
MEF
19

MEF19

Application Security for SD-WAN Services

Nicolas Thomas

SDN/APIs Strategist
Fortinet

Motivation – Enterprises are Overwhelmed

Enterprises are overwhelmed in handling IT security defense-in-depth postures

2018 Cost of a data breach
$3.86 million.* **+6.4%**

2021, cyber crime cost to global economy
$6 trillion in damages, annually.

Soft costs:

1. loss of brand equity
2. post-breach, stock prices fall avg of **5%**
3. customer churn increases up to **7%**.*

Security/Privacy Regulations
Adherence to regulations is challenging with large potential liabilities and fines.

- European Union's General Data Protection Regulations (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standards (PCI DSS)
- Manufacturing's International Traffic in Arms Regulations (ITAR)
- California SB 1386
- The Gramm-Leach Bliley Act (GLBA)
- The Sarbanes-Oxley Act
- Family Educational Rights and Privacy Act (FERPA)
- Cybersecurity Information Sharing Act
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Freedom of Information Act (FOIA)

*Source: 2018 Ponemon's benchmark research

Definition and Benefits of Security-as-a-Service (SECaaS)

SECaaS is an outsourced service. An outside company handles and manages security for a given company.

Security solutions are no longer delivered locally. Instead security is outsourced to an external party using cloud based technologies with a SLA.

Definition

Benefits

- Latest & most updated security solutions available
- Best-of-breed, dedicated expertise
- Faster provisioning, increased agility to face dynamic security threat landscape
- Security focus with automation & tooling
- Simpler, cost-effective in-house security management
- Replaces capital burden with more economical operating expense

SECaaS Broad Market Potential

Worldwide Security Spending by Segment, 2016—2018

(Millions of Current Dollars)

Segment	2016	2017	2018
Identity Access Management	3,911	4,279	4,695
Infrastructure Protection	15,156	16,217	17,467
Network Security Equipment	9,789	10,934	11,669
Security Services	48,796	53,065	57,719
Consumer Security Software	4,573	4,637	4,746
Total	**82,225**	**89,133**	**96,296**

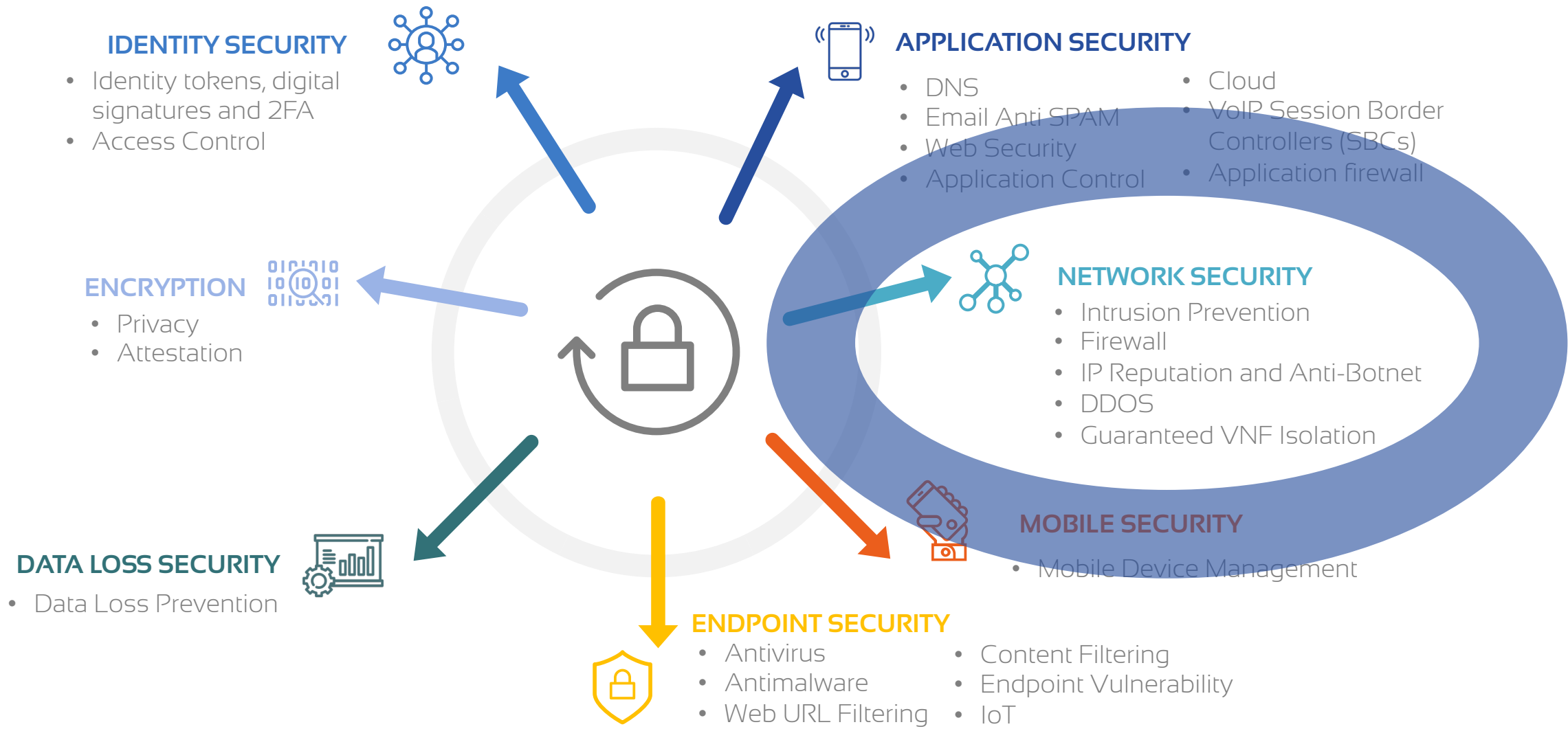
Enterprise security services spending will total **$57.7B** **in 2018.**

By 2020

MORE THAN **60%** of organizations will invest in multiple tools such as data loss prevention, encryption, and data-centric audit and protections tools. This is up from about 35 percent today, according to Gartner.

Source: Gartner and SDx Central https://www.sdxcentral.com/articles/news/enterprise-security-spending-will-total-96-3b-2018-gartner-says/2017/12/

Security is broad



MEF w88 Application Security for SD-WAN

MEF

Zone-based Access Use Case

Business Model

- Subscriber ABC buys SD-WAN service from *SD-WAN SP* and wants to attach Branch Site X to the service, as shown, with agreed security functions.

Zone Model

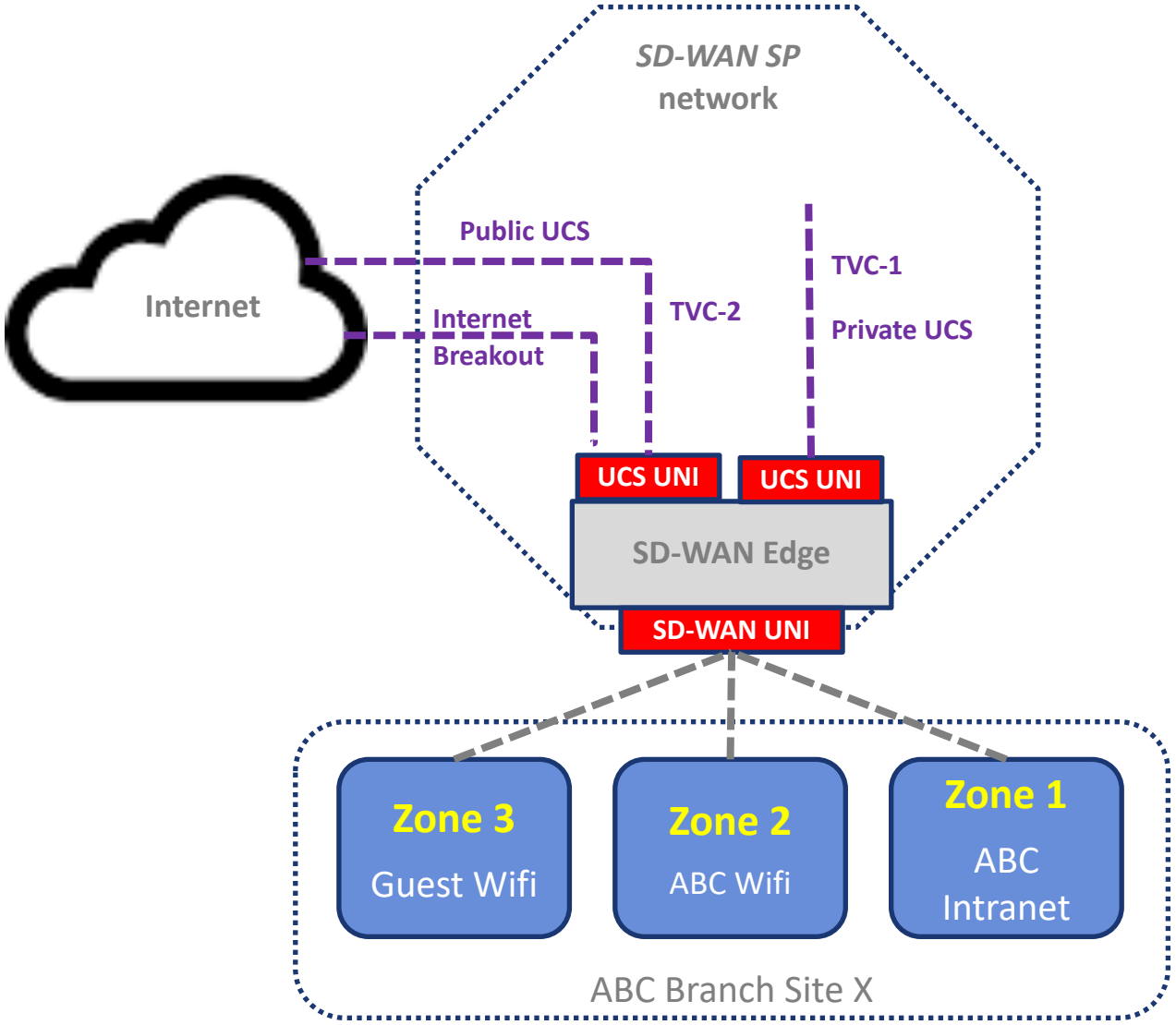
- Subscribers think in terms of zones - a zone is typically identified by a range of unique IP addresses at each site.
- Each zone is expected to be an isolated part of the customer's network (physical, virtual, etc..) under the customer's responsibility, i.e., zones are isolated from each other.
- Zones have relevance to SD-WAN Service in general.

Mapping Application Flows to UCSs

- Subscriber ABC and *SD-WAN SP* agree on the mapping of AFs within each zone to the UCSs, and on the security policy to be applied to each.

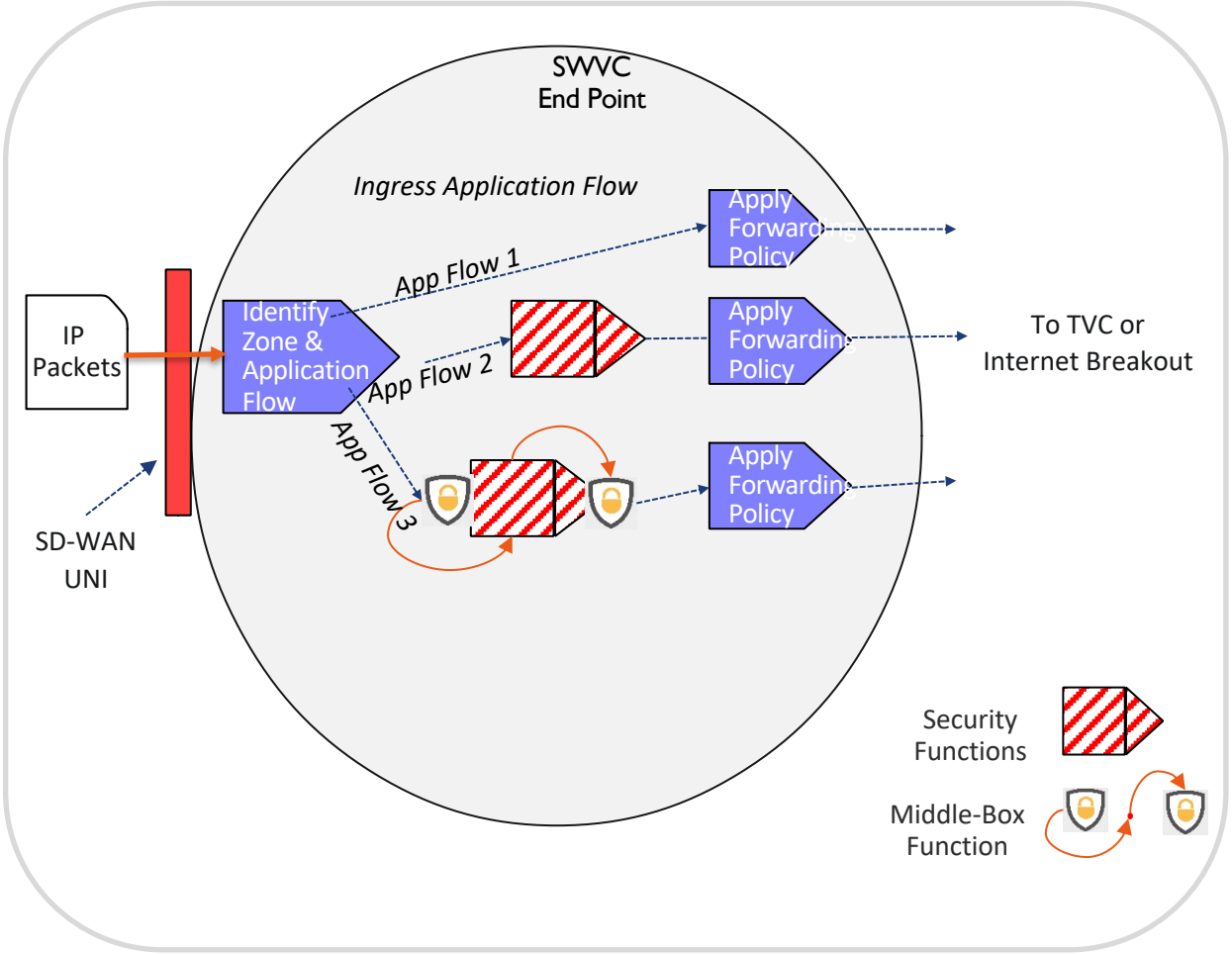
Security Functions

- Security functions can be applied on ingress and/or egress to specific Application Flows (AFs) per zone.
- Some AFs may be forwarded (e.g., no security threat), some may be blocked (e.g., security threat), some may be cleaned (e.g., security threat removed and the rest of the file forwarded), and some may be further rate limited.



Middle-box Function (MBF)

- MBF: a set of functions used to decrypt and re-encrypt the Subscriber's TLS sessions
- The term is adapted from ETSI (middle box)
- MBF support for TLS 1.2 is mandated
- An Application Flow can:
  a) By-pass security functions
  b) Have security functions applied without a MBF
  c) Use a MBF to see encrypted traffic in clear (and then security functions can be applied)



Security Functions - 1

Security Function	Description
DNS Protocol Filtering	When *enabled*, check whether DNS queries should be re-directed (based on metadata and/or reputation of the associated domain name).
Domain Name Filtering	When *enabled*, check whether access to a domain name should be blocked (based on Whitelist / Blacklist, metadata and/or reputation)
URL Filtering	When *enabled*, check whether access to a URL should be blocked (based on Whitelist / Blacklist, metadata and/or reputation)

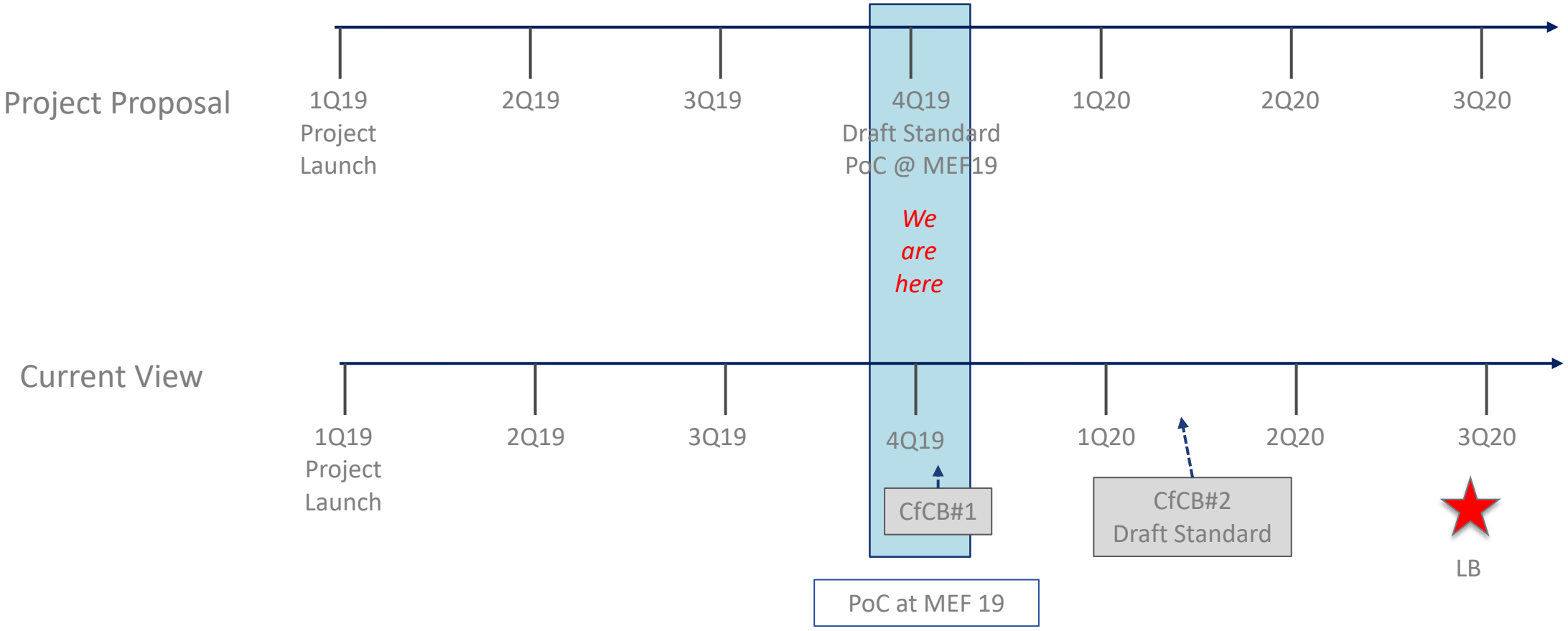
**Discussion planned in LA re: keeping these filtering functions separate or combining them into a 'web filtering service' – use case discussion possible*

Security Functions - 2

Security Function	Description
Malware Detection & Removal	Indicates whether or not the Application Flow requires detection and removal of malware
Data Leak Protection	Detect and block known sensitive data exfiltration (passwords, credit card, API token)
Network IDS / IPS	IDS: Detect possible incidents IPS: Attempt to stop detected incidents
Compromised System Notification (CSN)	Provides notification (internal or to Sub) re: Indicators of Compromise (IoC) – virus signature, MD5 hashes of malware files, URLs/domain names of botnet command & control servers

Q: How do we address DDoS attack? Use cases, requirements discussion in LA?

Project Schedule




MEF
19