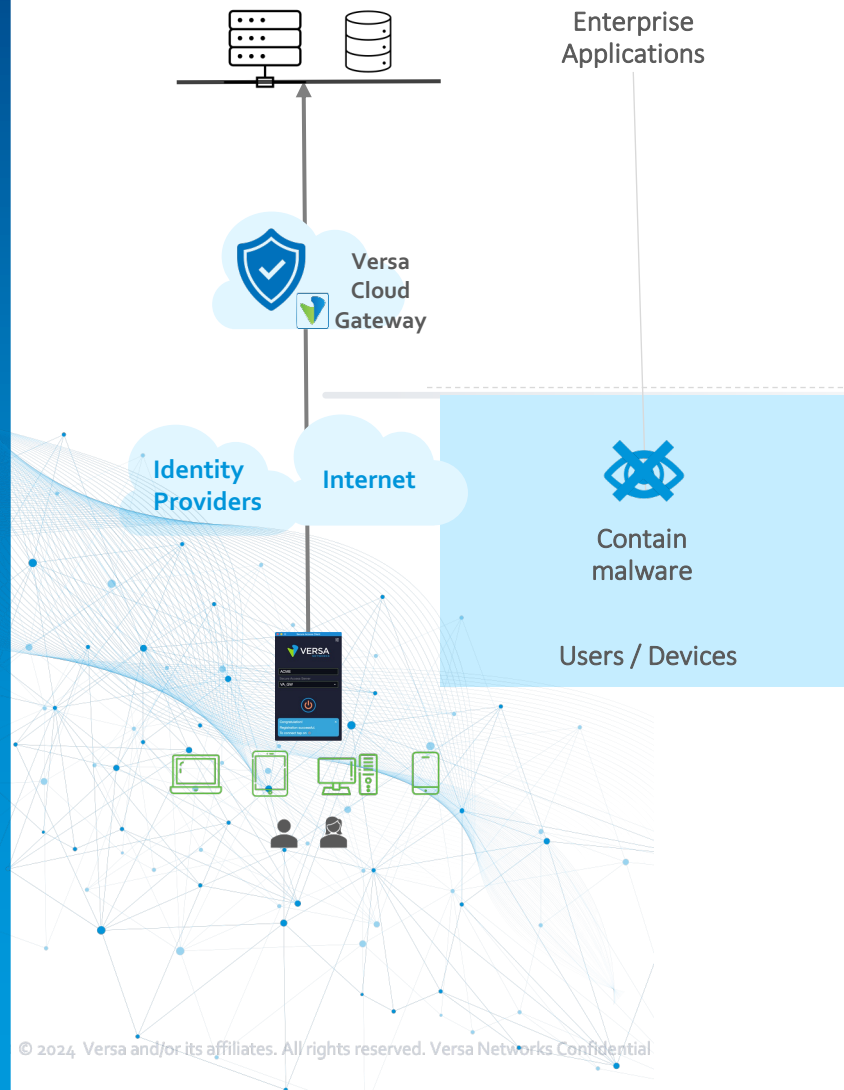


Use Case

Contain Malware

*Objective:
Prevent malware propagation
across applications and other
enterprise sites*

Versatility 2024



✓ Capabilities

- Contain malware within user/device
- Block propagation, C&C or botnet activity
- E.g.: Mirai malware affecting IoT devices
- Emotet variant –affecting bank branch office

✓ Benefits

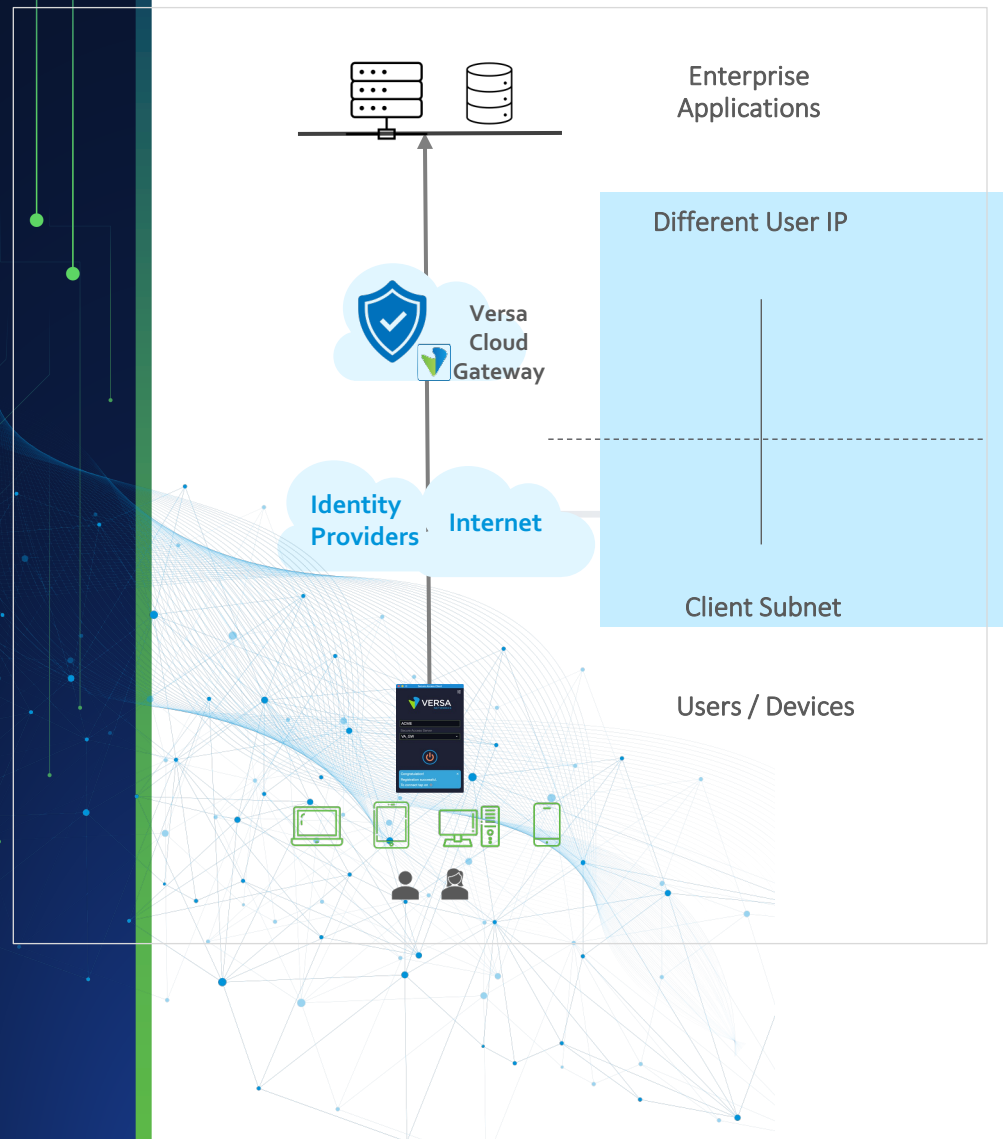
- Prevent malware propagation across applications and other enterprise sites



Use Case

Obfuscate Remote Users

*Objective:
Protect users and prevent lateral movement*



✓ Capabilities

- No default client IP address of gateway
- Create a Dark cloud / Dark network
- Hide enterprise users

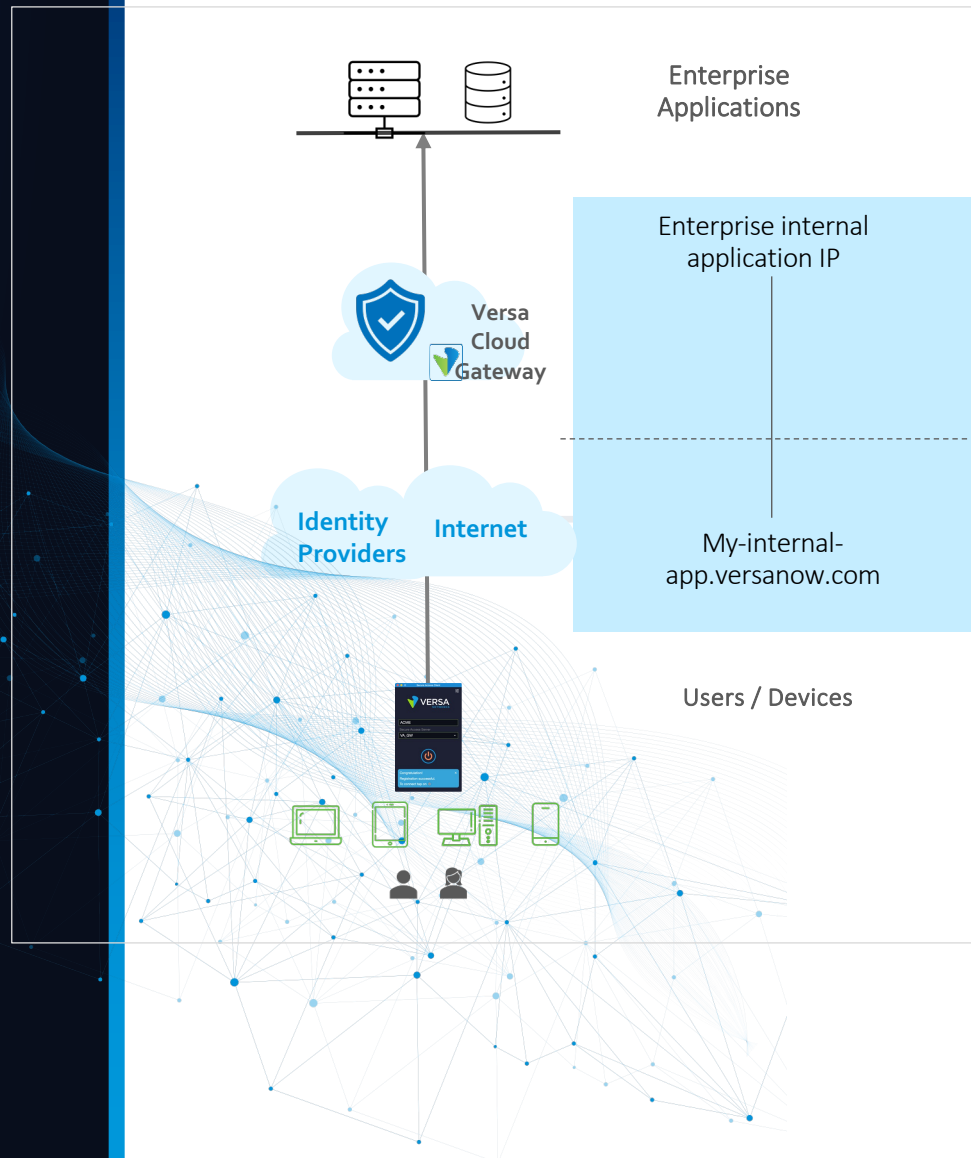
✓ Benefits

- Protect enterprise users/clients
- Prevent lateral movement

Use Case

Obfuscate Enterprise Applications

*Objective:
Protect enterprise applications
and prevent lateral movement*



✓ Capabilities

- Do not expose enterprise IP addresses
- Create a Dark cloud / Dark network
- Hide enterprise applications and services

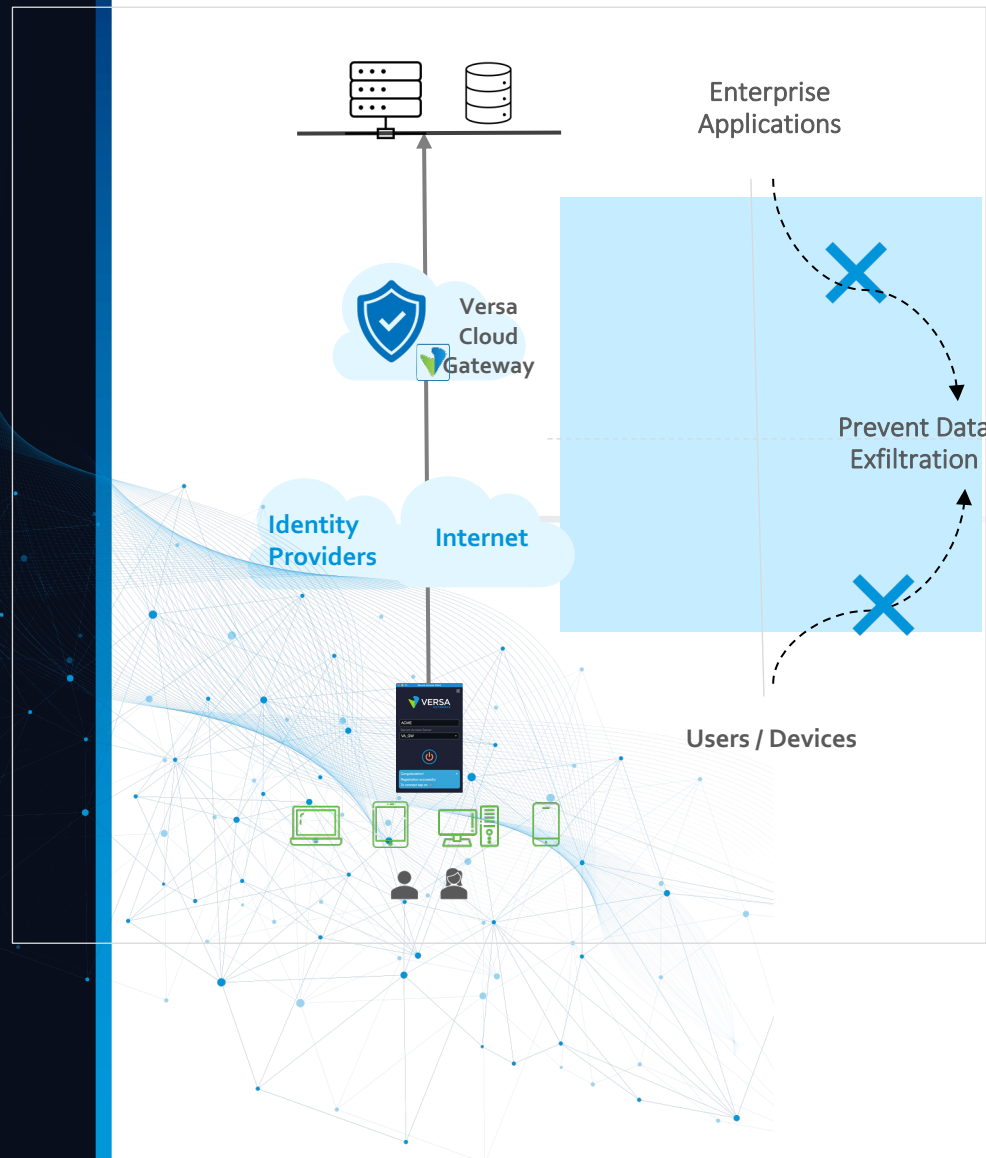
✓ Benefits

- Protect enterprise applications
- Prevent lateral movement

Use Case

Prevent Data Loss

*Objective:
Prevent data exfiltration from
users, devices or through
application access*



✓ Capabilities

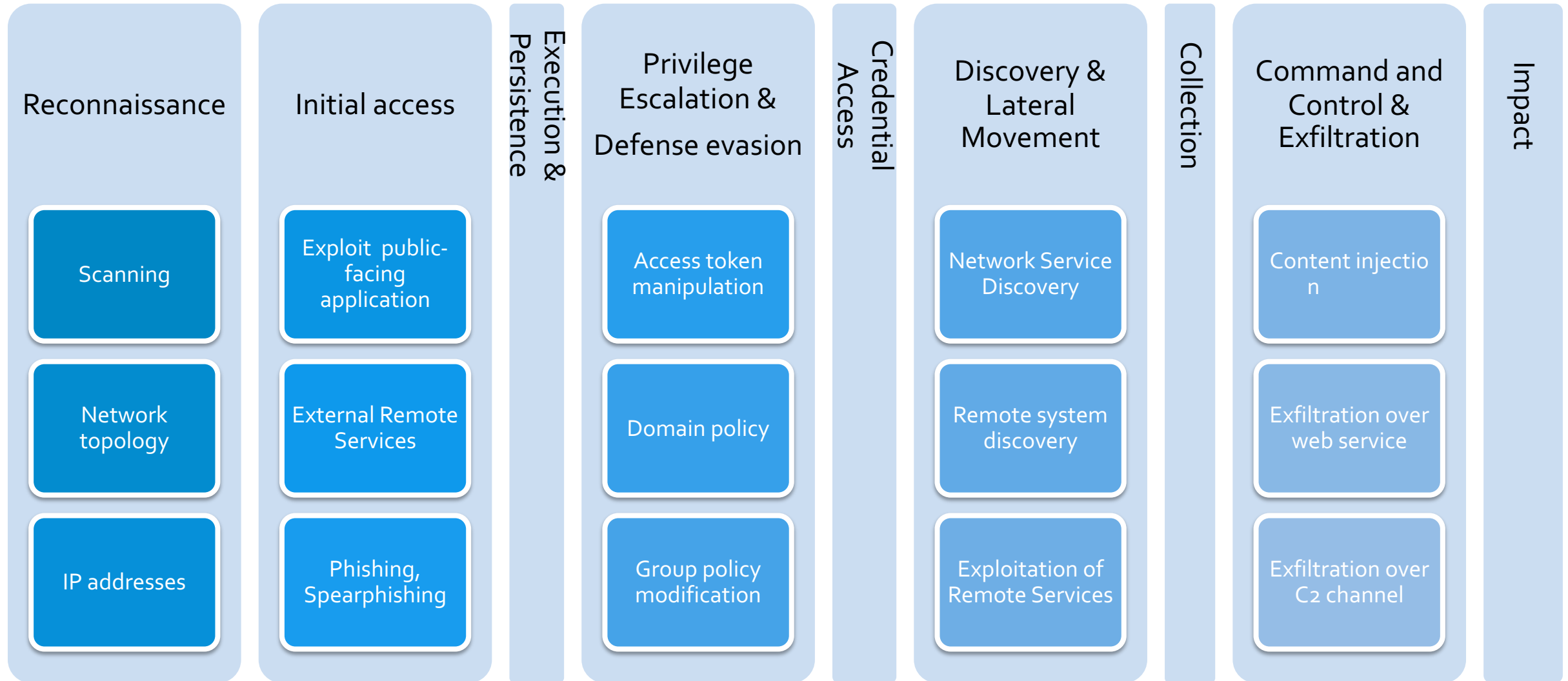
- Sensitive data protection
- Contextual analysis on data patterns and predefined profiles e.g.: PCI-DSS, HIPAA, PII, credit card, SSN
- Variety of file types, protocols

✓ Benefits

- Prevent unintended or deliberate data exfiltration

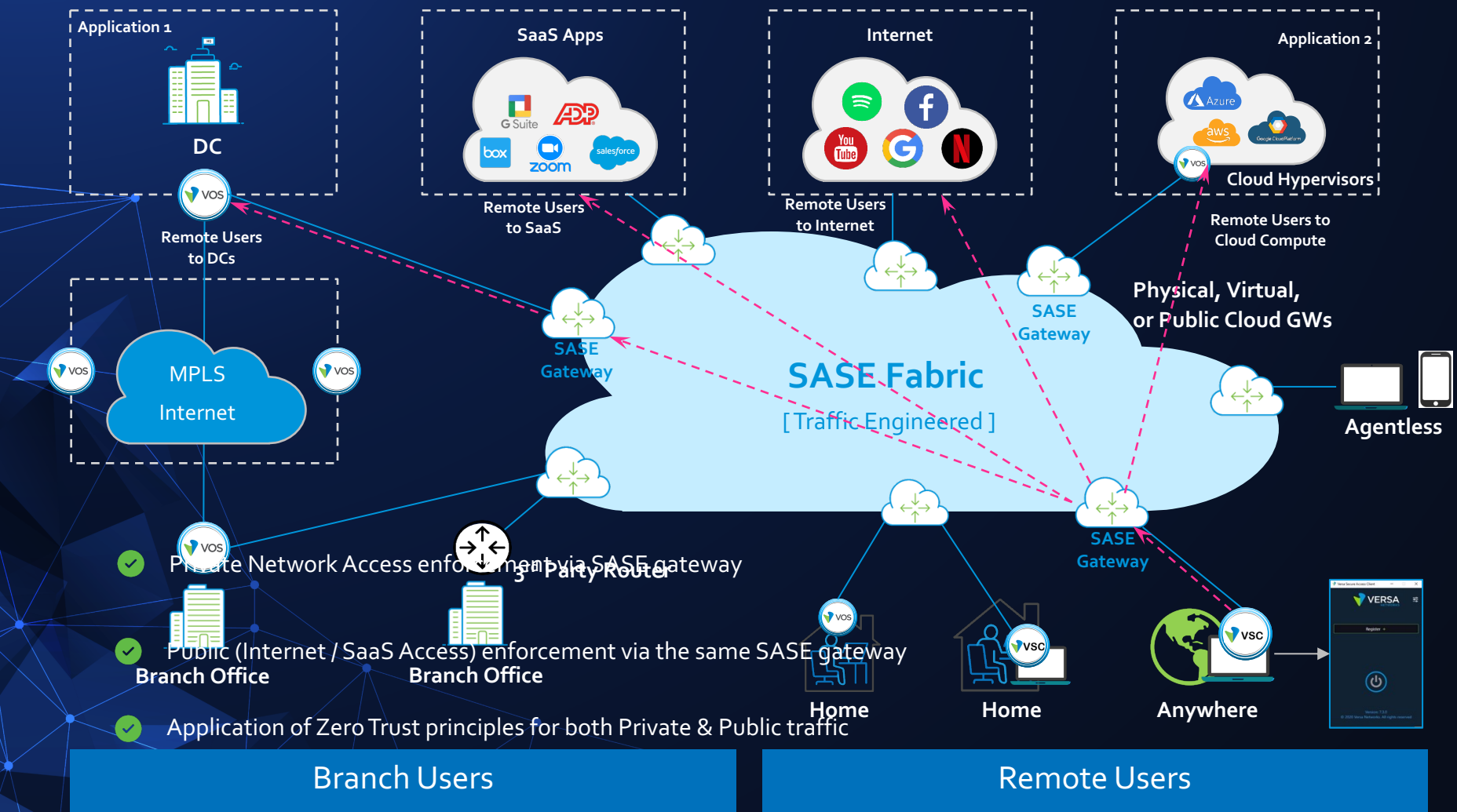
Versa ZTNA with Built-in Security

Protects against several MITRE ATT&CK techniques



Versatility 2024

Unified Platform for Both Private & Public Access

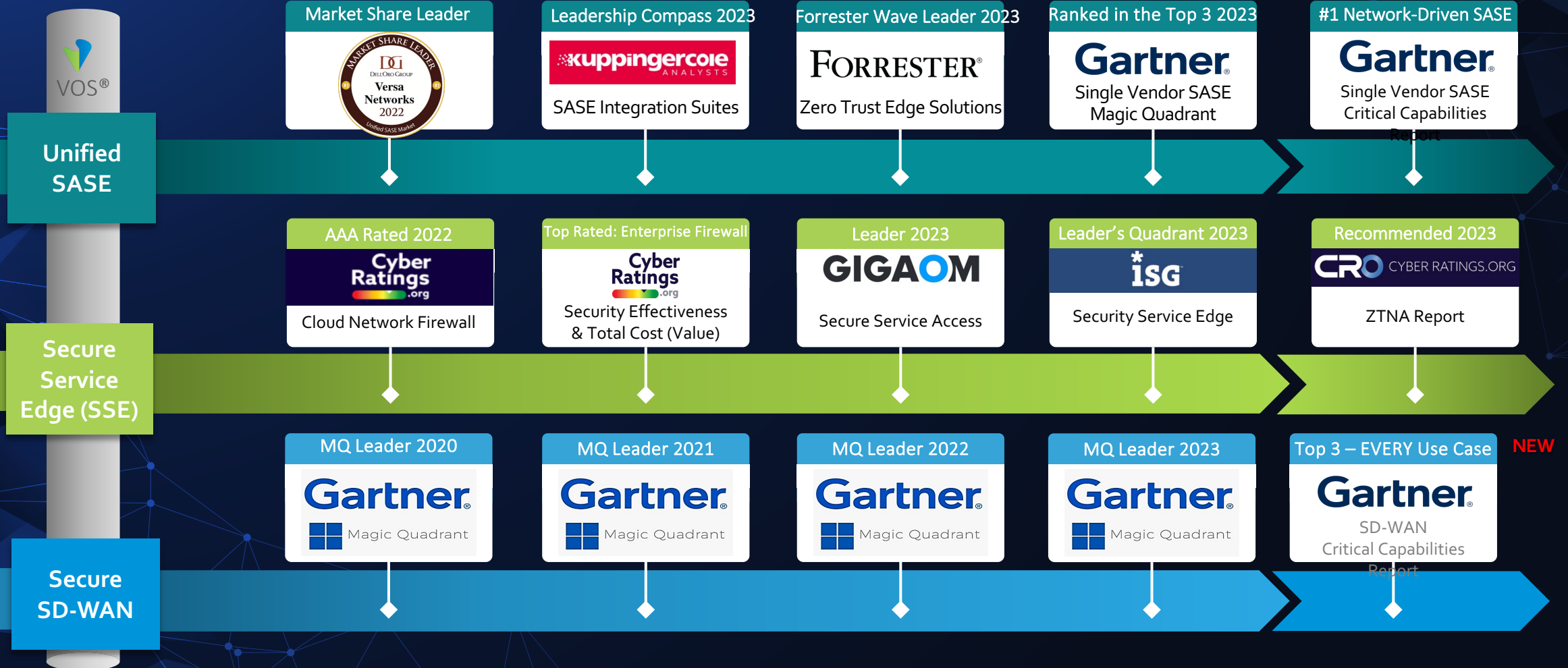


Single Pane of Management,
Monitoring and Visibility

Versatility 2024



Why industry experts are raving about Versa Networks



Versatility 2024

Cyber Ratings.org

Zero Trust Network Access (ZTNA) Report 2023



ZTNA | Q3 2023

Versa Networks Zero Trust Network Access Earns **RECOMMENDED** Rating from Independent Testing Lab CyberRatings.org

Received the highest (Recommended) Rating by CyberRatings.org, including passing all Authentication & Identity, Resource Access, Routing & Policy Enforcement, and TLS/SSL tests.



Authentication & Identity

Authenticate and identify all connections and users

Prove they can then apply identity-aware policies.

Versa ZTNA
passed 100%
of the tests



Resource Access

Apply identity-based access control

Restrict lateral movement

Versa ZTNA
passed 100%
of the tests



TLS/SSL

Tested to detect attacks concealed by encryption

Tested for attacks against the encryption protocols.

Versa ZTNA
passed 100%
of the tests



Performance

Measured performance under various load conditions, traffic profiles, encryption

930 Mbps on 1Gbps
test

Versatility 2024



ZTNA Independent Evaluation – CyberRatings Test Results



Versa Networks ZTNA

RECOMMENDED

In Q3 2023, CyberRatings.org conducted an independent test of Versa Networks against the Zero Trust Network Access (ZTNA) Test Methodology v2.0, using Amazon Web Services and our facility in Austin, Texas. The product was thoroughly tested to determine how it handled Authentication & Identity, Resource Access, Routing & Policy enforcement, and TLS/SSL 1.2 and 1.3 cipher suites. Both clear text and encrypted traffic were measured for performance. For this test, we tested up to 1 Gbps.

AUTHENTICATION & IDENTITY

SAML Authentication	
SAML Authentication using Okta	Pass
SAML Authentication using Ping	Pass
SAML Authentication using Azure AD	Pass
Identity Aware Policies	Pass

RESOURCE ACCESS

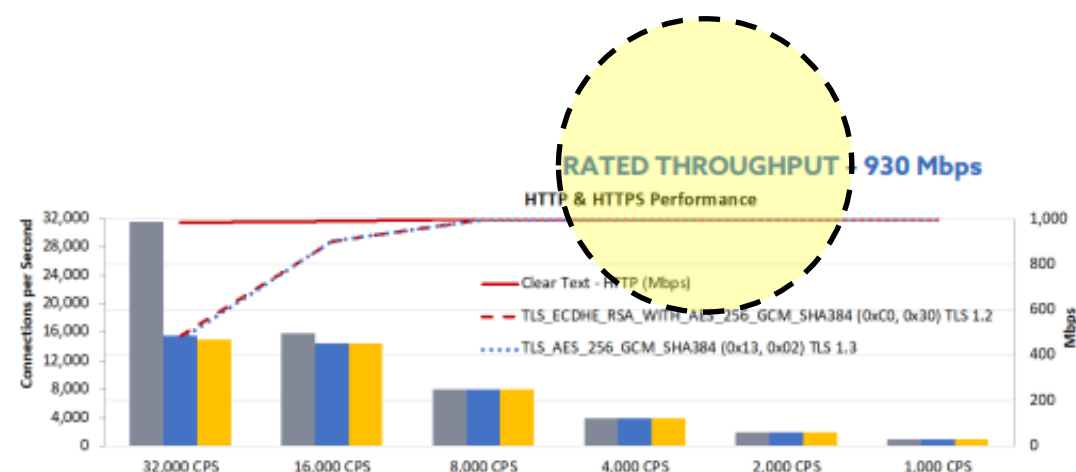
Support for unrouteable "hidden" networks	Pass
Remote access to "hidden" network via ZTNA service	Pass
Identity/app/location access control for "hidden"	Pass
No full network access (identity/application)	Pass
Support for non-standard ports and non-web	Pass

SSL/TLS SUPPORT

Cipher Suite Support	
Top 10 Cipher Support	10/10 Supported
Insecure Cipher Suites	
Null ciphers (no encryption of data)	Pass
Anonymous Ciphers (no authorization)	Pass
Decryption Validation	
Exploit + Legitimate Traffic - Un-Encrypted	Pass
Exploit + Legitimate Traffic - Encrypted	Pass
Decryption Bypass Exceptions	Pass

ROUTING & POLICY ENFORCEMENT

Network Segmentation			Pass
Overlapping Subnets			Pass
Access Control			Pass
Network Services			
HTTP			Pass
HTTPS			Pass
FTP			Pass
SFTP			Pass
SMB			Pass
SMTP			Pass
DNS			Pass
ICMP			Pass
SSH			Pass
IMAP/POP			Pass
Application Access	Allow	Block	Block Specific
Social Networks	Pass	Pass	Pass
Streaming Media	Pass	Pass	Pass
Teleconferencing	Pass	Pass	Pass
Cloud Storage	Pass	Pass	Pass
Email Applications	Pass	Pass	N/A
SaaS Applications	Pass	Pass	Pass



HTTP & HTTPS Performance	Clear Text (HTTP)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30) TLS 1.2		TLS_AES_256_GCM_SHA384 (0x13, 0x02) TLS 1.3	
	CPS	Mbps	CPS	Mbps	CPS	Mbps
Max Connections per Second (CPS)						
32,000 CPS	31,537	986	15,570	487	14,967	468
16,000 CPS	15,859	991	14,451	903	14,450	903
8,000 CPS	8,000	1,000	7,995	999	7,988	999
4,000 CPS	4,000	1,000	4,000	1,000	3,989	997
2,000 CPS	2,000	1,000	2,000	1,000	2,000	1,000
1,000 CPS	1,000	1,000	1,000	1,000	1,000	1,000

Versatility 2024



Questions



Versatility 2024

© 2024 Versa and/or its affiliates. All rights reserved. Versa Networks Confidential



Thank you!



CYBERRATINGS.ORG RESEARCH REPORT

Versa Networks Earns
RECOMMENDED Rating
for Real-World Test of Zero
Trust Network Access

Download
ZTNA Report
www.versa-networks.com

Versatility 2024

© 2024 Versa and/or its affiliates. All rights reserved. Versa Networks Confidential

