MEF

WEBINAR

GAIN A COMPETITIVE EDGE WITH MEF-CERTIFIED SASE & SD-WAN

22 April 2025 | 10–11 am EDT

Moderator

Kevin Vachon

COO,
MEF

Participants

Kevin Vachon
COO,
MEF

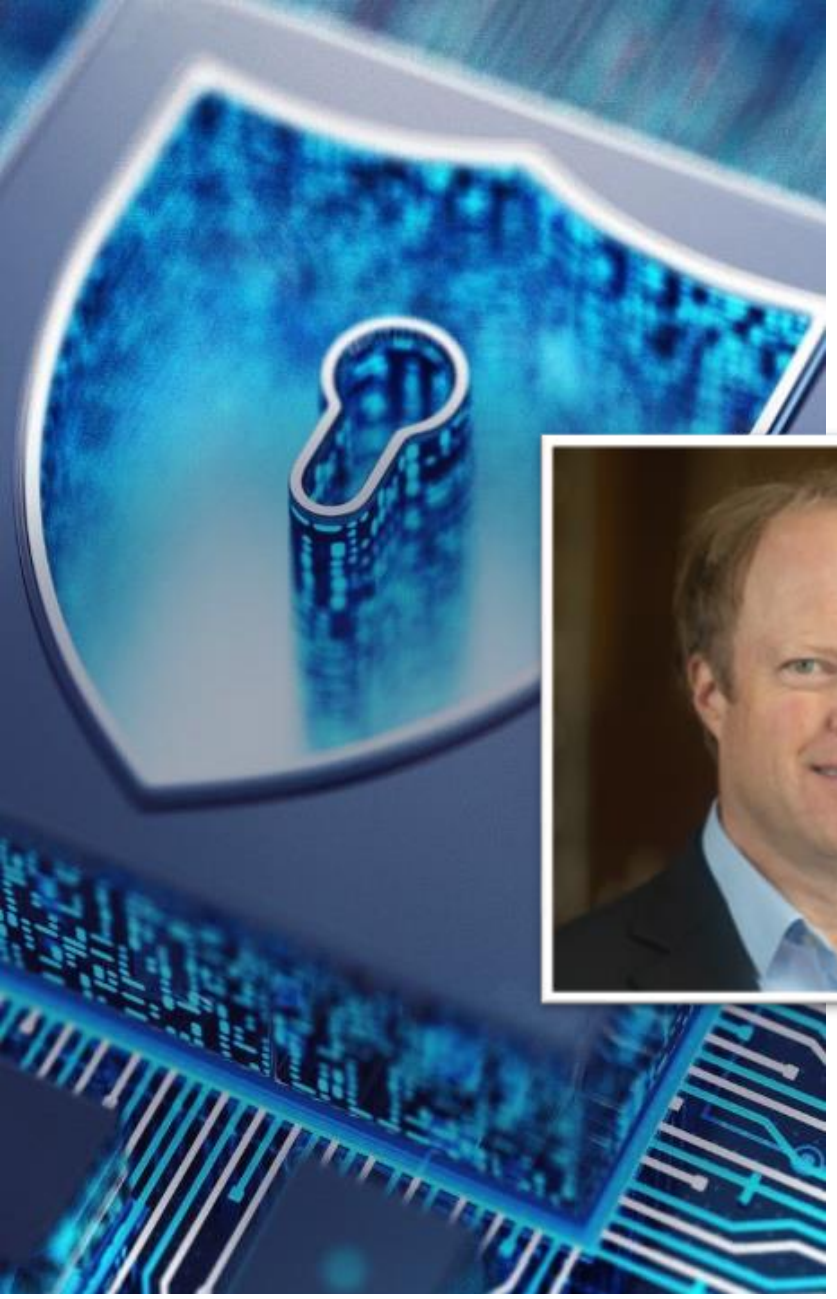
Stan Hubbard
Principal Analyst,
MEF

Daniel Bar-Lev
Chief Product
Officer, MEF

Ian Foo
CTO and EVP of
Product,
CyberRatings.org

Agenda

- Threat Environment & the Need for Industry Collaboration
- Intro to MEF Standards-Based SASE Certification Program
- Certification Benefits for Service Providers and Enterprises
- A Rigorous Testing Plan for Certification
- Marketing Resources to Maximize Your Certification Investment



Stan Hubbard

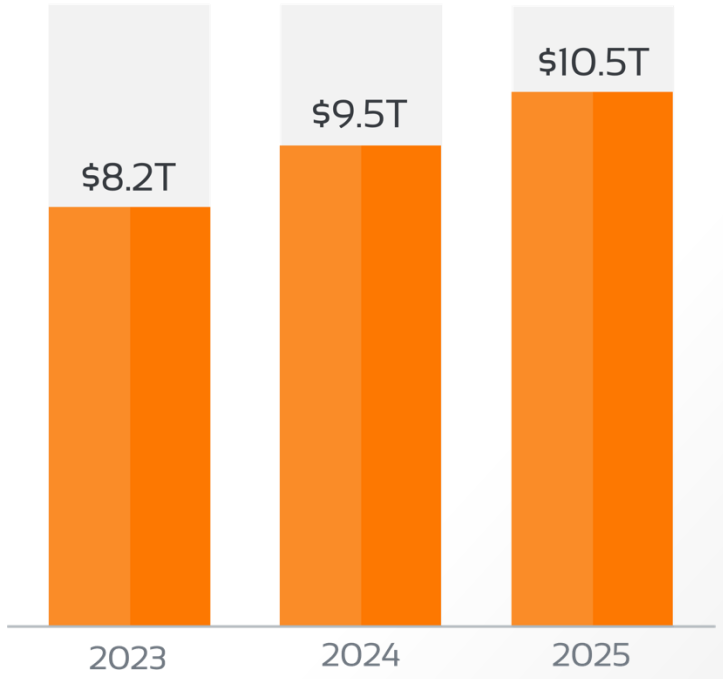
Principal Analyst,
MEF

Cybersecurity is Not Keeping Pace with Threats of Major Cyberattacks & Cybercrime

Risk of Major Cyberattacks Has Never Been Greater

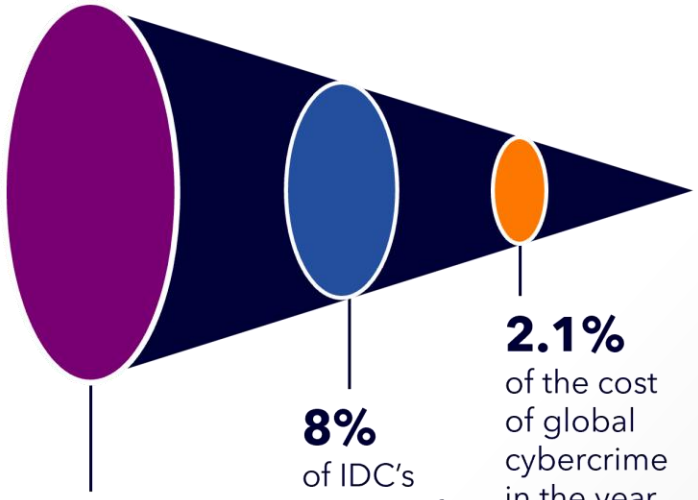
- Rapidly growing global digital economy
- Accelerating digital transformation
- Escalating vulnerabilities and cyberattacks
- AI and cybercrime-as-a-service
- Worldwide shortage of skilled cybersecurity experts
- Rising geopolitical instability

Cybercrime Costs Are Exploding Worldwide



Cybersecurity Ventures

Cybersecurity Spending is Not Keeping up with Challenge



$201B
2024 Global Spending on Information Security and Risk Management

8%
of IDC's estimate for total digital transformation spending

2.1%
of the cost of global cybercrime in the year

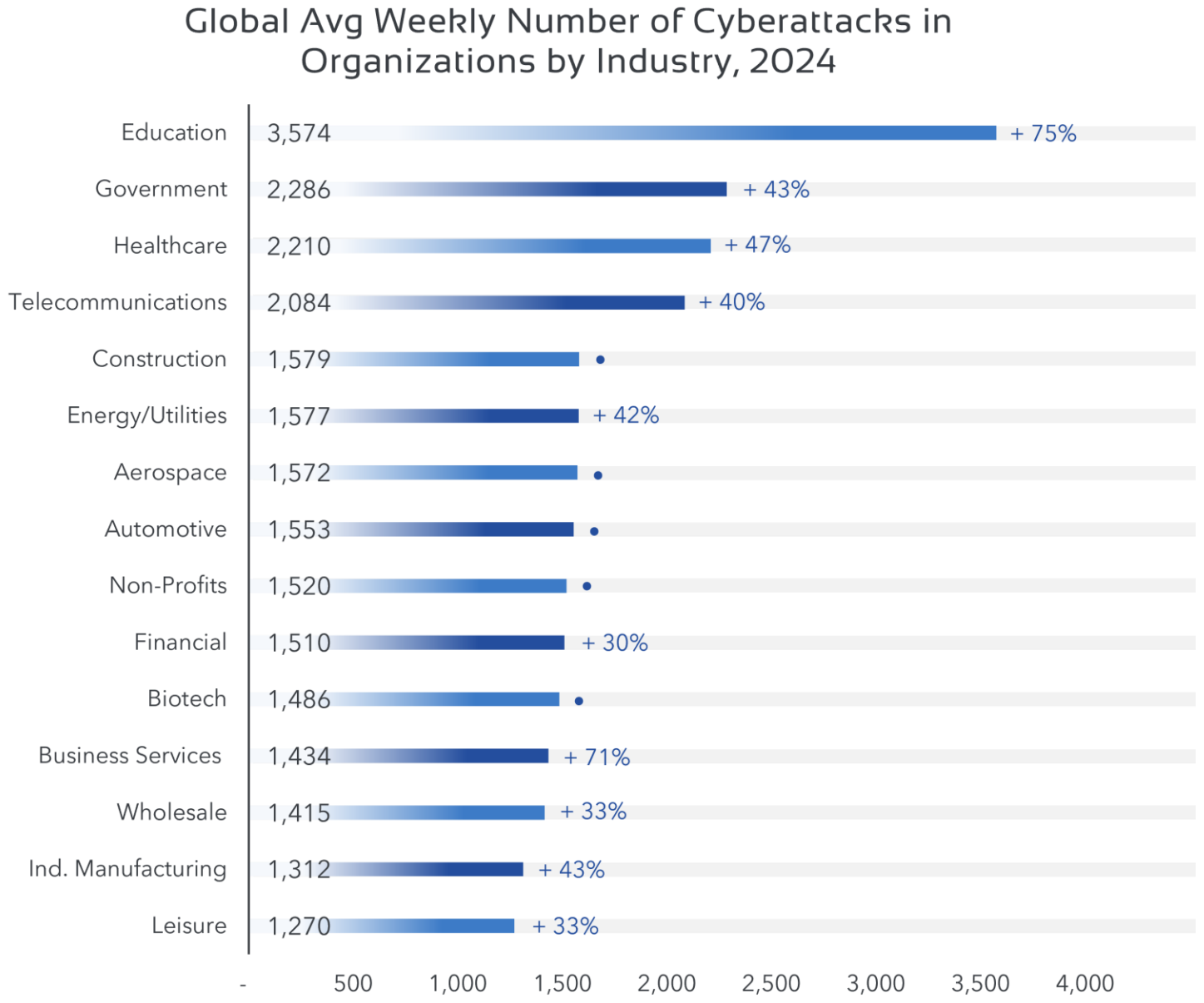
Statista, IDC

Average # of Global Weekly Attacks Against Organizations Surged

44% Higher

in 2024

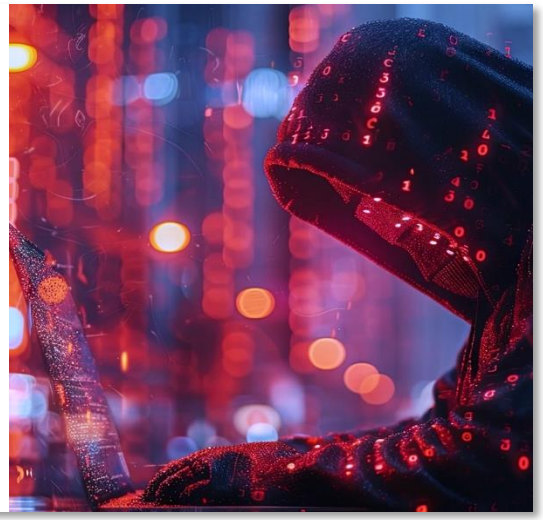
Source: Check Point



We Must Collaborate & Standardize to Accelerate Market Solutions to Address Threats

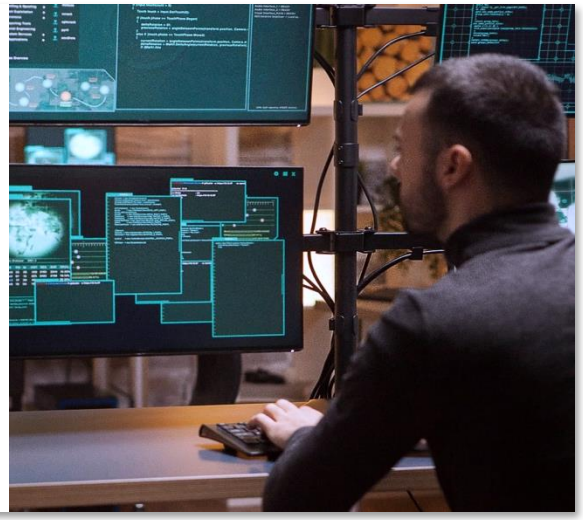
1

Cyber Threats are Outpacing Our Ability to Deal with Them



2

Organizations Should Prioritize Essential Actions to Strengthen Defenses



3

Suppliers must Embrace Secure by Design and Standardized Solutions

4

Private Sector is Under Pressure to Carry the Burden for Defending Critical Infrastructure

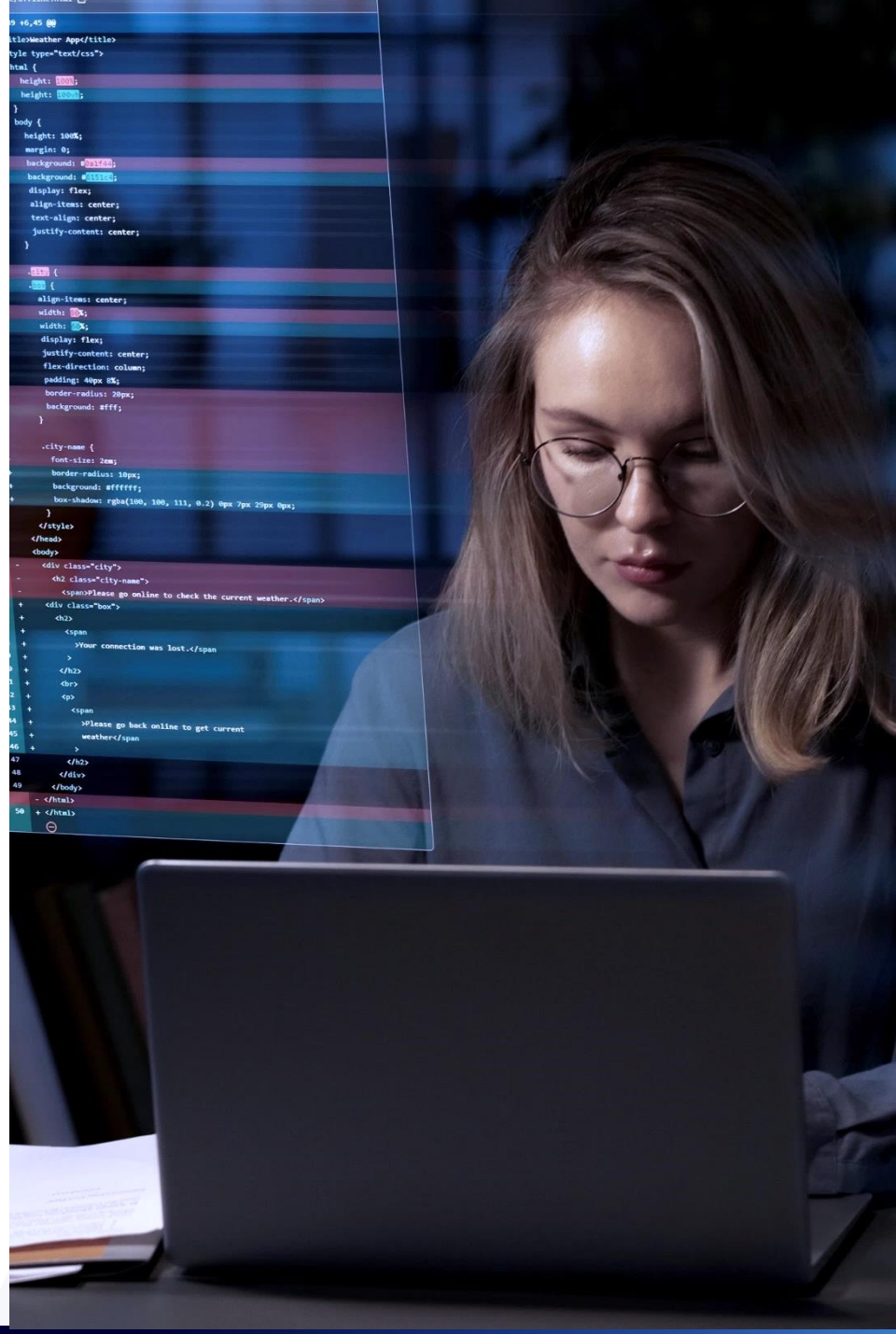
ClearanceJobs / News & Career Advice

U.S. Government Cybersecurity Cuts Could Be a Gift to Hackers—Experts Sound the Alarm

Enterprises Increasingly Embrace SASE to Address Key Secure Digital Transformation Challenges

1. Increased use of cloud services
2. Rise of remote & hybrid work
3. Need to apply Zero Trust principles

…are fueling explosive demand for SASE, which solves the problem of protecting users, devices, and applications at scale.



Daniel Bar-Lev

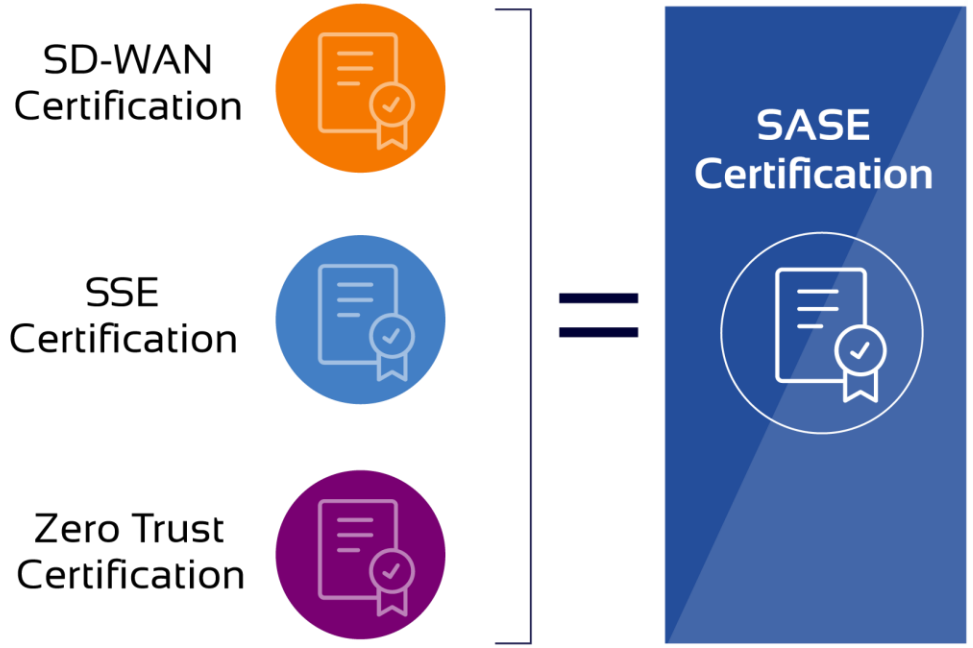
Chief Product Officer,
MEF

MEF SASE Certification Program Roadmap

Phase 1
Vendor Testing &
SP Inheritance

Phase 2
SP In-Network
Testing

Phase 3
Integrated
Solution Testing



What is the MEF SASE Certification Program?

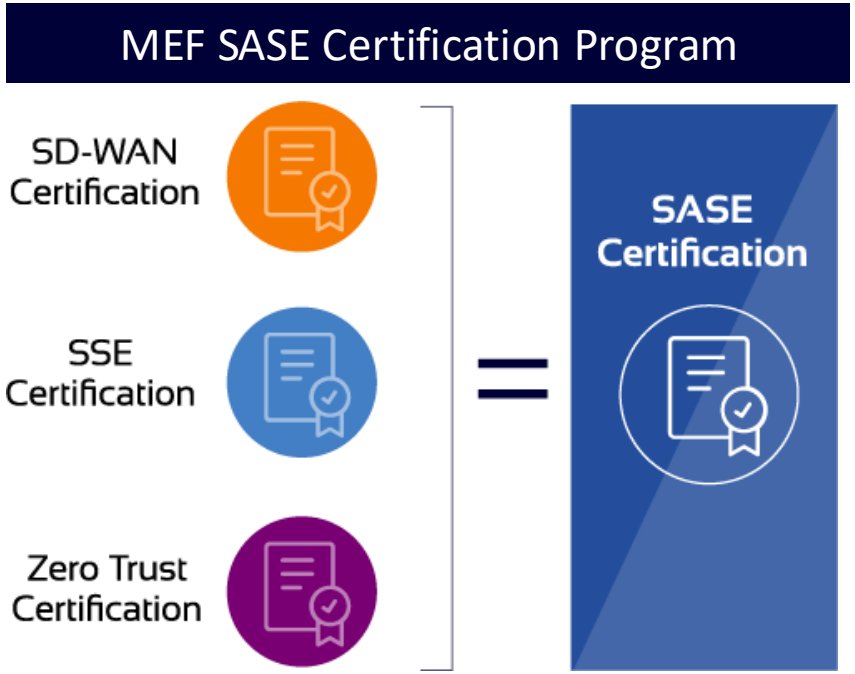
SASE integrates networking and cybersecurity functions under a single policy management framework. It ensures secure access and connectivity for continuously verified users, devices, and applications to targeted resources.

Phase 1 SASE certification program testing validates the effectiveness and application performance of the three components of SASE solutions – SD-WAN, SSE and Zero Trust

MEF SASE certification program aims to:

- Align stakeholders on common terminology and expectations
- Build trust and confidence
- Assure vendor transparency and product effectiveness
- Accelerate adoption of SD-WAN, SSE and Zero Trust

Service providers currently can subscribe to inherit SASE or individual certifications from their technology suppliers.



MEF ATCP AUTHORIZED TEST & CERTIFICATION PARTNER

CRO CYBER RATINGS.ORG

MEF SASE Certification Program Benefits for Enterprises

Simplify Procurement & Provider Selection

- Accelerate shortlist creation

Confidently Purchase SASE Solutions

- Select solutions aligned with MEF global standards and using independently tested technology

Stay Ahead with Continuous Security & Compliance

- Meet evolving regulatory requirements

MEF SASE Certification Program Benefits for Service Providers

Competitive Advantage & Credibility

- Stand out as a trust leader in the crowded SASE market
- Independently validate SD-WAN, SSE and Zero Trust solutions meet MEF's stringent security and application performance criteria

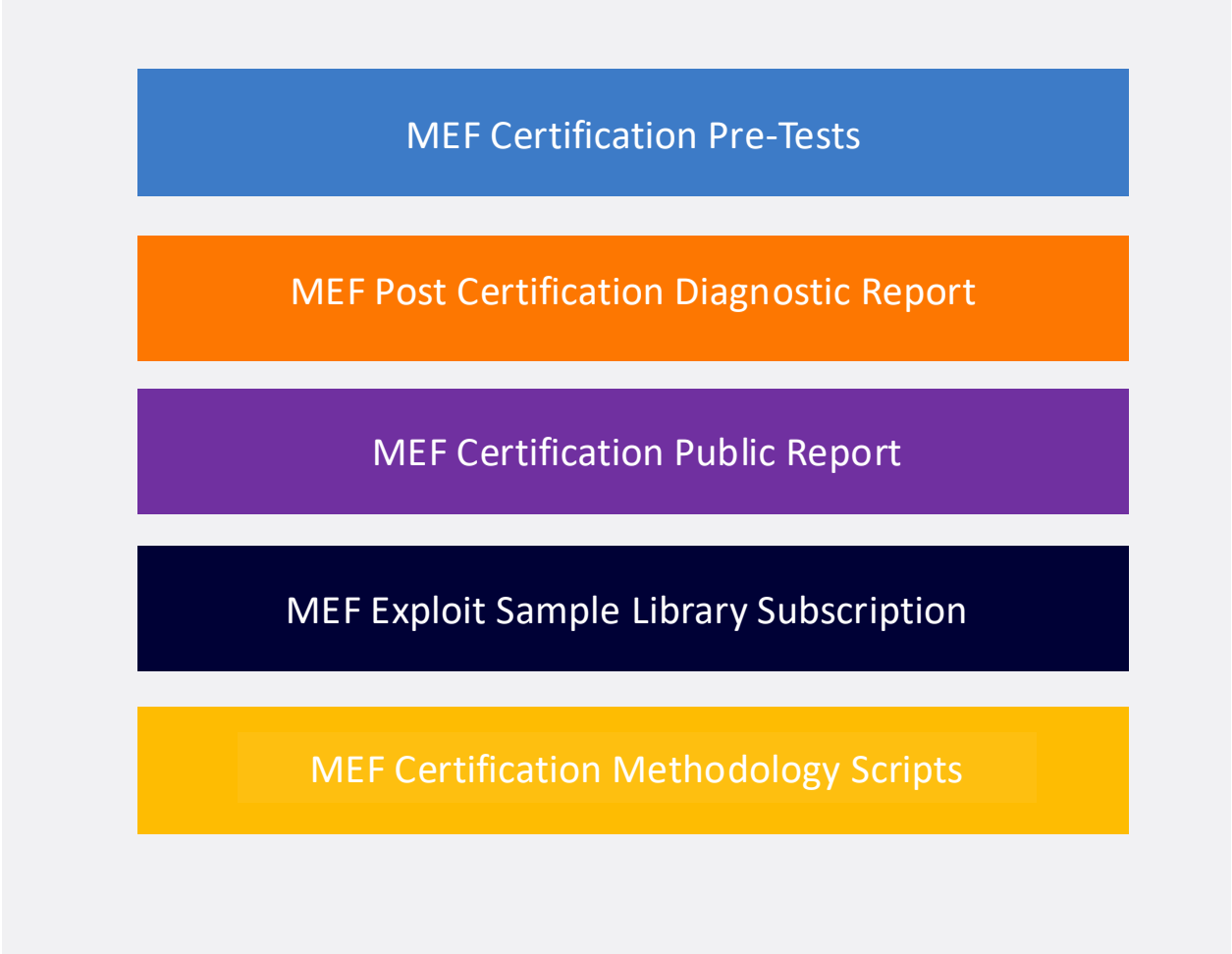
Faster Sales & Procurement Process

- Streamline RFI/RFP responses by leveraging inherited certifications from rigorously tested supplier technology
- Accelerate shortlist placement

Proven Security & Application Performance

- Highlight resilience against known and evolving threats with regular cyber defense testing of supplier technology

Additional MEF SASE Certification Program Options



SASE Certification Process for Service Providers

1

Initial Engagement

Service Provider requests Certification Information Kit

2

Planning Session

Certification schedule agreement

MEF SASE Certification Questionnaire answered

3

Preparation Phase

MEF validates certification eligibility based upon availability of certified Technology Provider

4

Contract & Payment

Service Provider contracts with MEF and processes payment

5

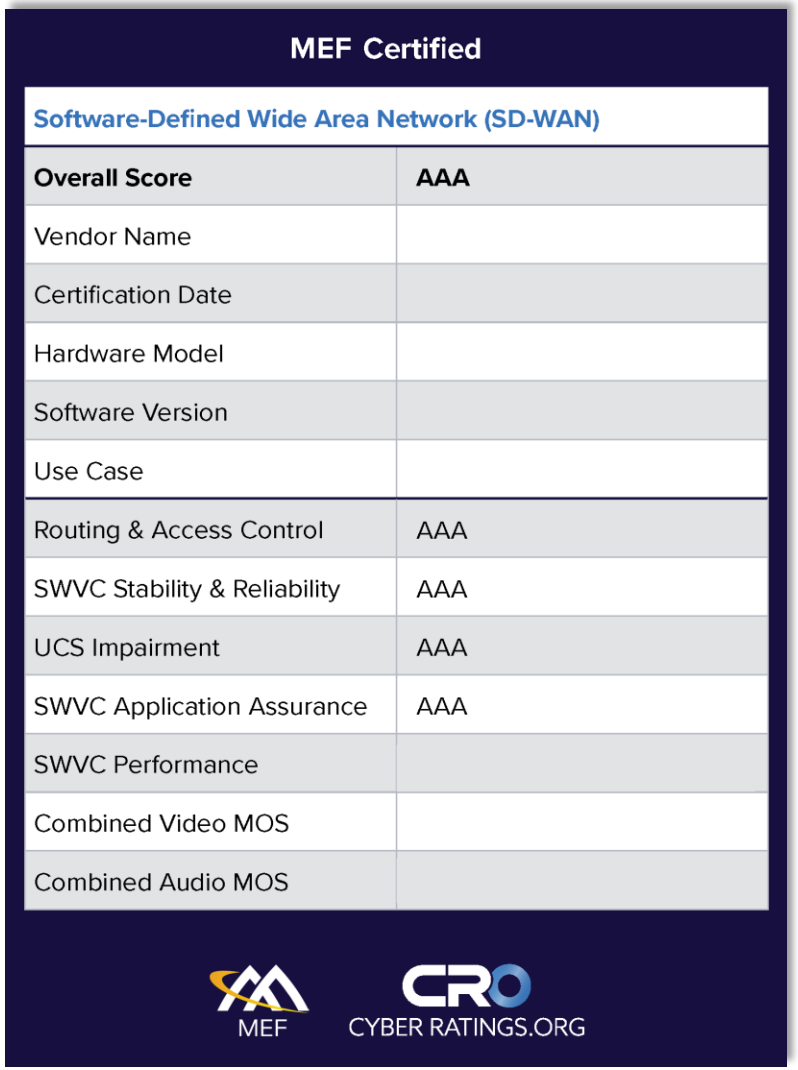
SASE Certification

MEF awards certification to Service Provider, publishes badge in MEF Registry and delivers SASE Marketing Kit

"We're proud to help spearhead a new initiative led by MEF to independently certify cybersecurity protections for networking services… This will be the gold standard for cybersecurity validation when it comes to next-gen network services."

Mike Troiano, Senior Vice President, Business Products, AT&T Business

Certification Report Card



MEF Certified

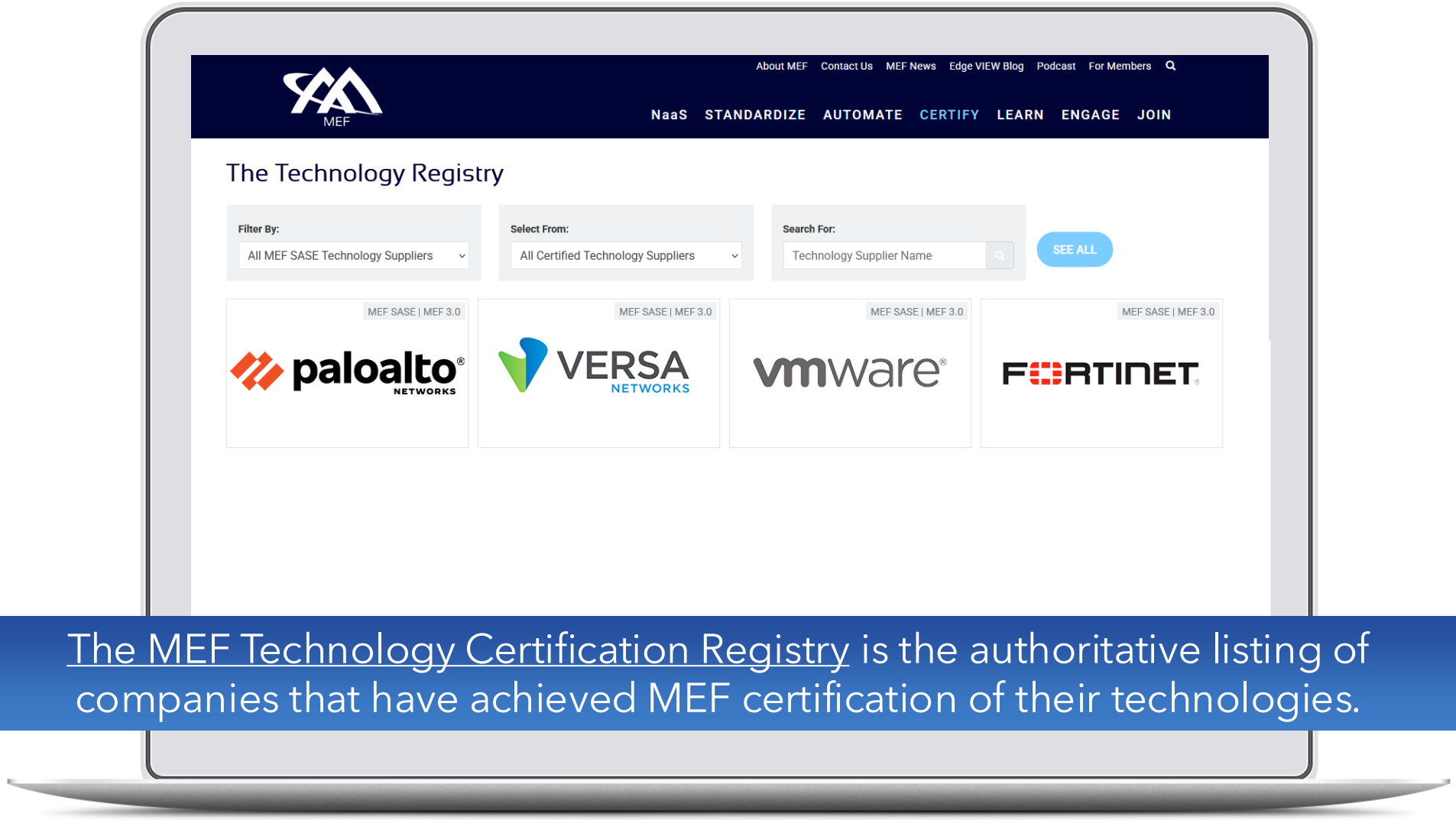
Software-Defined Wide Area Network (SD-WAN)	
Overall Score	**AAA**
Vendor Name	
Certification Date	
Hardware Model	
Software Version	
Use Case	
Routing & Access Control	AAA
SWVC Stability & Reliability	AAA
UCS Impairment	AAA
SWVC Application Assurance	AAA
SWVC Performance	
Combined Video MOS	
Combined Audio MOS	

MEF CYBER RATINGS.ORG

Report Cards for each certified Hardware Model:

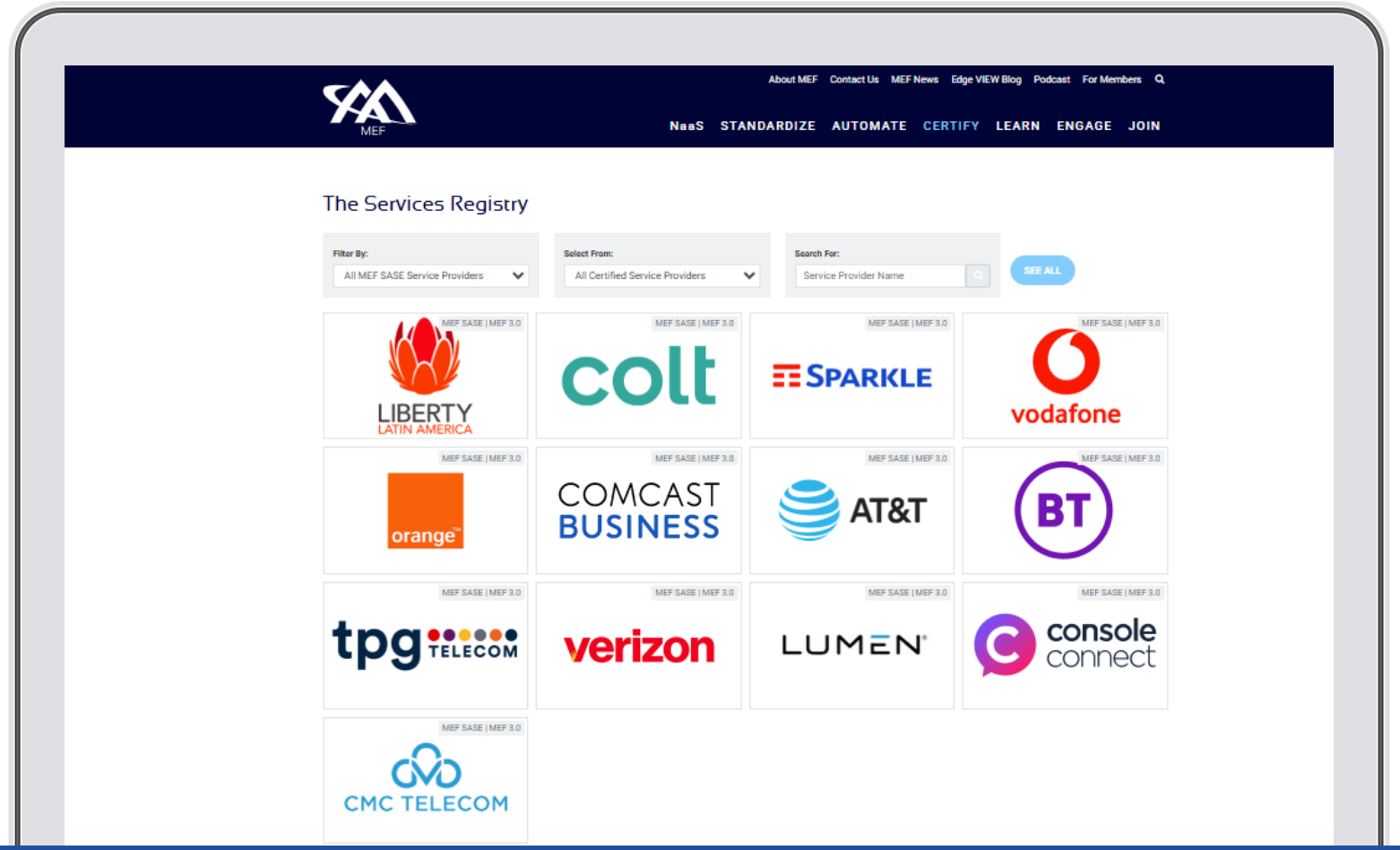
- Technology Provider Name
- MEF Certification Date
- Hardware Model
- Software Version
- Routing and Access Control Rating
- SWVC Performance Rating
- SWVC Stability and Reliability Rating
- UCS Impairment Rating
- Measured Throughput
- Video MOS
- Audio MOS

MEF Certified Technology Registry

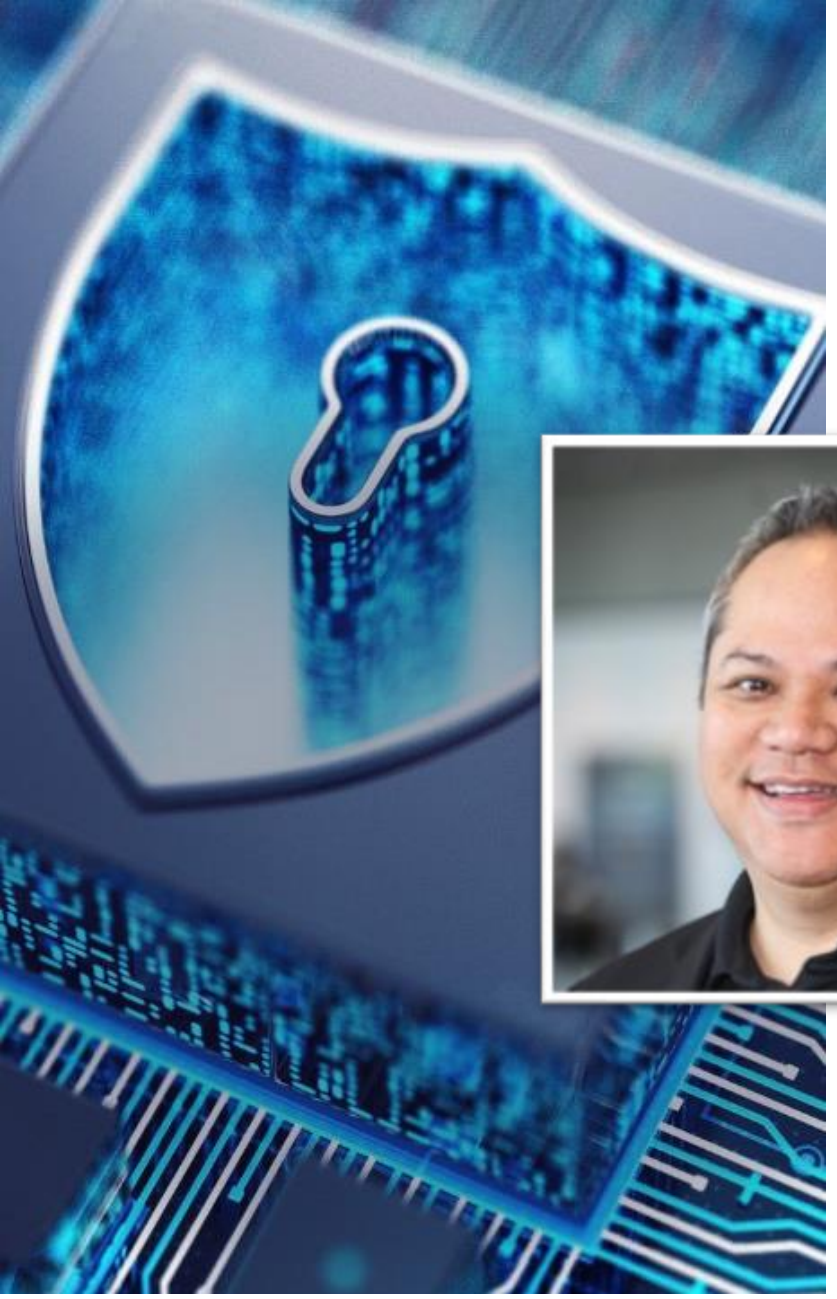


The MEF Technology Certification Registry is the authoritative listing of companies that have achieved MEF certification of their technologies.

MEF Certified Services Registry



The MEF Service Certification Registry is the authoritative listing of MEF member companies that have achieved MEF certification of their services.



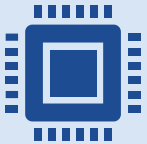
Ian Foo

CTO and EVP of Product,
CyberRatings.org

About CyberRatings.org

501(c)6 non-profit organization

Dedicated to driving transparency in the cybersecurity technology space.



Decades of experience in evaluating and validating cybersecurity technology and products by conducting in-depth testing.

Certification & Validation Through Rigorous Testing

The certification process for technology suppliers follows defined methodologies that validates important functions for each component technology area:

SD-WAN

- Application performance
- Application classification/prioritization accuracy
- Application Assurance & Protection

Zero Trust

- Granular Policy Enforcement & Access Control
- Identity Provider (IdP) Integration & SSO
- SSL/TLS Functionality
- Reporting & Management

SSE

- Exploit Protection effectiveness
  - Library of 250,000+ known exploits
- Evasion Resistance
  - 1000+ evasion techniques
- Malware Protection effectiveness
  - Library of 1,500,000+ real world malware
- False Positives Accuracy
- TLS/SSL cipher suite validation
  - Validation of “top 10” ciphers in use

SD-WAN Testing

Is the product or solution actually able to reliably deliver applications according to business requirements using a mix of public and private transport?

Application Performance: Real-world and worst case, not best case

Application Classification: Business critical vs best effort

Application Assurance: Business critical vs best effort when contention is an issue

Security Effectiveness (SSE) Testing

Does the product or solution actually provide effective protection against real-world threats that organizations are facing?

Exploits: a method used by threat actors to take advantage of a weakness in a computer system or software to gain unauthorized access or cause harm.

Evasions: techniques used by threat actors to avoid being detected by security systems while carrying out an attack.

Malware: harmful software designed to damage, disrupt, or gain unauthorized access to a computer or network.

Believe in data, not vendor sheets.

Zero-Trust Testing

Does the solution deliver on the promised components & capabilities of a zero-trust architecture approach?

Identity, device, location context awareness	Application/Service Policy Granularity	SSL/TLS Functionality & Cipher Support	Identity Provider (IdP) & SSO Integration

Kevin Vachon

COO,
MEF

PROMOTE YOUR CERTIFICATION

MEF Certification includes:

- The Report Card(s) documented for the Certification
- Publication in the MEF Certified Services Registry

The Marketing Kit includes the following:

- Introduction to Promoting Your SASE Certification
- SASE Certification Press Release Template
- SASE Certification Social Media Promotional Posts
- SASE Certification Sales Presentation Materials
- Certified SASE RFI Template for Enterprises

Contact: sase@mef.net to learn more

MEF Resources

At MEF.net, you'll find a comprehensive set of resources to support your SASE & SD-WAN certification journey, including:

- Certified SASE RFI Template for Enterprises
- State of the Industry Report: SASE
- 2025 NaaS Industry Blueprint
- NaaS Customer Experience White Paper

More About MEF's SASE Program Happening at the MEF's Members Summit

MEF

MEMBERS SUMMIT

19–22 May 2025 | London, UK

Hosted by BT


GNE
Global NaaS Event
10–14 November 2025
Live! by Loews | Dallas, Texas, USA
Accelerating NaaS Innovation
for an AI-Powered Digital World
Learn more at GNE.mef.net
MEF

NaaS Excellence Awards

2025

Submissions open
1 May

Conclusion

1. SASE and SD-WAN support secure digital transformation
2. We must collaborate & standardize to accelerate adoption of these solutions to address threats
3. Get MEF certified – gain a competitive edge and accelerate sales & procurement process

Q&A

Follow-on Questions or Feedback?

Feel free to email kevin@mef.net


MEF
WEBINAR
THANK YOU
GAIN A COMPETITIVE EDGE WITH
MEF-CERTIFIED SASE & SD-WAN
22 April 2025 | 10–11 am EDT

Resources & Information

State of the Industry Report - SASE

SASE & NaaS

Foundational SASE Standards

SASE Certification Testing Details

www.MEF/SASE

Covers
- Threats
- Trends
- Certified Solutions

State of the Industry Report on SASE:

Validating Cyber Defense in Era of Unprecedented Threats

June 2024

with Contributions from

AvidThink

Dell'Oro Group

Frost & Sullivan

Omdia

TeleGeography

Vertical Systems Group

with Support from

AT&T Business

Cisco

colt

Comcast Business

consoleconnect

CRO Cyber Ratings.org

Fortinet

Keysight

Liberty Latin America

Lumen

Microsoft Azure

orange

paloalto Networks

Sparkle

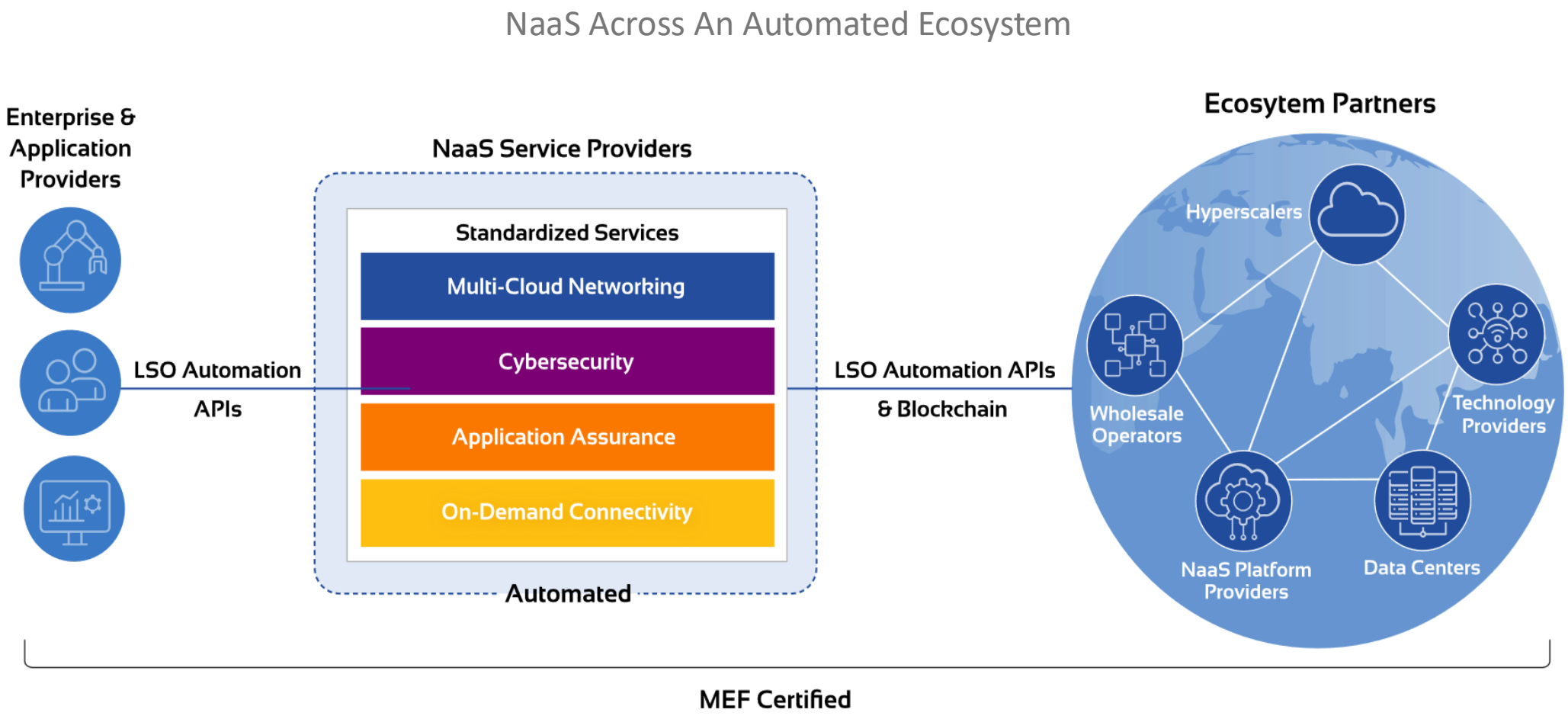
verizon

Versa

vmware by Broadcom

Certified SASE Smoothly Integrates Into NaaS Ecosystem

MEF has developed standardized, certified SASE within the context of the industry transformation toward NaaS across an automated ecosystem. Many organizations will evolve from SD-WAN to SASE and eventually NaaS with integrated SASE.



Foundational SASE Standards

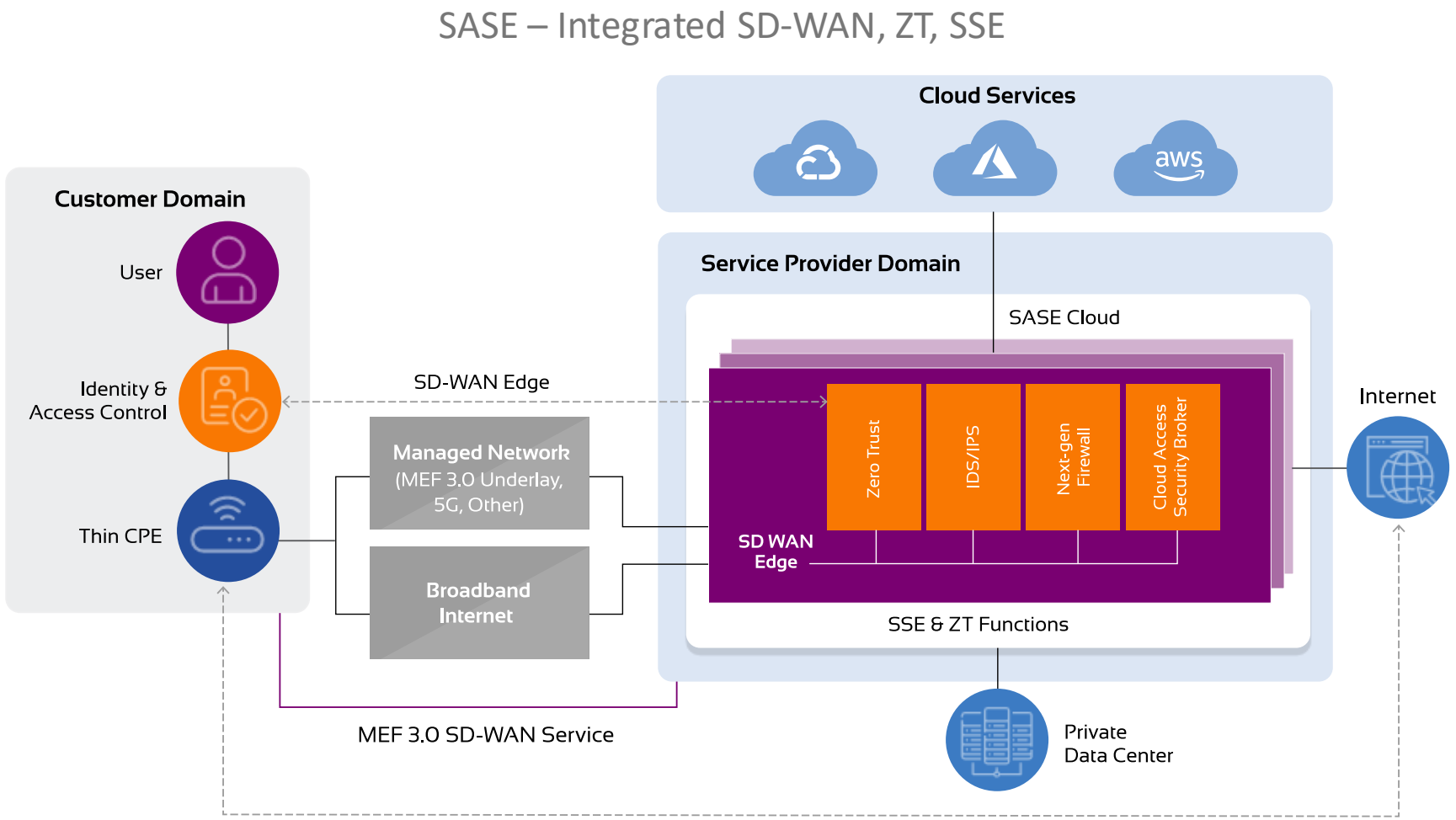
MEF has launched close to 30 SASE-related standards initiatives, with the four listed here being key standards.

MEF 117 / MEF W117.1
SASE Service Attributes and Services Framework

MEF W169
Security Service Edge Framework

MEF 118.1
Zero Trust Framework for MEF Services

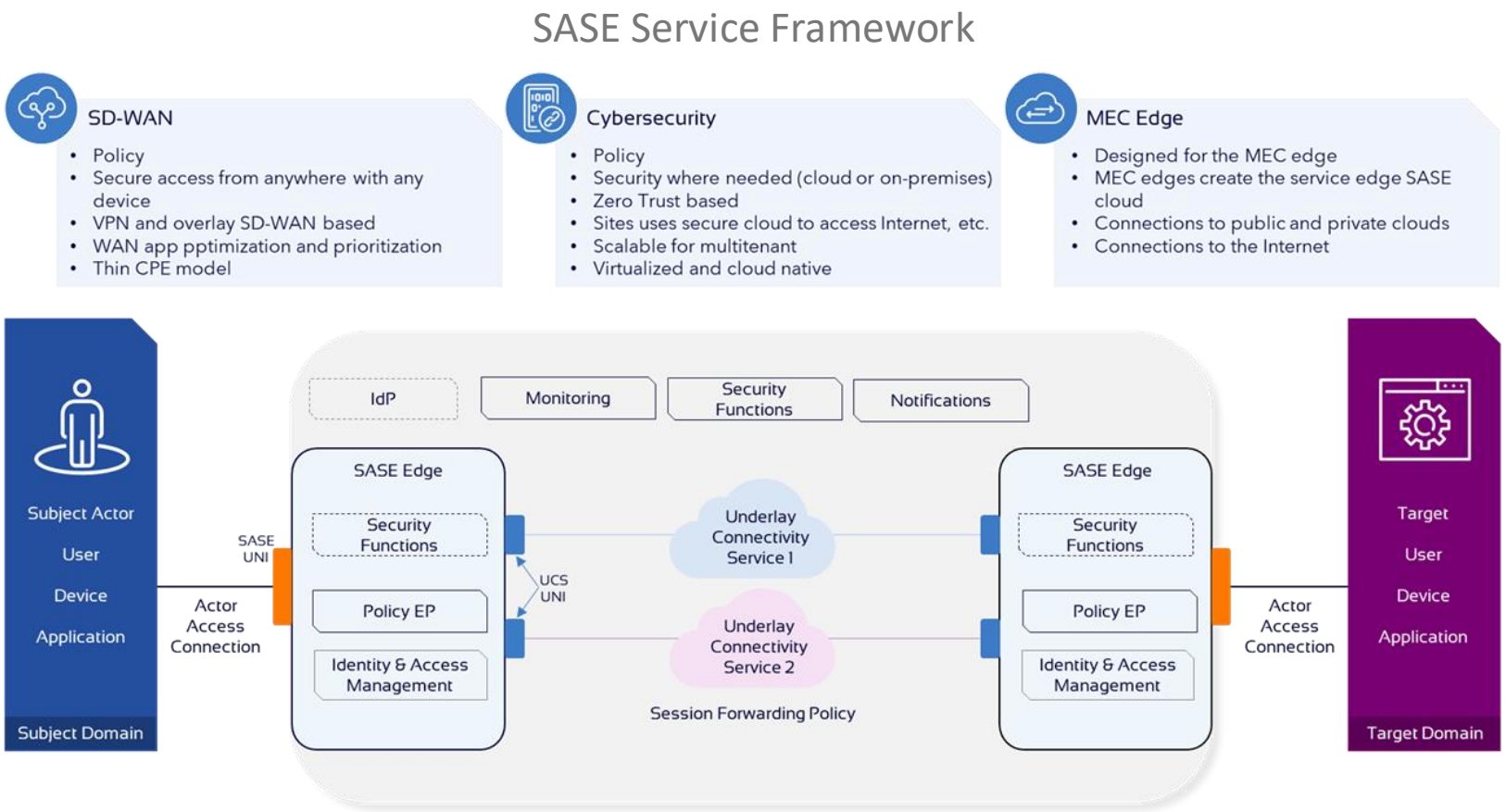
MEF 70.2
SD-WAN Service Attributes and Service Framework



MEF 117 & W117.1 SASE Service Attributes and Service Framework

MEF 117 & W117.1 define the attributes and framework for SASE services that combine network connectivity (SD-WAN) and cybersecurity functions (ZT and SSE) with subscriber policies.

A SASE service is an overlay service that integrates SD-WAN, ZT, and SSE to grant a subject actor (user, device, or application) secure access to a target actor (user, device, or application) for a given session. Access is based on the subject actor's identity, context, and role in accordance with the performance criteria and security policies set by the SASE service subscriber. This framework ensures scalability and adaptability, meeting the demands of hybrid work environments and multi-cloud architectures.

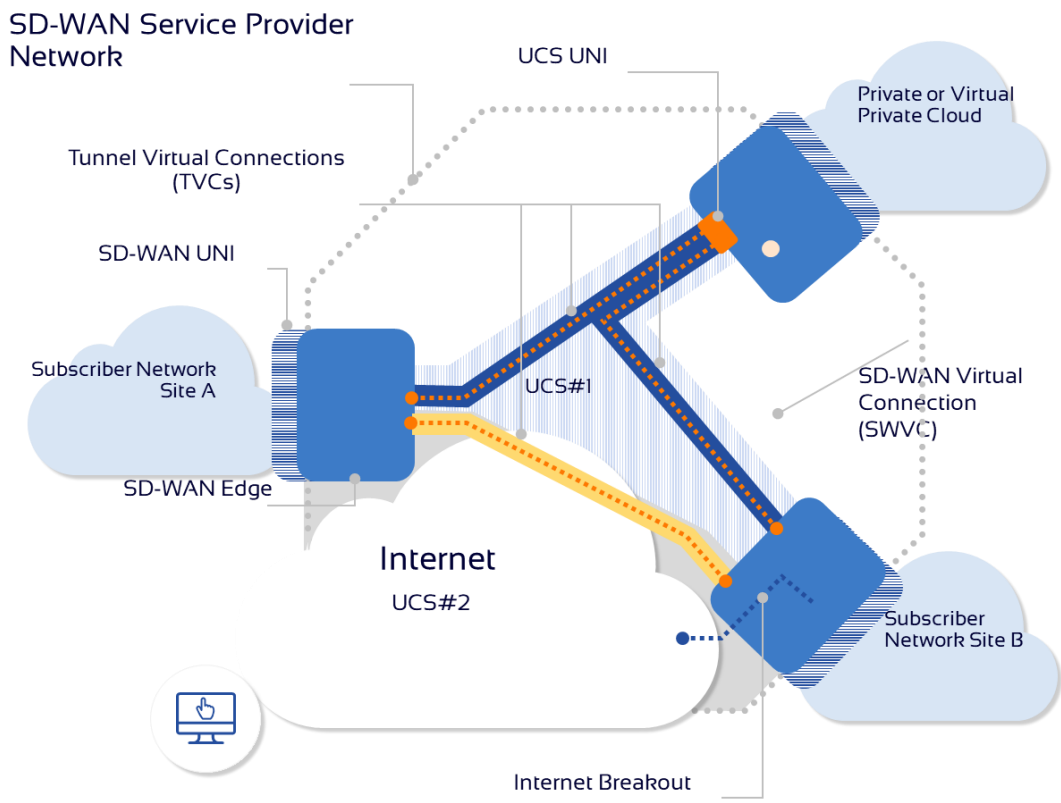


MEF 70.2 SD-WAN Service Attributes and Service Framework

MEF 70.2 defines SD-WAN as an application-aware, over-the-top WAN connectivity service that uses policies to direct application flows over one or more underlay networks.

MEF 70.2 outlines the foundational SD-WAN framework, covering service concepts, components, performance metrics, and policies for application flow security and virtual topologies. It also covers enhancements like dynamic path selection based on performance monitoring, prioritization of application flows during resource contention, and improved mechanisms for bandwidth sharing and performance metrics. SD-WAN serves as a critical component of modern SASE and NaaS solutions.

SD-WAN Service Components

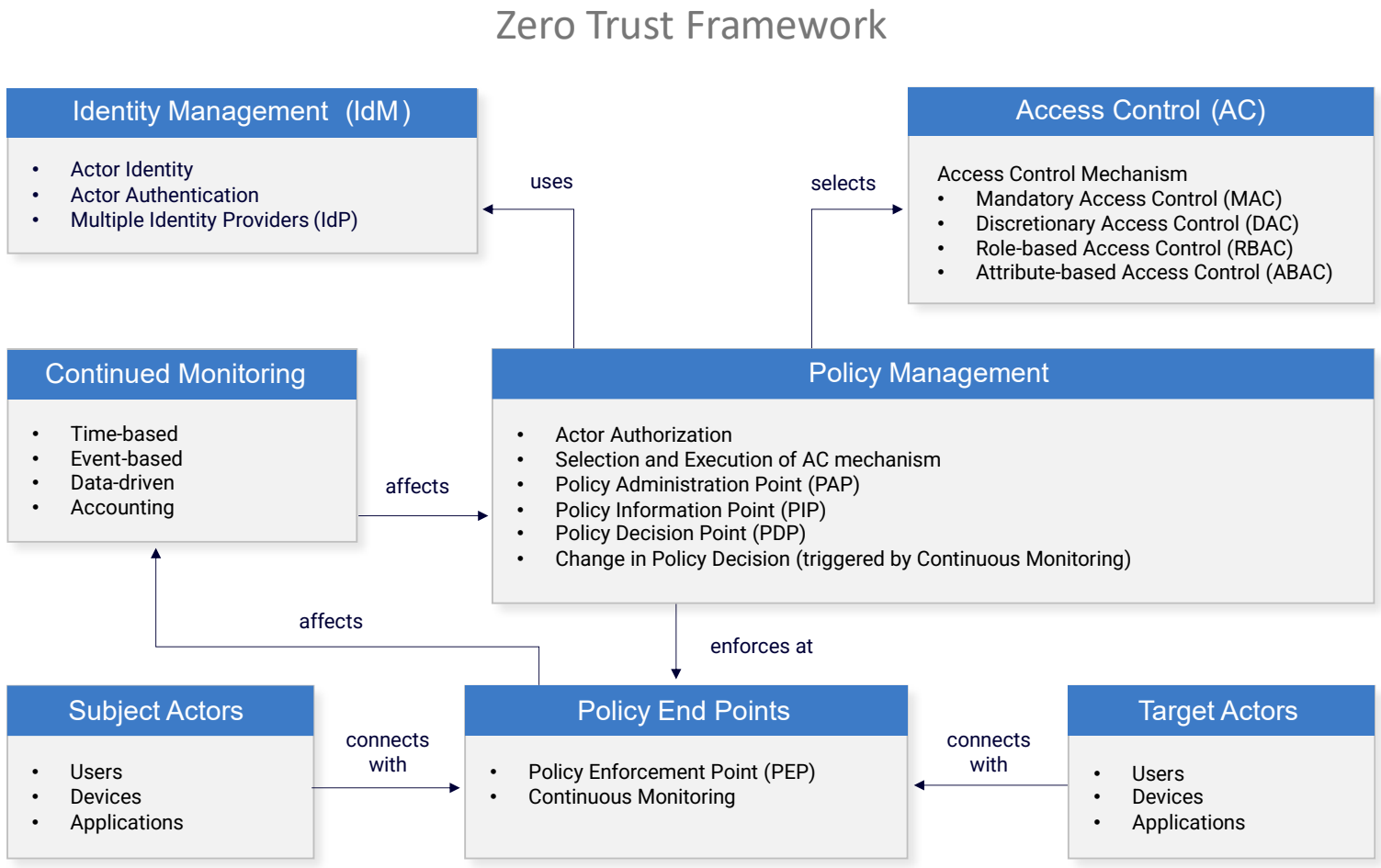


- **SD-WAN User to Network Interface (UNI)**
  Demarcation between Service Provider and Subscriber responsibility
- **SD-WAN Virtual Connection (SWVC)**
  Logical multipoint connection between the SD-WAN UNIs that corresponds to the SD-WAN Service
- **SD-WAN Virtual Connection End-Point (SWVC EP)**
  Logical point where application flow policies are assigned and applied
- **SD-WAN Edge**
  Connects SD-WAN UNI to UCSs, maps packets to application flows, enforces policies, and selects TVC over which to forward each flow
- **Underlay Connectivity Service (UCS)**
  Any WAN service used by the SD-WAN, e.g., MEF Ethernet Services (MEF 6.2), MEF IP Services (MEF 61.1), MPLS VPNs and Internet Access, and MEF Optical Transport Services (MEF 63)
- **Tunnel Virtual Connection (TVC)**
  Point-to-point paths across UCSs that compose an SD-WAN Service
- **Internet Breakout**
  Application Flows forwarded from an SD-WAN UNI directly to the Internet rather than delivered to another SD-WAN UNI.

MEF 118.1 Zero Trust Framework for MEF Services

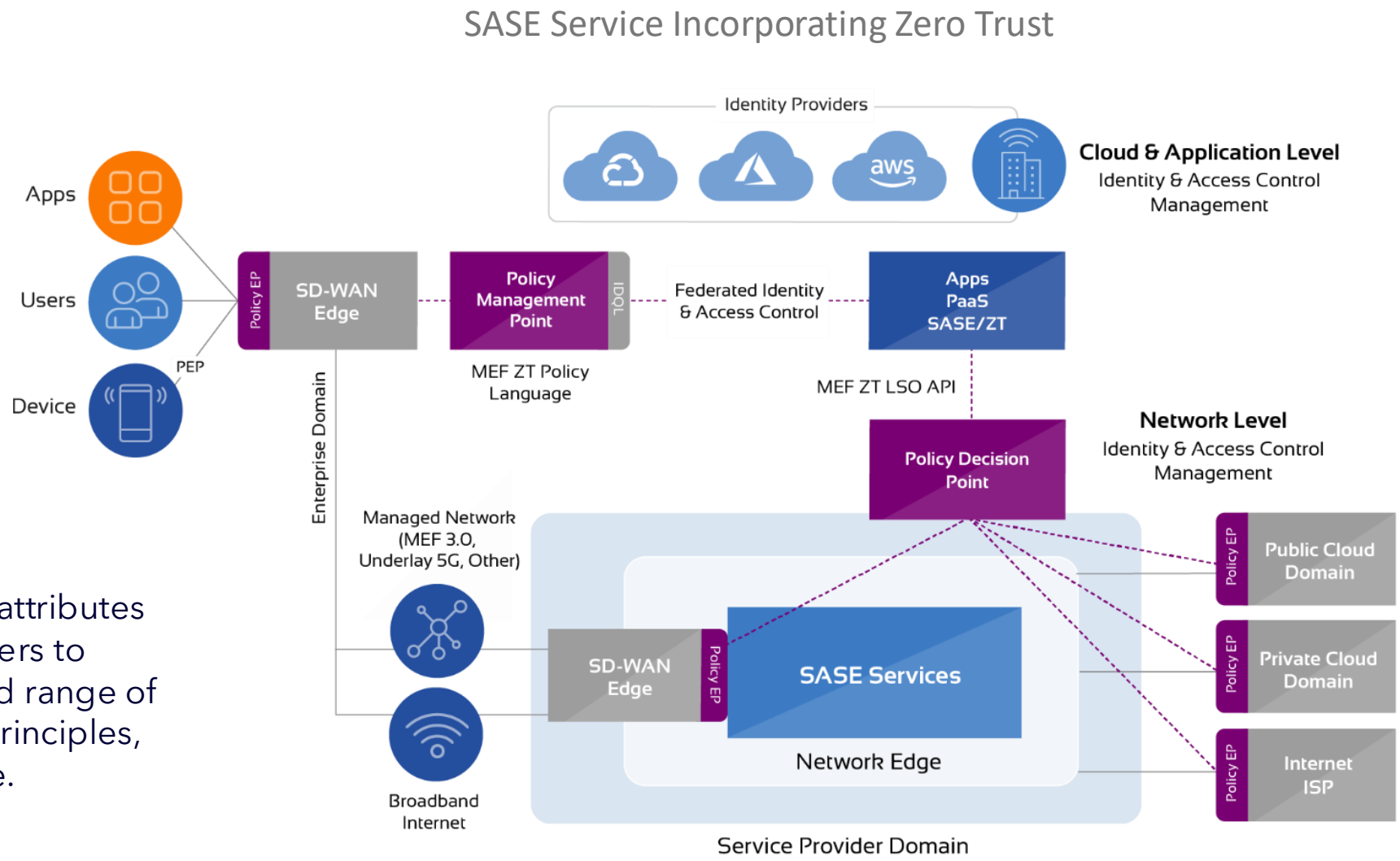
MEF 118.1 defines a Zero Trust Framework (ZTF) and service attributes for dynamic, policy-based access control, emphasizing identity management, access authorization, and continuous monitoring of users, devices, and applications.

ZT secures networked resources by removing the assumption of trust, employing micro-segmentation, real-time access evaluations, and continuous recalibration of policies during sessions. The standard includes requirements for multi-factor authentication (MFA), logging of authentication attempts for breach analysis, and risk scoring of actors. It also offers use cases, best practices, and provisions for non-programmatic interactions, such as AI-driven chatbot communication.



Zero Trust in SASE Service

MEF 118-defined ZTF service attributes can be used by service providers to implement and deliver a broad range of services that comply with ZT principles, as shown in the SASE example.

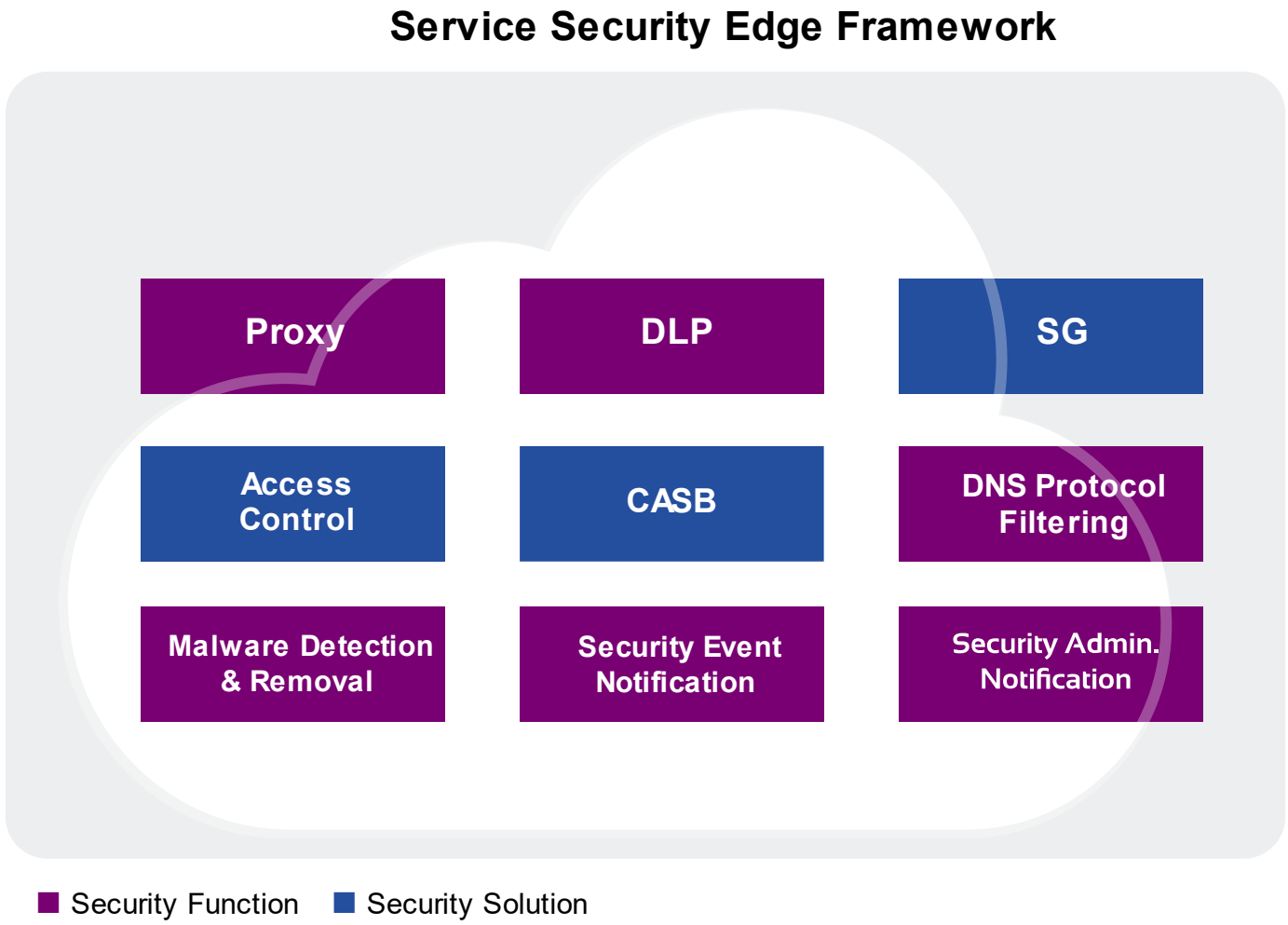


MEF W169 Security Service Edge Framework

MEF W169, currently in the working draft stage, defines the service attributes and framework for Security Service Edge offerings.

SSE is a security-centric pillar of SASE, focusing on cloud-delivered services to protect users, devices, and data. It enforces policies, monitors activity, and protects against threats across distributed environments. Key capabilities of an SSE offering include:

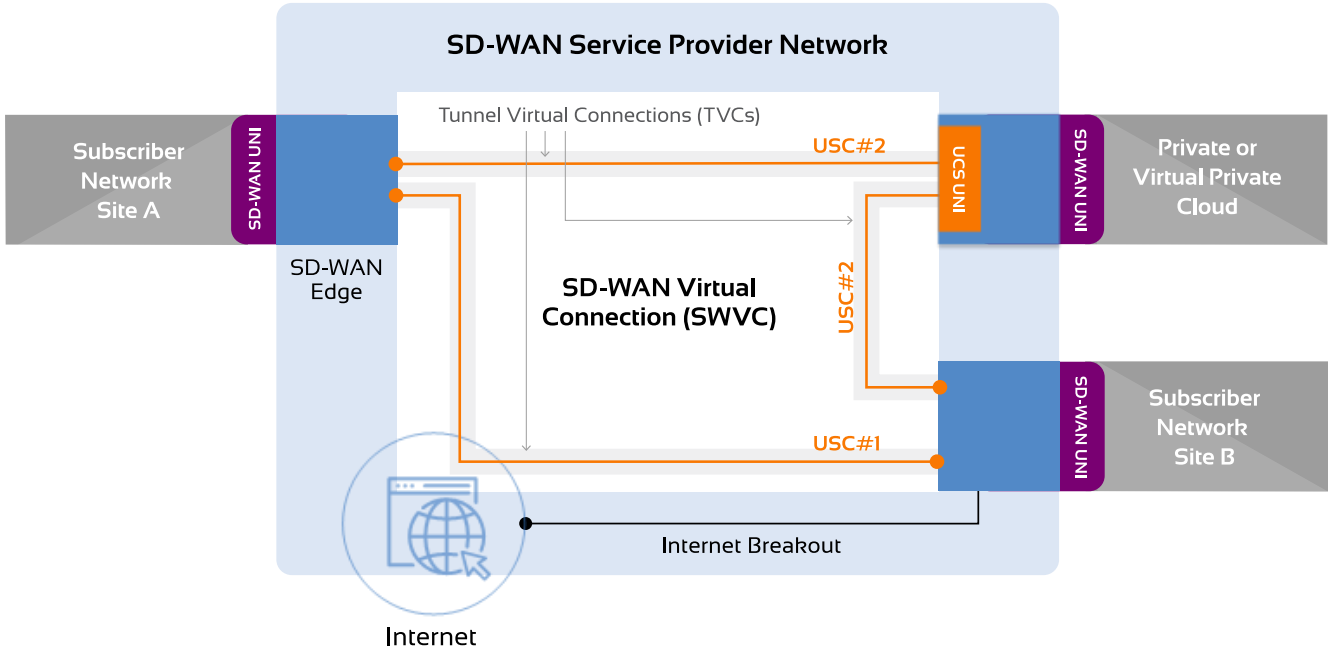
- Access Control
- Proxy
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Secure Gateway (SG)
- DNS Protocol Filtering
- Malware Detection and Removal
- Security Event Notification
- Security Admin Notification



MEF SD-WAN Certification

SD-WAN Certification is tested by creating a multi-node simulated enterprise network with each node having specific traffic and performance characteristics (e.g., Datacenter, Cloud, Corporate Office, Regional Office, Remote Office, Retail Outlets, etc.

Certification steps through various use cases (e.g., voice call, video call, access to files, data transfer, email, retail transaction, access to SharePoint, Salesforce, Dropbox, etc.).



SD-WAN policies are applied, and the SD-WAN is tested:

- Routing and Access Control
- WAN Impairments
- Performance
- Classification Verification
- Conformance to MEF 70.1 and future evolving standards
- Based SD-WAN Certification Phase 2 Requirement Specification IG 90.2

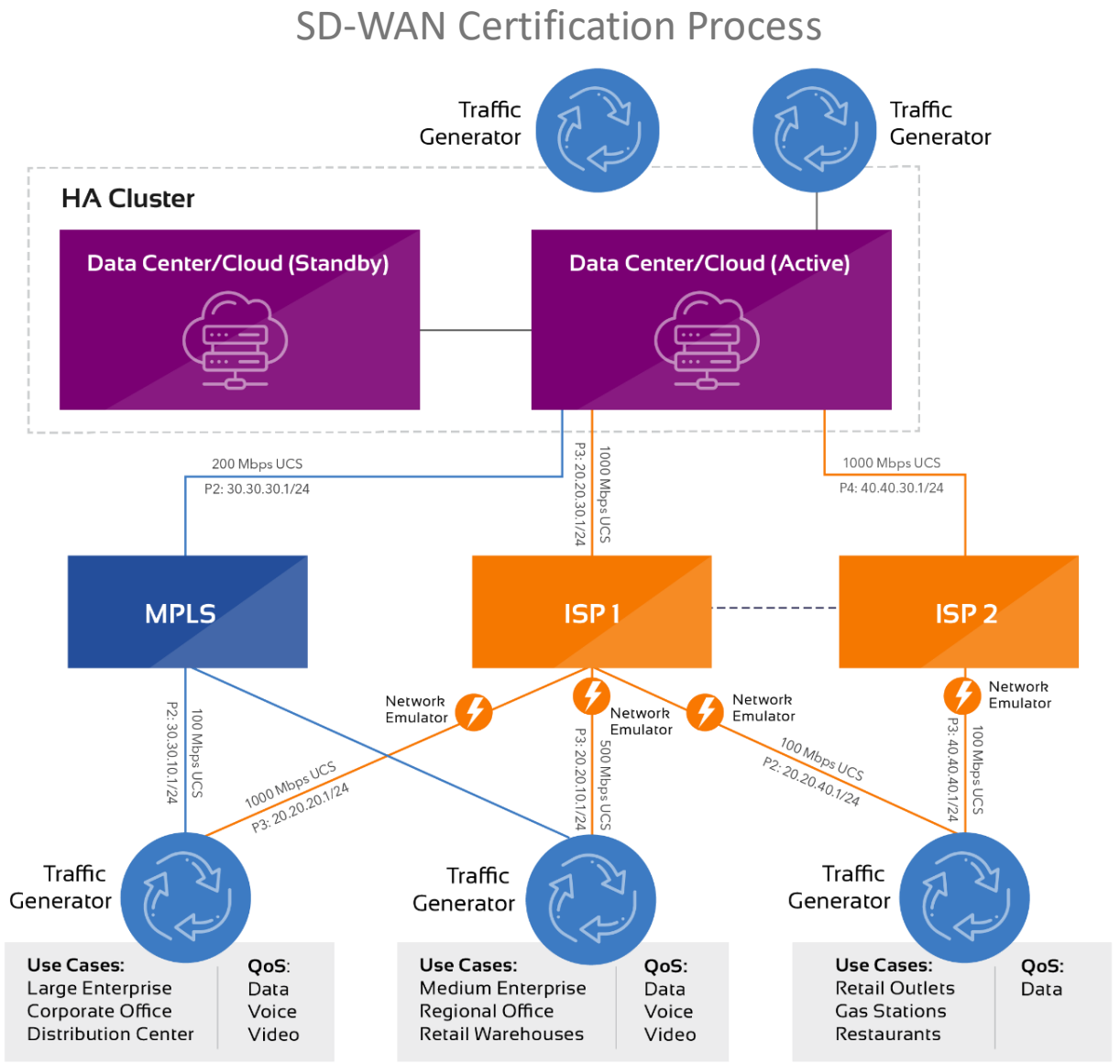
SD-WAN Certification Testing of Technology Suppliers

Testing Standard: MEF W90.2 SD-WAN Certification Test Cases & Requirements – Phase 2

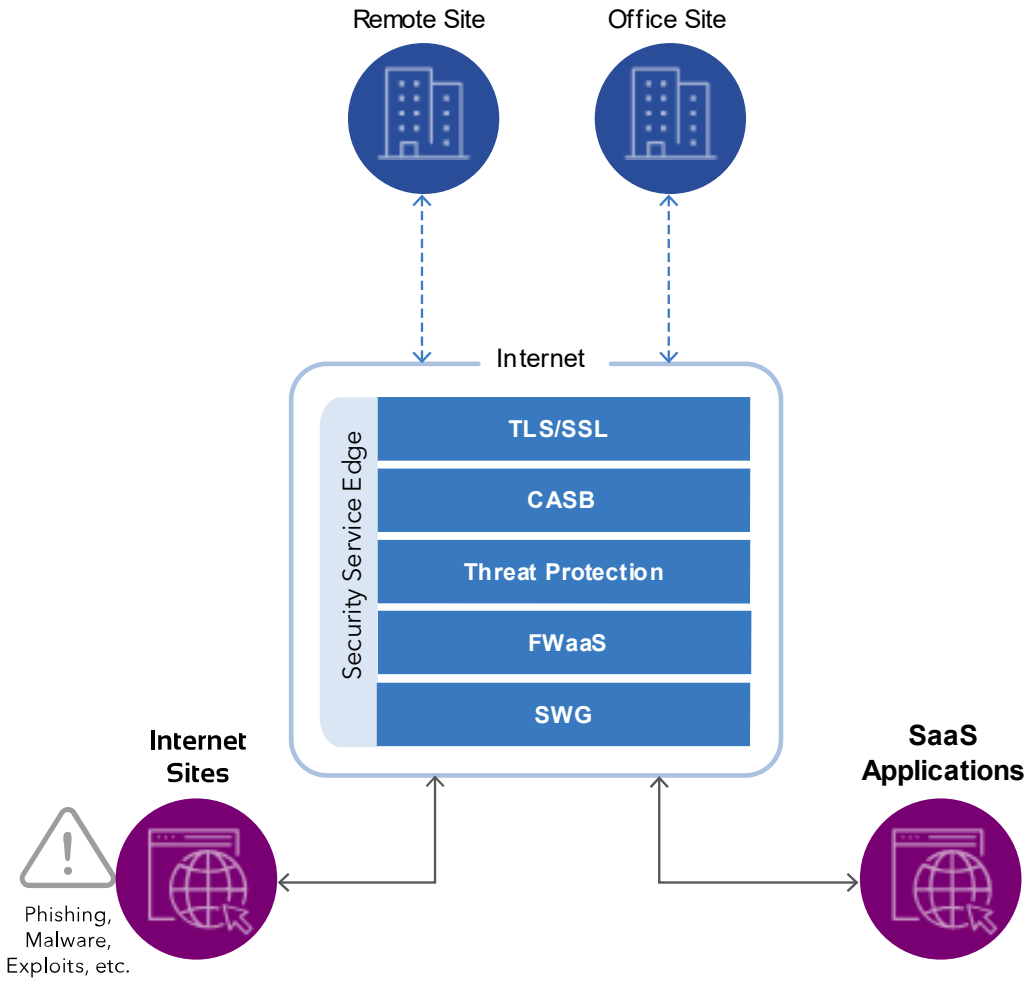
MEF W90.2 SD-WAN Certification Test Cases and Requirements – Phase 2 defines the test cases and requirements for SD-WAN certification.

The certification includes a test methodology that is not limited to just the service attributes defined in *MEF 70.1*, but also describes test cases for routing and access control, UCS impairment, SWVC performance, and SWVC stability and reliability.

Certification includes both conformance with *MEF 70.1* and ratings on defined test cases. The certification aims to inform customers which SD-WAN solutions are certified and most highly rated.



MEF Security Service Edge Certification



SSE Certification is tested by creating a multi-node simulated enterprise network with each node having specific traffic and performance characteristics.

Certification steps through various use cases for SaaS, IaaS applications and Internet Sites.

SSE policies are applied, and SSE is tested:

- Threat Protection (evasion, exploits and malware)
- TLS/SSL Functionality
- Scalability Performance
- Classification Verification
- Compliance to MEF 117, 88 & future evolving standards
- Based SSE Certification Requirement Specification IG

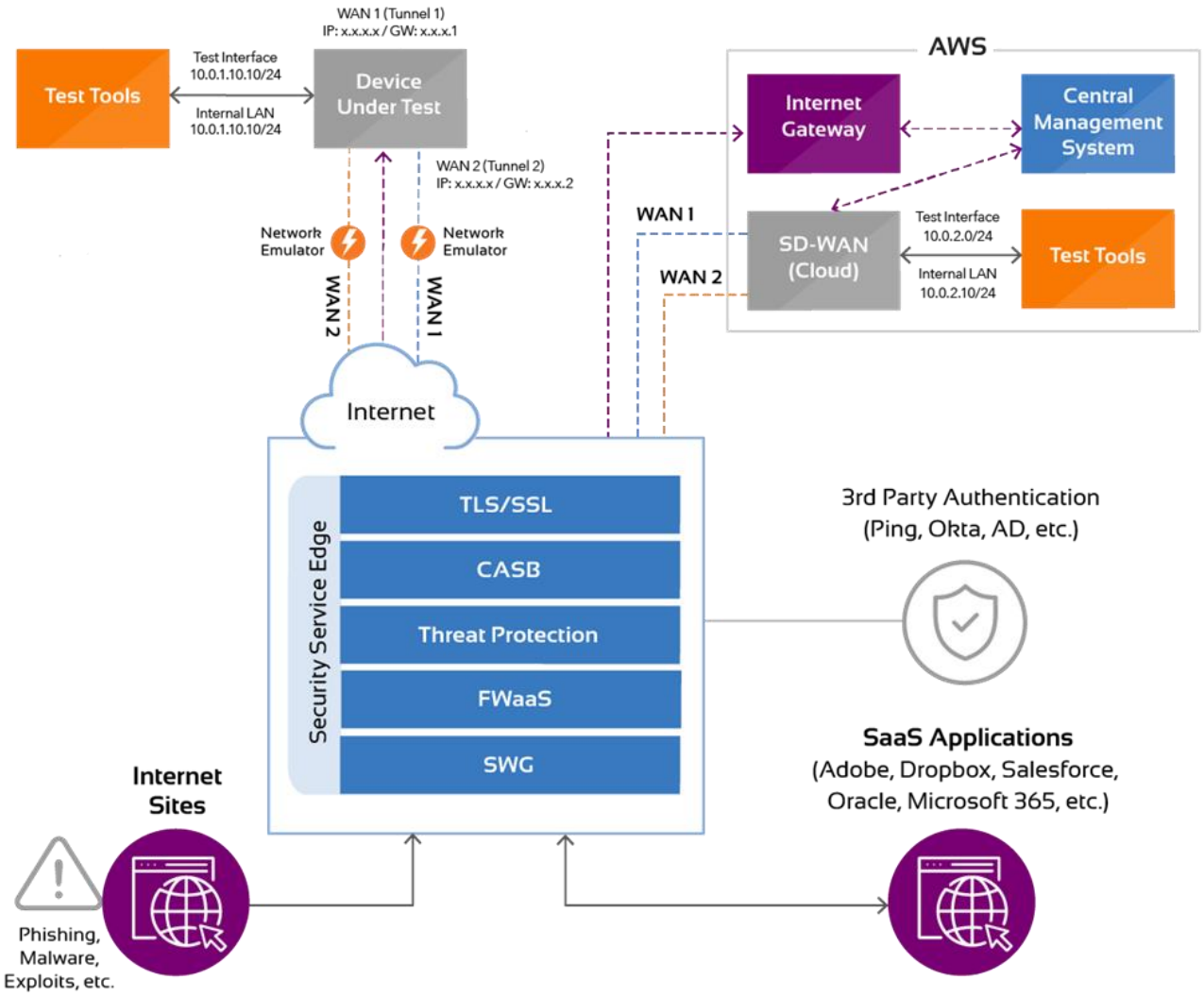
Security Service Edge Testing of Technology Suppliers

Testing Standard: MEF W162 Security Service Edge Certification Test Cases & Requirements

MEF W162 Security Service Edge Test Cases & Requirements defines the test cases and requirements for SSE certification. The scope of the test methodologies includes the following capabilities that are considered essential in any SSE offering: test traffic onboarding methods; segmentation, policy enforcement, and access control; decryption validation and bypass exceptions; threat efficacy testing; data protection validation; and performance impact, redundancy, and monitoring capabilities.

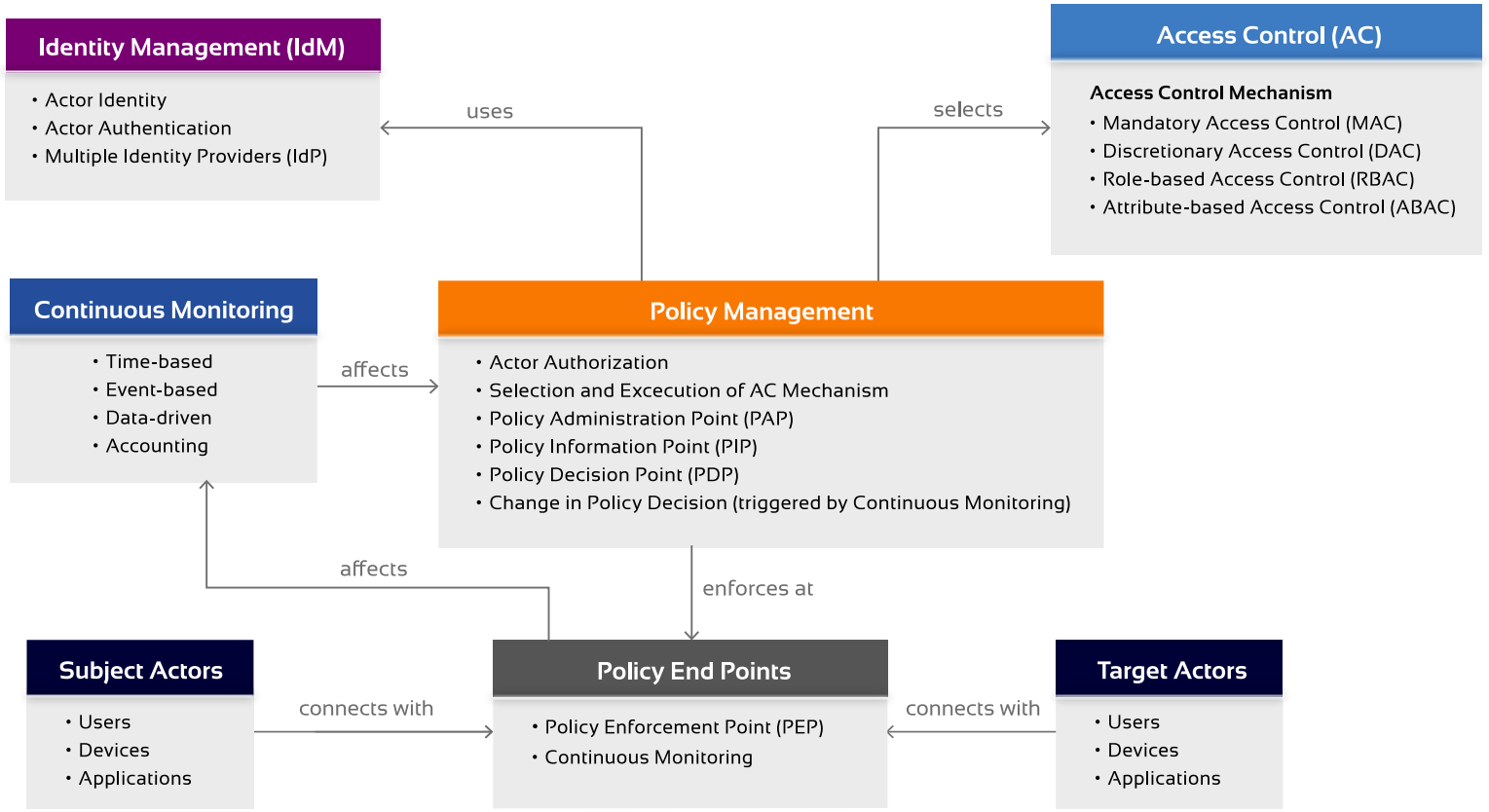
SSE technology is tested by creating a simulated multi-node enterprise network with each node having specific traffic and performance characteristics. Certification steps through various use cases for SaaS, IaaS applications, and Internet sites.

SSE Certification Process



MEF Zero Trust Certification

Zero Trust Certification is tested by creating a multi-node simulated enterprise network with each node having specific traffic and performance characteristics.



Certification steps through various use cases including:

- Access Control
- Zero Trust
- Authentication
- Policy
- Change Control
- Reporting capabilities including Logs and Reports
- Cloud Access/Application Control

Zero Trust Certification Testing of Technology Suppliers

Testing Standard: MEF W163 Zero Trust Certification

MEF W163 Zero Trust Certification defines the test cases and requirements for certification of ZT implementations. The scope of test methodologies includes the following capabilities which are considered essential in any ZT offering: policy enforcement and access control; authentication via integration with identity providers (IdP); reporting capabilities; and management capabilities.

ZT technology is tested by creating a simulated multi-node enterprise network with each node having specific traffic and performance characteristics. Certification steps through various use cases.