



Secure Web Gateway

Guide



carahsoft.

For more information, contact Carahsoft or our reseller partners:
CAmarketing@carahsoft.com | 703-871-8539

The background features a dark gradient with a pattern of binary code (0s and 1s). Several hexagonal icons are scattered across the scene, including a computer monitor, a group of people, a cloud, a Wi-Fi signal, a padlock, a document, and a server rack. A large, prominent shield with a padlock inside is centered in the upper half of the image.

Discovery Guide

Symantec Secure Web Gateway

July 2020



Secure Web Gateway | Introduction

A brief introduction to Secure Web Gateway

INDEX

[Key Personas](#)

[Positioning](#)

[Prospecting](#)

[Competitive Battlecards](#)

[Proof Points](#)

[What is Secure Web Gateway](#)

[Customer Win Examples](#)

THE CHALLENGES OF WEB SECURITY

Enterprises face four primary challenges for effective Web Security:

1. New, sophisticated threats are going beyond simple, web-based attacks and organizations require more demanding security measures to properly protect against threats targeting web, cloud and application environments and ensure a safe user experience.
2. Disjointed solutions that require multiple agents can hurt network performance and lead to a poor user experience.
3. The volume threats hiding in encrypted traffic creates a challenge for threat detection, protection and remediation.
4. Digital Transformation can add to the cost and complexity of supporting on-premises, in the cloud, at headquarters or branch offices or with remote users.

HOW SWG TECHNOLOGIES HELP

Modern SWG solutions provide the critical termination point so all web traffic can be analyzed and fully inspected for threats to protect the organization and ensure a safe and productive user experience

- **Defense in depth** – Multiple inspection layers (site categorization and risk scoring, reputation, anti-malware engines and sandboxing) identify more threats and prevent advanced attacks.
- **Massive Threat Intelligence** – Analyze and categorize all web traffic and cloud applications using the world's largest civilian threat intelligence network
- **Secure SSL Inspection** – stronger TLS protocol support and cryptology are needed to preserve encryption strength.
- **Choice of implementation** – Enterprise-grade on-premises physical or virtual appliances, public/private cloud deployments or hosted security services

SYMANTEC SWG COMPONENTS

Symantec SWG solutions includes various security components:

- **Secure Web Proxy** provides the critical termination point to stop threats
- **Encrypted Traffic Visibility** to see all threats avoiding detection
- **Web Isolation** for safe web browsing
- **CASB** application identification to ensure approved cloud app use
- **Multi-layered file inspection** and sandboxing to analyze unknown content
- **Cloud Firewall** to create a secure cloud network perimeter
- **Universal Policy Enforcement** to ensure consistent security across on-premises, virtual, cloud or hosted services
- **Intelligence Services** to tap into Symantec's Global Intelligence Network for the latest threat details

Proxy/Web Security

Personas & Pain



**Network
Operations**
Becca

Pain Points

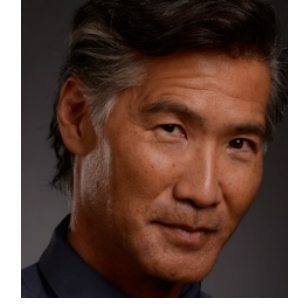
- Backhauling web traffic to enforce security/compliance controls is costly, slow, and inefficient.
- Managing an on-premise/hybrid environment can be complex and time-consuming, requiring lots of cycles from limited resources.
- “Over-blocking” web access is upsetting users
- Time-consuming to manage VPN access policies for Apps moving to IaaS



**Network Security
& Security Arch**
Marcus

Pain Points

- New advanced threats are getting around our traditional defenses, targeting C-levels, and will get me noticed for the wrong reasons.
- Lack of SaaS app controls is a huge compliance and security risk.
- Secure access to corporate applications using technologies like VPNs is complicated, costly and insecure, especially considering today’s mobile workforce, mix of managed and BYOD devices, etc.



**C-Level
(CISO/CIO)**
Grant

Pain Points

- Increased complexity and costs of trying to secure their organization as it goes through its digital transformation
- Need to align with tenants of emerging concepts like Zero Trust Security and SASE
- Lack of talent/resource to manage & deploy infrastructure
- Want to be viewed as a business enabler by their C-Level peers

Secure Web Gateway | Positioning



Elevator Pitch

Symantec™ Secure Web Gateway (SWG) delivers a sophisticated ecosystem of technologies to protect your organization from advanced threats – in the cloud, across the web or in corporate or remote networks. Symantec SWG solutions deliver strong proxy-based security in the form factor your organization needs: on-premises appliance, virtual appliance, in public or private clouds, as a hosted security service – or in a unified hybrid combination deployed as you need it.

Market Trends

Rise in Web Attacks

- One in 10 URLs are malicious
- 70%+ of malware in 2020 will use encryption to hide
- Web Attacks are up 56%
- Supply Chain Attacks up 78%
- Enterprise Ransomware up 12%
- 25% increase in the number of attack groups using destructive malware

Impact of Data Breach

- Average cost of a breach \$3.9M US

Leading Questions

What security layers do you employ to deal with web-based threats?

What do you do about targeted attacks?

Are you using Secure Web Gateway primarily for compliance?

How do you inspect encrypted traffic?

Are you aware of the recent advancements in Symantec's SWG technologies?

Value Proposition

In <15 words:

Symantec SWG provides comprehensive threat protection against attacks targeting your web, cloud and network environments.

In <75 words:

Symantec SWG provides a comprehensive portfolio of security technologies to detect and prevent sophisticated web-based attacks by utilizing industry-leading proxy-based architecture, in-depth content inspection and massive threat intelligence for integrated cyber defense. With granular policy control, and deployment options to meet any organization's needs, Symantec SWG ensures the protection of your web, cloud or network environments and a safe and productive user experience.

Differentiators

Layered Defense

Proxy-based architecture combined with layered content inspection and sandboxing, web application classification, web isolation and cloud firewall create the ultimate defense

Encrypted Traffic Management

Symantec SSL decryption technology ensures complete visibility without compromising cipher integrity

Web Threat Protection

Integrated CASB components and Web Isolation ensure accurate web application control and a safe browsing experience

Deployment Flexibility

Unlike competitors, Symantec offers flexible deployment options including on-premises, virtual, public/private cloud, hosted security service or hybrid

Leadership

Symantec is recognized as a leader in SWG technology by customers and analysts, including a leader in Gartner's Magic Quadrant for for 12 years in a row.

Proof Points

Analyst Quotes

"The ProxySG and Advanced Secure Gateway (ASG) families remain the strongest proxies in the market in terms of breadth of protocols and the number of advanced features. It also supports multiple authentication and directory integration options."

"Symantec's cloud service is a good option for most enterprises, particularly those that require hybrid (cloud and on-premises) implementations."

- Gartner SWG MQ, 2019

Gartner Customer Choice Quotes

- "Proxy solution complete, versatile and very granular"
- "The best product you can use to ensure our users' internet security"
- "Good performance and scalability."
- "Great cloud protection for all user endpoints"



Secure Web Gateway | Prospecting

How to position and sell Symantec Secure Web Gateway

Goal	Challenges	Discovery	Positioning	Enablement
SELL SWG INTO NEW ACCOUNTS	<ul style="list-style-type: none"> Customer is worried about protecting their organization from web-borne threats and sophisticated attacks that bypass traditional defenses. Customer feels the pressure to move their security to the cloud but have reservations that limit their progress. Customer is experiencing a massive increase in encrypted traffic and they struggle to have visibility they need. 	<ul style="list-style-type: none"> What issues do you have controlling where users go on the internet, and preventing infected systems from relaying private information? What security tools do you employ for web-based threats? What do you do about targeted attacks? What is your approach to multi-layered defense-in-depth security? 	<ul style="list-style-type: none"> If customer owns one or more other Symantec products, then position the PLA If customer does not own any Symantec products, then position Symantec SWG solution or the Network Security PLA. 	<ul style="list-style-type: none"> SWG Training and Partner Resources SWG Customer Deck
Assets	Awareness	Education	Validation	Adoption
BUYER & CUSTOMER JOURNEY	<ul style="list-style-type: none"> Video – Cloud Network Generation Next Generation Secure Web Gateway: The Cornerstone of Your Security Architecture Securing the Digital Transformation with Symantec SASE Webinar: Symantec Network Security 	<ul style="list-style-type: none"> Why Chose Symantec Eight Things to Know About a Secure Web Gateway 5 Steps to Ensure Strong Advanced Threat Protection White Paper – Three Reasons Secure Web Gateway is Vital for your Security Stance Secure Web Gateway Appliances Data Sheet FAQ – SWG Hardware and Licensing 	<ul style="list-style-type: none"> Gartner 2019 MQ for SWG KC 2020 Compass for Network Detection and Response Radicati Corporate Web Security Market Quadrant 	<ul style="list-style-type: none"> ProxySG Licensing Guide

Zscaler Battle Card



ZSCALER APPROACH

Sell the cloud-only story

- Position the Zscaler solution as the simplest to deploy and manage with no hardware/software – 100% cloud. **Virtual Zscaler Enforcement Nodes** (vZEN) may still be a necessary add-on for “scalability and load distribution”.

In competitive situations bid a lower priced suite

- Zscaler offers many different product packages. Functionality varies widely from one suite to another. Some suites don’t include mobility or SSL inspection. They may appear to be less expensive this way.

SYMANTEC APPROACH

Best-in-class Secure Web Gateway (SWG) cloud-service across access control, malware protection, information security, and CASB; with hybrid deployment flexibility

- Symantec SWG has been recognized as the market-leader for more than 12 years.
- Comprehensive defense-in-depth and integration with our other market leading security products, e.g. ATP, CASB, DLP, Sandboxing, Symantec Endpoint Protection (SEP + SEP Mobile), Web Isolation, and Secure Access Cloud.
- World’s largest civilian threat intelligence network utilizing data from thousands of engineers and researchers. Plus, intelligence detected and discovered by our comprehensive security stack.

KEY CAPABILITIES	Zscaler	Symantec
Web App Visibility (CASB)	Partnership (Bitglass, McAfee & Microsoft)	Yes (30K+)
Web Isolation	Yes (Appsluate)	Yes
Data Loss Prevention (DLP)	Basic w/ limited Exact Data Match (EDM) features	Yes (MQ & Wave leader)
ATP/Malware Analysis	Yes	Yes
Predictive File Analysis	No	Yes
SSL Inspection	29 Cipher Suites	40(SG) & 20(WSS) Cipher Suites
Endpoint Integrations	No	Yes (SEP + SEP Mobile)
*Data Centers	Claims 100+; ~48 listed. Not identical, ISO 27001	40, ISO 27001 & SSAE
Email URL Protection	No	Yes
Office 365 Inspection	Yes (Bypassed recommended)	Yes
Secure Access Cloud**	Yes (ZPA)	Yes
Cloud Firewall Service	Yes	Yes

PRODUCT SUITES

COMPONENTS

Professional Suite	URL/Content Filtering, File Type, AV & Antispyware, Reputation Threats, Std Cloud FW, and Std Cloud Sandbox
Business Suite	Professional plus SSL, Nanolog Service, BW Controls, ATP, CASB, Mobile App, and Web Access Control
Transformation Suite	Business plus, Adv Cloud FW, Adv Cloud Sandbox, Cloud IPS
Enterprise License	Transformation plus, Data Loss Protection (DLP), Premium Support, 10K+ seats

SYMANTEC DIFFERENTIATORS – Elevator Counter Pitch to CrowdStrike

Symantec Offers Superior Security

- Secure Access Cloud – improves Zero Trust by providing more granular visibility & control, security, and ease of deployment
- Unified perimeter and Network policy - Symantec Endpoint Protection (SEP & SEP Mobile) integration with WSS
 - Endpoint agent flexibility - utilize WSS Agent, Cloud Connector Defense, and SEP WTR (WSS Traffic Redirection)
- Web & email Isolation – Prevent threats while allowing broad web access by isolating uncategorized and potentially risky traffic
- Up to 4 categories per URL – offers More granular policy
- Largest Civilian Global Intelligence Network – provides visibility into multiple attack vectors from email to endpoint; from DLP to Consumers
- Visibility and Inspection of Office 365 traffic. Zscaler highly recommends bypassing all O365 traffic
- Recognized by Analyst for Market Leading Secure Gateway, CASB, DLP, Endpoint, MSS, email, ZTNA/SDP, and Data Security Portfolio

Open Architecture that integrates with your existing security solutions to increase ROI

- ICDx unifies products, services, and reduce cost & complexity, while protecting enterprises against sophisticated threats
- Integration with third party security solutions
- Automation through Open API with 100s of partners

Superior visibility and control

- Superior SSL Inspection without reordering/downgrading
- Self-managed certificates hosted in a customer’s AWS Cloud HSM
- Extensive Cloud Access Security Broker (CASB) visibility and controls; delivered from a single vendor
- Mirror Gateway for unmanaged endpoints for any sanctioned applications utilizing isolation technology
- Secure Access Cloud – improves Zero Trust by providing visibility & control
- (* Zscaler recently acquired Appsluate, so awaiting integration announcement in the next few months. However, they do not have an email solution; so cannot offer email isolation.)

Zscaler Battle Card

COMBATTING ZSCALER CLAIMS

Claim: Zscaler has 100+ data centers worldwide

While Zscaler likes to tout their 100+ data centers, it is essential to understand what classifies as a data center. Some of their “data centers” do not proxy traffic. Some are by invitation only. Some are running in a customer’s own data center, which is only accessible by that customer. Some have capabilities that others do not have, like IPSec support. Symantec has 52 data centers, fully meshed, ISO 27001 and SSAE 16 certified. All our data centers support IPSec and are available to all our customers.

Claim: Cloud-only is better

While a cloud security service offers a flexible pricing model and savings compared to on-premise gear, many enterprises can benefit the most by deploying a hybrid appliance/cloud model in which they can strategically secure select offices and HQs with appliances and remote offices and users with cloud security service. This approach enables continued ROI from appliances with the flexibility of cloud security service. Moreover, with Symantec, a mixed estate can be managed in one application (Universal Policy Enforcement). **Note that Zscaler is also offering an on-premises vZEN product.

Claim: Zscaler’s bigger network sees more threats

Zscaler claims its platform sees over 40 billion transactions per day. However, it is only protecting 10 million users. Symantec’s Global Intelligence network scans traffic from over 175 million users and is the world’s largest civilian threat intelligence network.

Claim: Symantec requires backhauling

Zscaler continues to spread false information including the claim that Symantec customers must backhaul their traffic. Customers have a wide range of options to secure offices, laptop users, tablet users, and smartphone users via an appliance or cloud security services; all done without the need to backhaul traffic.

Claim: Zscaler supports stronger elliptical curve ciphers

Zscaler is slowly rolling out support for ECDHE_RSA throughout their data centers. However, Zscaler service is still leaving users vulnerable by using ECDHE_RSA_AES_128_CBC_SHA1, but SHA1 hashing algorithm has been deprecated by internet providers such as Microsoft and Google. (<https://blog.qualys.com/ssllabs/2014/09/09/sha1-deprecation-what-you-need-to-know>)

Claim: Exact Data Match (EDM) for massive data sets covering users globally

Zscaler provides EDM functionality in their DLP product to maximize data protection. However, the feature set is limited, e.g., only 17 numbers of indexing data types, data matching combinations, limited response options (allow, block, or notify), exception handling, and non-Latin language. In contrast, Symantec Enterprise, market leading, DLP supports over 100 data types, 25+ languages (e.g., non-Latin-Arabic, Chinese, Japanese, Korean), 40+ response options, and several levels of exception handling.

ADDRESSING ZSCALER ADVANTAGES

Zscaler has specific support for Office 365

The biggest benefit Zscaler offers for Office 365 is being able to set a minimum or guaranteed bandwidth level. Their other benefits are exaggerated. Symantec does not currently offer bandwidth management in the cloud but does offer it with ProxySG. Our CloudSOC (CASB) solution and Email Security.cloud services offers deep security and compliance features for Office 365.

Zscaler’s cloud products are easier to deploy and manage

Zscaler promotes easy to deploy but not secure methods to redirect connections to their cloud. Symantec promotes secure methods that support most of the Zscaler deployment methods. Zscaler simplified their policy management at the cost of flexibility and coverage. While being intuitive, the Symantec UI also offers flexibility and granular controls not available from Zscaler including custom scripts for on-premises appliances.

Zscaler is less expensive

Zscaler’s cheaper packages lack critical features like application control, bandwidth management, and VPN support. Enterprises must upgrade to much more expensive offerings, like the Enterprise Web Suite, to gain similar features and capabilities already built into the Symantec cloud security solution.

SETTING ZSCALER TRAPS

- Are you concerned about being able to detect and block advanced threats while keeping your false-positive rate manageable?
- Do you have on-premises proxies and if so, do you need to maintain two sets of policy?
- What would be the risk to your organization of sending traffic from mobile devices to the cloud over insecure connections? What if some mobile traffic is uninspected?
- How do you protect your endpoints? Do you need advanced endpoint protection? What about endpoint & mobile protection (not just redirection)?
- How complex is it to setup your CASB infrastructure?
- How do you detect and remedy malicious URLs in your email?
- What happens to your organization if your DLP policies are not consistently enforced?
- How much value do you place on first-class URL filtering and malware detection?
- Are you concerned about your service using a weak cipher suite when surfing the internet? Exposing your users to potential attacks?
- How about self-managing your certificates and keeping your keys private?

Palo Alto Networks Battle Card



PALO ALTO NETWORKS APPROACH

Secure the Enterprise and Secure the Cloud

- NGFW – Secure the Enterprise – utilizing the same NGFW and threat prevention technologies
- Prisma – Secure the Cloud - new marketing campaign solution, but underlying technologies have not changed
 - Prisma Access – Secure branch offices and mobile users (formerly GlobalProtect Cloud Services)
 - Prisma Public Cloud - continuous visibility, security, and compliance monitoring across public multi-cloud deployments (formerly RedLock)
 - Prisma SaaS - multi-mode cloud access security broker (CASB) service (formerly Aperture + GlobalProtect Cloud Services)
 - VM-Series – Virtual NGFWs for private and public cloud

SYMANTEC APPROACH

Market leading Secure Web Gateway, Endpoint, Isolation, ATP, CASB, and Zero Trust

- Symantec SWG has been recognized as the market leader for over 11 years.
- Comprehensive Integrated Cyber Defense (ICD) bring together our market-leading security products, e.g., ATP, CASB, DLP, Sandboxing, Symantec Endpoint Protection (SEP + SEP Mobile), Isolation, Email, and Secure Access Cloud.
- World's largest civilian threat intelligence network, utilizing data from 3800 engineers and researchers. Plus, threat intelligence detected and discovered by our comprehensive security stack continues to provide superior protection.

KEY CAPABILITIES	PAN	SYMANTEC
Web app controls (CASB)	Yes (3145)	Yes (31,000)
SSL inspection	Yes (Cipher downgrade)	Yes, stable performance and enterprise grade features
Isolation	Menlo Partnership	Comprehensive
Antimalware	Home grown 'stream-like' inspection	Kaspersky, McAfee, Sophos, Symantec
URL categories per site	PAN-DB (Up to four in 9.0) BrightCloud (Two)	Up to Four
Authentication options	Limited, more like identification	Comprehensive
Streaming media optimization	No	Yes
Sandbox	Limited features in cloud	On-premises (fast), real-time, predictive, gold-image can be uploaded, risk score, ghost user
Security analytics	Limited	Comprehensive

MODEL	FUNCTION	FW THR./PRICE
PA-3200	Next-generation firewall	2Gbps / ~62\$K
PA-5250	Next-generation firewall	10Gbps / ~\$172K
PA-7050	Next-generation firewall	60Gbps / \$1.3M
PA-7080	Next-generation firewall	100Gbps / \$1.9M
M-500	Centralized management	1,000 devices / \$75K
Prices include fully populated chassis, threat prevention, URL filtering, WildFire, & Standard support		

SYMANTEC DIFFERENTIATORS

Symantec Offers Superior Protection

- Secure Access Cloud – improves Zero Trust by providing more granular visibility & control, security, and ease of deployment
- Web and Email Isolation – Prevent threats while allowing broad web access by isolating uncategorized and potentially risky traffic
- Largest Global Intelligence Network – provides visibility into multiple attack vectors from email to endpoint; from DLP to Consumers
- Visibility and Inspection of Office 365 traffic – no bypass required
- Recognized by Analyst for Market Leading Secure Web Gateway, CASB, DLP, Endpoint, MSS, Email, Zero Trust, and Data Security Portfolio
- In-depth malware analysis – virtualization & emulation, utilize golden OS image, ghost user, withhold file until good/bad sandbox verdict

Superior visibility and control

- Secure Access Cloud – extensive visibility & control through Zero Trust
- CloudSOC Mirror Gateway for unmanaged endpoints for any sanctioned applications
- Isolation with WSS, ProxySG, CloudSOC, and Secure Access Cloud
- Self-managed certificates hosted in a customer's AWS Cloud HSM – Minimize certificate exposure
- Cloud Firewall Service to allow/block non-HTTP/HTTPS traffic

Unmatched Resources

- 3800 Engineers and Researchers
- 9 Global Threat Response Centers

Palo Alto Battle Card

COMBATting PALO ALTO NETWORKS CLAIMS

Claim: Prisma SaaS (formerly Aperture) provides Web App security solution

While this looks like a CASB offering, it falls short of competing with Symantec's CASB solution. Prisma SaaS is a sanctioned cloud application control component, which only supports 736 applications. It is also an API based only solution, which means it can only detect malware after the fact. Prisma SaaS does not enforce any policy through Palo Alto's Next-Gen Firewall. Symantec's CASB solution can identify over 31,000 applications and enforce comprehensive policies.

Claim: PAN's Wildfire™ is a competitive sandboxing product

Wildfire is missing many key features found in Symantec's Malware Analysis Appliance. It can't replicate corporate gold images, detect VM-evasive malware by simulating user actions, accept manually submitted files for analysis, provide risk scores or even provide a detailed analysis of files. These features are critical for catching advanced malware. Furthermore, Wildfire lacks features like real-time sandboxing or predictive sandboxing, which are essential in large organizations.

Claim: PAN appliances provide extremely high performance

PAN appliances do provide very high performance – if you restrict them to firewall and IPS functionality. There is performance degradation when you turn on Threat Prevention, anti-spyware or SSL (See NSS Lab 2018 NGFW Test Report). Customers will get much better performance and security by using PAN (or another vendor) for their NGFW, and Symantec for effective web security, visibility, and SSL decryption.

Claim: PAN provides more details and context for analyzing threats

PAN claims to provide complete visibility into threat activity through its "App-ID™," "Content-ID™" and "User-ID™" technologies. These give some insight into attacks and help apply policies. However, they have nowhere near the power of Symantec's Security Analytics Platform to capture and index all traffic, reconstruct entire attacks, including emails, attachments and IM conversations and provide detailed forensics and root cause analysis.

ADDRESSING PALO ALTO NETWORKS ADVANTAGES

PAN inspects all 65K+ ports, not just web traffic

The web channel continues to pose the most risk of advanced threats and targeted attacks. Symantec provides outstanding protection against even the most sophisticated web-based threats via Cloud Firewall Service, Web Filter, Content Analysis System, and the Malware Analysis Appliance. All of which connect to the Global Intelligence Network (GIN).

AutoFocus prioritizes attacks

Prioritizing attacks does not mitigate them. Palo Alto requires human analysts to review and respond to alerts, and even then it does not provide the full packet capture or root cause analysis of Security Analytics. A better solution is Symantec's SA coupled with our GIN. Not only can SA alert on attacks, but it can also replay them and track the cause.

Many applications on one appliance (NGFW, IPS, VPN, AV, URL filtering)

SMB customers may perceive NGFW and UTM products to be less costly and easier to manage than multiple appliances. However, the security is not nearly as good, and the performance degrades quickly when all services are turned on, requiring the customer to buy more appliances. Symantec's cloud solutions can simplify deployment and management for SMB customers.

SETTING ZSCALER TRAPS

- How would you rate your effectiveness today at preventing advanced threats?
- What is your approach to incorporating the best security solutions versus obtaining all security products from one vendor?
- What concerns do you have about the impact of SSL inspection on your firewall?
- What do you see as the most important capabilities for URL filtering and malware detection?
- Would you prefer a customizable sandboxing environment or a generic one?
- What forensic tools do you have to address a post-breach analysis?
- How do you enforce your policies over Web Apps (Shadow IT)?

SETTING ZSCALER TRAPS

- PA-xxxx NGFW appliances
- Panorama software and appliance management
- Wildfire cloud service and appliance (sandboxing)
- URL filtering subscription
- Threat Prevention subscription
- AutoFocus (Threat Intelligence)
- Prisma SaaS
- DNS Security

Cisco Battle Card



CISCO UMBRELLA APPROACH

Provide 100% Security all the time anywhere

- Cisco positions their Secure Internet Gateway (SIG) - Umbrella Platform - as the easiest and fastest way to protect users 100% of the time, by extending coverage beyond the corporate network without the need for a VPN. DNS as the foundational component of Umbrella
- Cisco boasts 100% uptime since they established their network in 2006; a global network that processes 175 billion daily internet requests from some 90 million users across 30 datacenters worldwide.

SYMANTEC APPROACH

Recognized market leading Secure Web Gateway (SWG) with capabilities spanning access control, advanced threat prevention, information security, web isolation, endpoint protection, and CASB; available as a cloud service, virtual, or physical appliance

- Symantec SWG has been recognized as a market leader for more than 12 years.
- Comprehensive defense-in-depth and integration with our other market-leading security products, e.g. ATP, CASB, DLP, Sandboxing, Symantec Endpoint Protection (SEP + SEP Mobile), and Web Isolation.
- World's largest civilian threat intelligence network utilizing data from 3800 engineers and researchers. Plus, intelligence detected and discovered by our comprehensive security stack.

KEY CAPABILITIES	CISCO UMBRELLA	SYMANTEC
Full Traffic Inspection	No (intelligent proxy - only URL's and Domains)	Yes
Web Isolation	No	Yes
Endpoint Integration	Yes	Yes
Data Loss Prevention (DLP)	No	Yes
Granular web usage controls	No	Yes
Shadow IT application visibility and control	Limited (App Discovery)	Yes (24K)
Log Storage Geography	Yes (Calif. and EU-Germany, or Amazon S3)	Yes
File Inspection	Yes	Yes
Data Centers	30 DCs, ISO 27001, SOC2	40 Fully Meshed, ISO 27001, SSAE 16, SOC2

PRODUCT SUITES

COMPONENTS

UMBRELLA	Cloud Security Platform providing SIG → based on OpenDNS
UMBRELLA INVESTIGATE	Live graph of global DNS requests and data - leverages predictive intelligence → based on OpenDNS Investigate
UMBRELLA FOR MSPS	Umbrella with centralized console settings and reports for Managed Service Providers → based on OpenDNS for MSPs
INTEGRATIONS	Cisco AMP Threat Grid, AMP for Endpoint, Cloudlock, ThreatConnect, ThreatQuotient, FireEye, and Check Point

SYMANTEC DIFFERENTIATORS – Elevator Counter Pitch to CrowdStrike

Integrated and superior *CASB offering with deployment options – in-line or API

With automated log ingestion from WSS to Symantec CloudSOC and Unified authentication between WSS and Symantec CloudSOC, deployment options are streamlined and more integrated than other vendors currently. In contrast, Umbrella recently added App Discovery for visibility into Shadow IT. Additionally, full CASB functionality requires the use of CloudLock, but that is API based only.

A Secure Internet Gateway that decrypts and inspects all web traffic all the time

Just like the on-premises SWG product, WSS inspects all web traffic all the time as well as supporting numerous protocols and advanced features. Cisco Umbrella will only selectively decrypt and inspect traffic based on reputation or policy, leaving all traffic to “reputable” sites uninspected, even though “reputable” sites (especially cloud apps like Dropbox and Google Drive) are seeing increased use in phishing attacks.

WSS presents a Secure Internet Gateway integrated with the industry's leading DLP solution

Symantec WSS provides cloud-based or on-premises DLP integration with the ability to leverage existing infrastructure and policy-simplifying adoption and deployment. Additionally, Symantec WSS can inspect SSL encrypted traffic, further ensuring compliance and security. Cisco Umbrella is allowing a direct connection – with no inspection – to “sanctioned” sites like Dropbox and Google Drive, preventing any in-line DLP, and moreover, no content sandboxing, granular application control, or packet shaping. In contrast, Cisco utilizes limited Cloudlock Cloud DLP Policy Engine or deploy Digital Guardian's DLP.

Web Isolation protects against web-borne malware and phishing

Web Isolation delivers business continuity while protecting users from web-borne malware and phishing from uncategorized and risky websites. The technology provides a secure environment, isolating the users and the web, and sending only safe rendered information to users' browsers.

Symantec offers best-in-class threat intelligence and a cloud network engineered for performance

Symantec leverages the largest Civilian Global Intelligence Network in the world, consisting of threat telemetry from over 15k enterprises, 175 Million users, and 3,800 engineers and researchers. Symantec's cloud service has 40 data centers worldwide with coverage across 6 continents, providing a rich service of high performance and low latency.

Symantec recognizes the requirement for strict control over where data resides

With Symantec WSS, you can specify which data centers to connect. You can specify the continent or specific country. Control where and how long reports and other information are maintained. Cisco Umbrella log storage is limited to California (US), Frankfurt (EU), and AWS S3 locations.

Cisco Battle Card

COMBATTING CISCO UMBRELLA FUD

Claim: Claim: Cisco Umbrella enjoys 100% uptime with global failover

Symantec has 40 data centers, fully meshed, ISO 27001 and SSAE 16 certified. All our data centers support IPSEC and are available to all our customers. Additionally, Symantec offers 99.999% SLA with global failover and presence on 6 continents. 175 million users trust and rely on the backbone that Symantec has built.

Claim: Umbrella SIG can identify and control SaaS apps

Cisco states that the Umbrella Secure Internet Gateway can identify which SaaS apps are being accessed and enforce policies to block risky or inappropriate apps. Cisco also adds this disclaimer "...by integrating with a Cloud Access Security Broker (CASB) you can gain even more visibility and control for usage and data." Recently, Cisco incorporated an App Discovery feature to identify cloud/Shadow IT apps in use. App Discovery can only block users from going to cloud apps that are marked "Block this app". Symantec Integrated CloudSOC and WSS, however, provide the ability to dynamically control Shadow IT based on risk metrics or app name. Risk metrics are unique to Symantec; a dynamic control that is always updated, alleviating the hassle of updating individual app filters. Additionally, CloudSOC and WSS provide granular inline DLP controls for unsanctioned apps – Cisco is not doing this.

Claim: Gain granular application control with Cisco WSA

Cisco does offer the Web Security Appliance (WSA), but this is an on-premises appliance and not cloud-ready; the WSA is required to provide proper SWG inspection capabilities. Cisco WSA does not match the Symantec SWG – Gartner places Symantec in the Leaders quadrant again (10 years running) while Cisco remains a "Challenger" in the Magic Quadrant for Secure Web Gateways. They are not included in the latest Radicati Corporate Web Security - Market Quadrant 2018.

Claim: Cisco Umbrella provides coverage on and off network while SWG solutions are "on network" only

Symantec WSS provides security anywhere on any device. WSS supports laptops, smartphones, tablets, and entire offices to secure every use case covering all options. Symantec Endpoint Protection integration with WSS provides in-depth perimeter protection.

Claim: Cisco Umbrella provides secure access to the internet and SaaS apps

Cisco Umbrella allows you to directly connect to SaaS apps like Box and Google Drive without any inspection whatsoever because the reputation of these cloud apps are "good" and therefore Umbrella is allowing the connection directly. Increasingly, these cloud apps are targeted for phishing attacks and need a proxied connection - not just for content sandboxing, but for in-line DLP! The DNS "look-up" feature of Umbrella is pretty much useless, since all sites, even those that are thought to be good, need to be vetted in today's threat environment.

ADDRESSING CISCO UMBRELLA ADVANTAGES

Cisco Umbrella provides enforcement across all ports while SWG solutions do not

Symantec SWG focuses on the security of your content, which is why it inspects everything. By design, the SWG is not targeting all ports and protocols but is instead thoroughly examining HTTP/S traffic to monitor, control, and secure traffic ensuring a safe web and cloud experience. Currently, the decision to proxy a domain by Cisco Umbrella is not under your control, and when it does proxy a domain, it is only looking at URL's and domain names, and not providing the deep controls required for security and compliance.

Cisco Umbrella is easier to deploy and manage

Cisco Umbrella has a very simplified deployment that requires no hardware. Symantec WSS is a cloud-based SWG that requires some simple configuration to enforce cloud and web access control policies, protect users from malware and advanced threats, and integrates with SEP, Web Isolation, and DLP. Cisco Umbrella cannot provide this level of in-depth inspection and analysis.

Cisco Umbrella is less expensive

The DNS lookup capability provides little to no value, and all traffic should route through the entire security stack (which may increase the Cisco price-point).

SETTING ZSCALER TRAPS

- If you are considering a cloud-based SIG/SWG, how important is it that they offer the same enterprise-class capabilities you have in your on-premises gear?
- Do you want to inspect all your traffic? Are you ok NOT inspecting traffic to reputable sites and domains, like Dropbox, even though they are vectors for phishing attacks and future cloud attacks?
- How are you controlling unsanctioned cloud use and enforcing compliant and secure cloud app adoption?
- What about Web Isolation technology? How does Umbrella protect against uncategorized and risky sites?
- Can Umbrella prevent users from disclosing corporate credentials or sensitive info to potential phishing sites?
- How do you inspect encrypted traffic for malware and zero-day threats? Is cipher-suite coverage an important consideration for you given the US-Cert warning?
- How is your DLP solution inspecting encrypted traffic across all channels?
- How are you controlling end-users going to sanctioned cloud apps off the network circumventing your in-line DLP inspection?

Cisco Umbrella Components

- Umbrella Platform – enterprise level with all features and API for integration
- Umbrella Insights – for medium size business with everything from Platform with more options for reporting and DNS log retention
- Umbrella Professional – for small size business has all the basics
- Umbrella Wireless LAN – for protecting guest wireless users

Powerful Results

Fortune 20 Company

All Web Traffic

ProxySG/ASG
Secure Web Gateway

41.7B

Web Requests

48.1M malicious sites blocked

ASG/Content Analysis
Threat Inspection

2.4B

Files Scanned

7.7K Files blocked

Content Analysis
Sandboxing

539K

Files Sandboxed

389

Risky Files Identified

Prior to Proxy/Content Analysis, 4,000 events sent to SOC for investigation

**30 Days of actual traffic at Fortune 20 Customer*

Gartner's 2019 SWG Magic Quadrant

A leader – 12 years in a row

Figure 1. Magic Quadrant for Secure Web Gateways



Source: Gartner (November 2019)



[Gartner Magic Quadrant for Secure Web Gateways](#), 11 November 2019, Lawrence Orans, Peter Firstbrook, John Watts

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Symantec. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

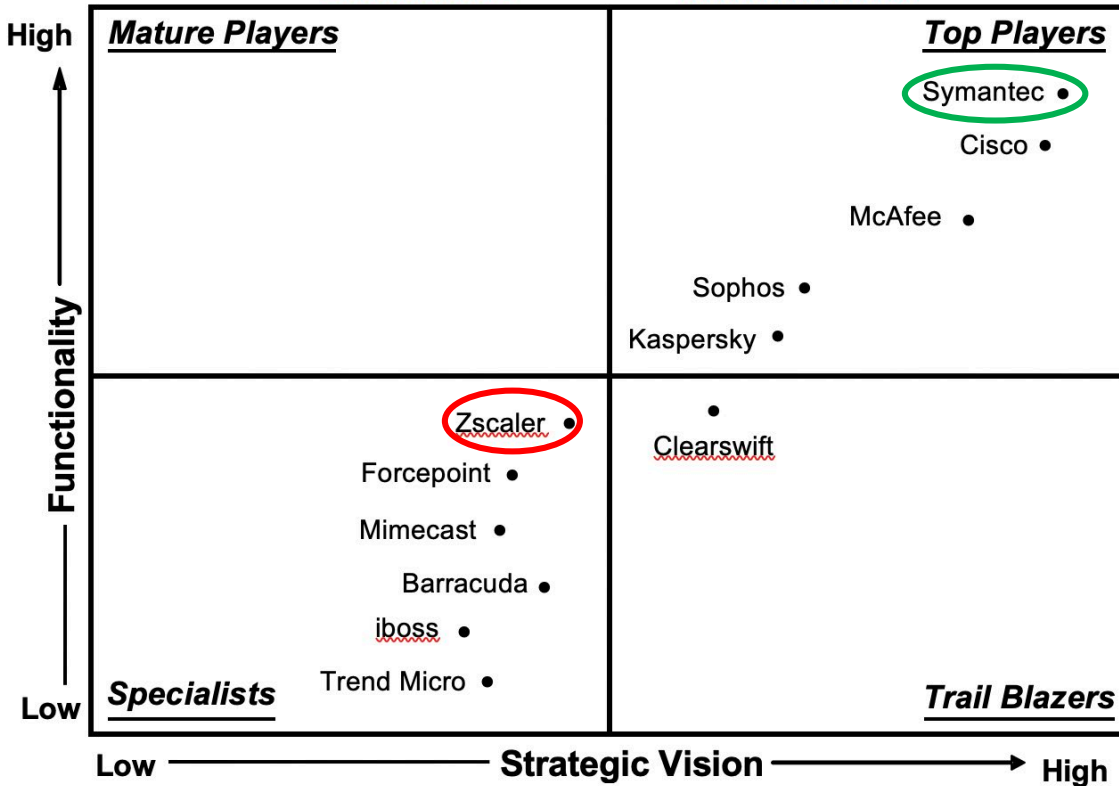
Radicati Market Quadrant 2020

Corporate Web Security – Top Player 13 Years in a Row

MARKET QUADRANT – CORPORATE WEB SECURITY



Radicati Market QuadrantSM



“Symantec, now part of Broadcom, also has a leg up given the combined company’s annual \$4.7 billion commitment to research and development, paving the way for significant investment in product enhancements.”

“Symantec’s Web Security solutions are available as cloud services, appliances, and virtual appliances. All Symantec web security solutions are backed by the Symantec Global Intelligence Network, that offers real-time protection from malware and real-time URL filtering. The solutions also offer real-time, reputation-based malware filtering which helps detect new, targeted attacks.”

Figure 3: Corporate Web Security Market Quadrant, 2020*

Leadership Compass: Network Detection and Response

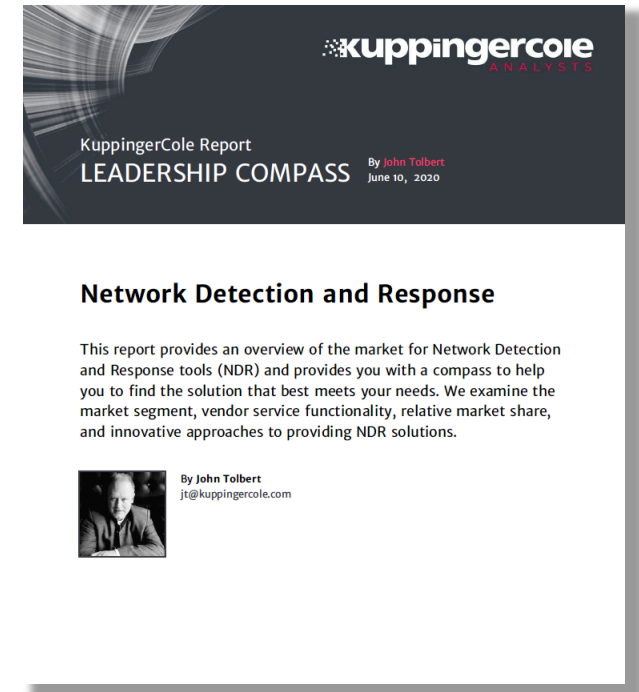
KuppingerCole names Symantec a Leader in all four categories



Security	●●●●○
Functionality	●●●●●
Integration	●●●●○
Interoperability	●●●●○
Usability	●●●●●



- Strengths**
- Extreme scalability, processing billions of lookups per day
 - Packet decryption and sandboxing available
 - Deception/tripwire capabilities
 - Customizable ML models
 - Tight integration with Symantec security products



Source: Kuppinger Cole. Leadership Compass Report for Network Detection and Response, John Tolbert, June 2020

What is Symantec Secure Web Gateway?



Symantec Secure Web Gateway (Product Family Term)

Secure Web Gateway

The Secure Web Gateway secures the enterprise and their users from multiple connection points to the Internet and any cloud-hosted applications or data. Built with deployment scalability and flexibility, the Secure Web Gateway offers a variety of Symantec security technologies for Enterprises to deploy either on-premises, in the cloud or a hybrid deployment.

Security Technologies



Proxy



Web Isolation



Threat Protection



CASB



Other...

Deployment Options



Appliance



Dedicated Cloud



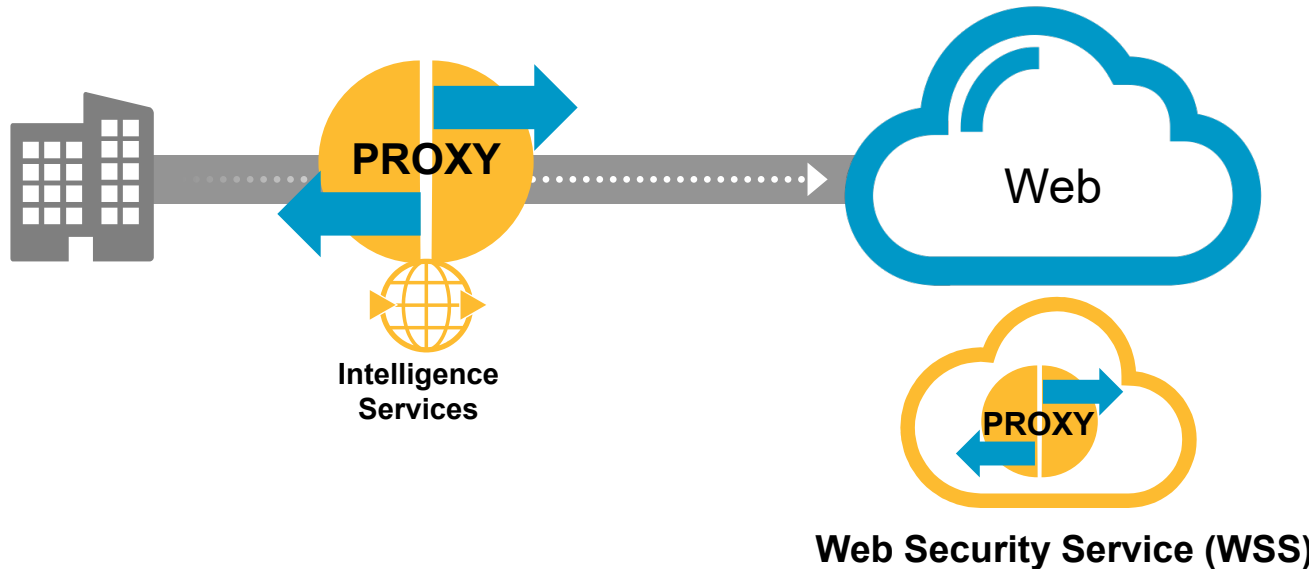
Virtual / IaaS



SaaS

Proxy-based Secure Web Gateway

Critical Network Control Point for Security and Compliance



- Appliance (ProxySG, ASG)
- Virtual Appliance (VSWG, SG-VA)
- Web Security Service (WSS)
- + Symantec Intelligence Services (IS)
or Symantec Web Filter (WF) subscriptions

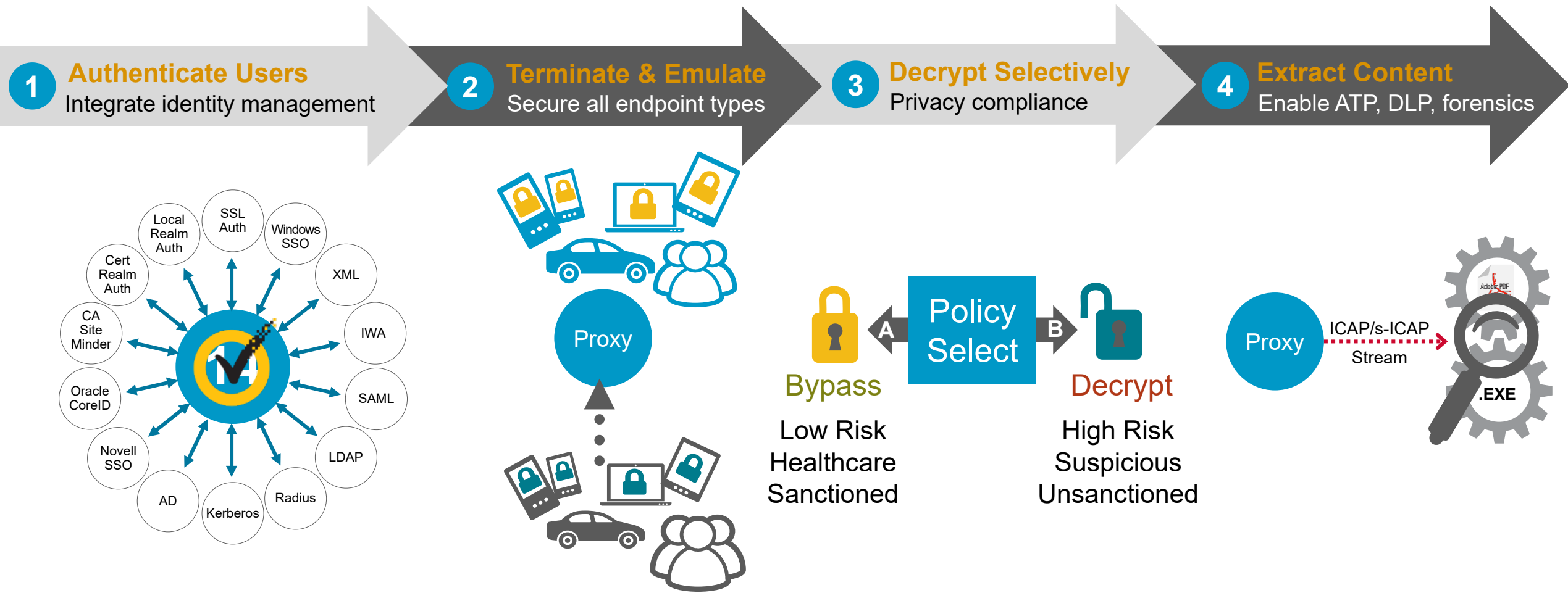
**Web Access Governance
& Threat Protection**

**File Extraction & Orchestration
Services (ATP, DLP)**

**Powerful, Open Policy Platform
- In Cloud, On Prem, Virtual, AWS**

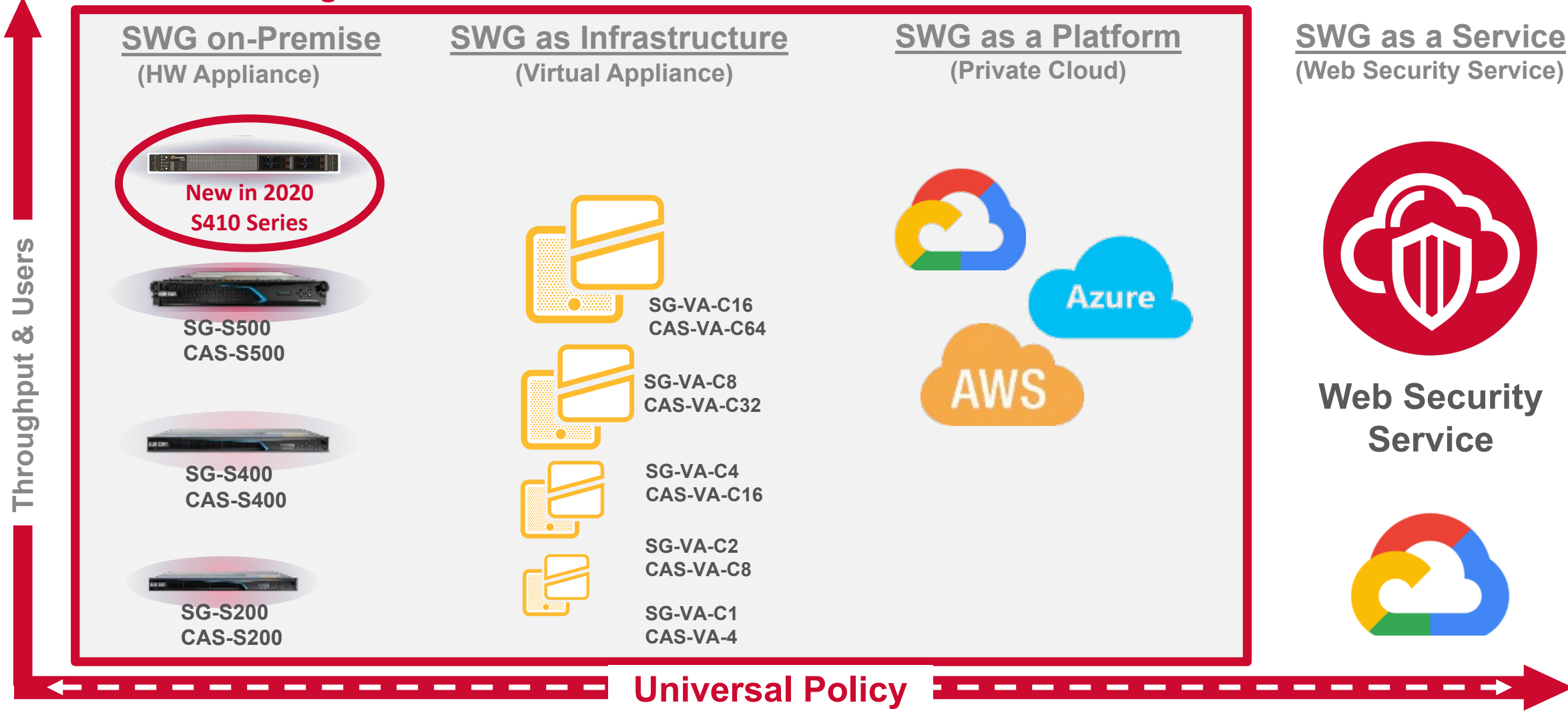
Proxy All Endpoints

Architecture for Content Extraction and Device Emulation



SWG Solution Spectrum – On-premises, Cloud and In-between

Single instance/dedicated tenant solutions



Simplification – Appliance Evolution (Update – Proxy only first)


Product specific HW appliances

Product specific virtual appliances with fixed configurations

Common HW platform

HW platforms + Enterprise license

Current Generation Appliances



SG-S500 RP-S500

SG-S400 RP-S400

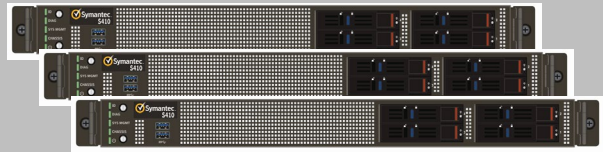
SG-S200 RP-S200

ProxySG (SG), Reverse Proxy (RP)

SG-VAs
RP-VAs



Next Generation Appliance



SSP-S410

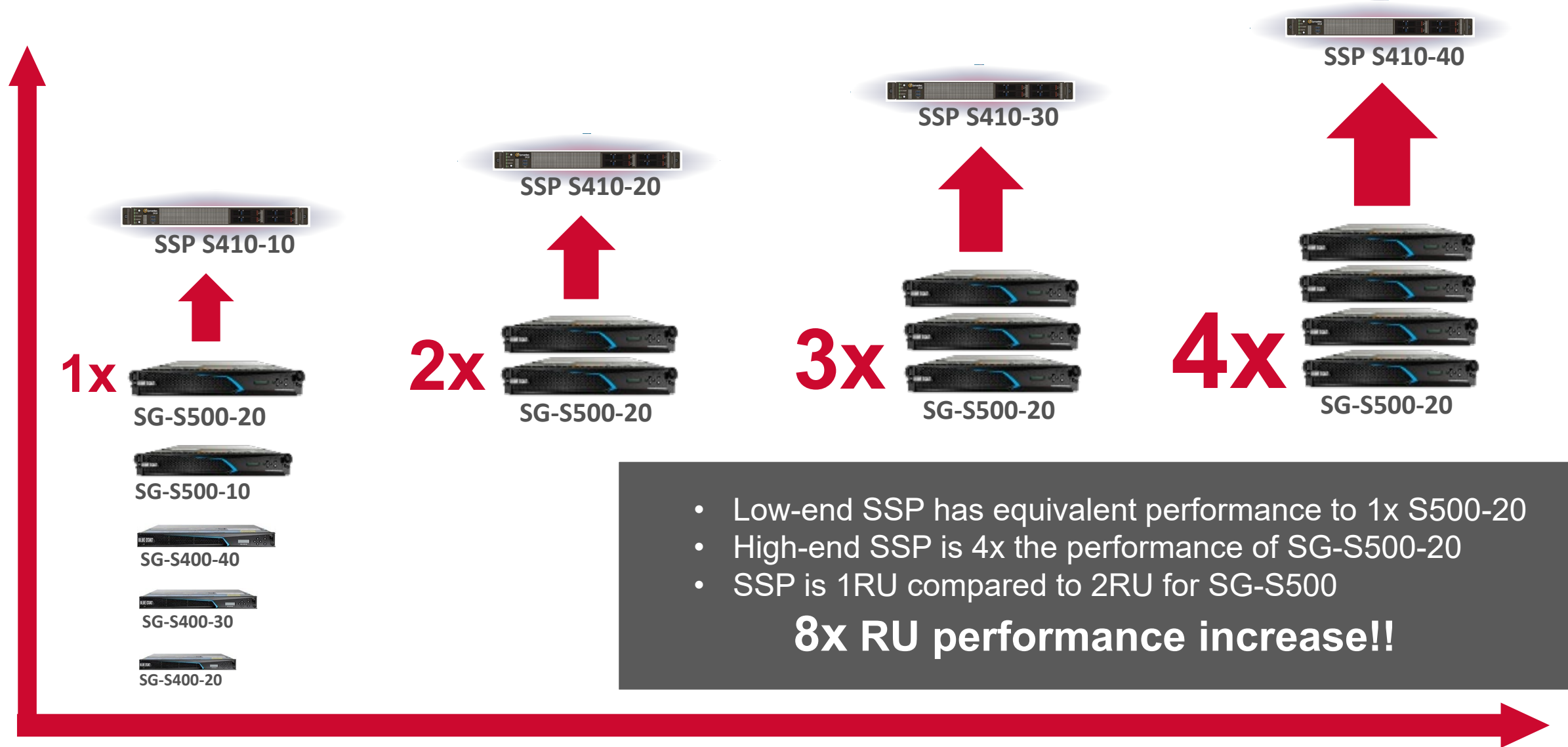
+

ISG
Enterprise
License

Proxy, RP/WAF

Decouple SW from HW

Performance – SSP HW Performance Compared to S-series



Secure Web Gateway – Added Value Enabled by New Platform

Secure Web Gateway (current)

New Web Security Requirements

- Adoption and transition to Cloud applications
- Increasing reliance on Web (O365)



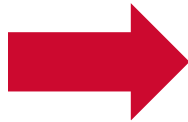
Shifting datacenter strategy

- Reduce Datacenter costs
- Capacity forecasting challenges
- Transition between on-prem and Cloud



Procurement

- Simplify procurement
- Minimize Capex investment



Secure Web Gateway (S410 + ISG)

Increases demand on SWG capacity

- More conns, all encrypted (O365, G-suite)
- New Internet protocol support (TLS1.3, HTTP2, DoH)
- Integrated CASB visibility

Benefit: Higher performance baseline and include CASB shadow IT discovery with New Platform

Deployment Flexibility

- New HW with rack dense performance
- Just in time expansion of capacity (expand VA)
- Flexibility to use licenses in Cloud

Benefit: Flexible licensing and portability with New Platform

Capex vs Opex

- Enterprise Licensing (capacity)
- Adopt newest/highest performing HW

Benefit: Decouple Capex/Opex spend with New Platform

Securing the Digital Transformation

The Challenges of Delivering on the Promise



The user experience suffers from complexity and poor performance

IT suffers from reduced security visibility & control, and increased complexity

Organizations suffer from increased technology costs and impacted productivity

What is SASE?

Network-as-a-Service



- Remote Access
- URL Filtering
- DNS, VPN, QoS

Cloud Security



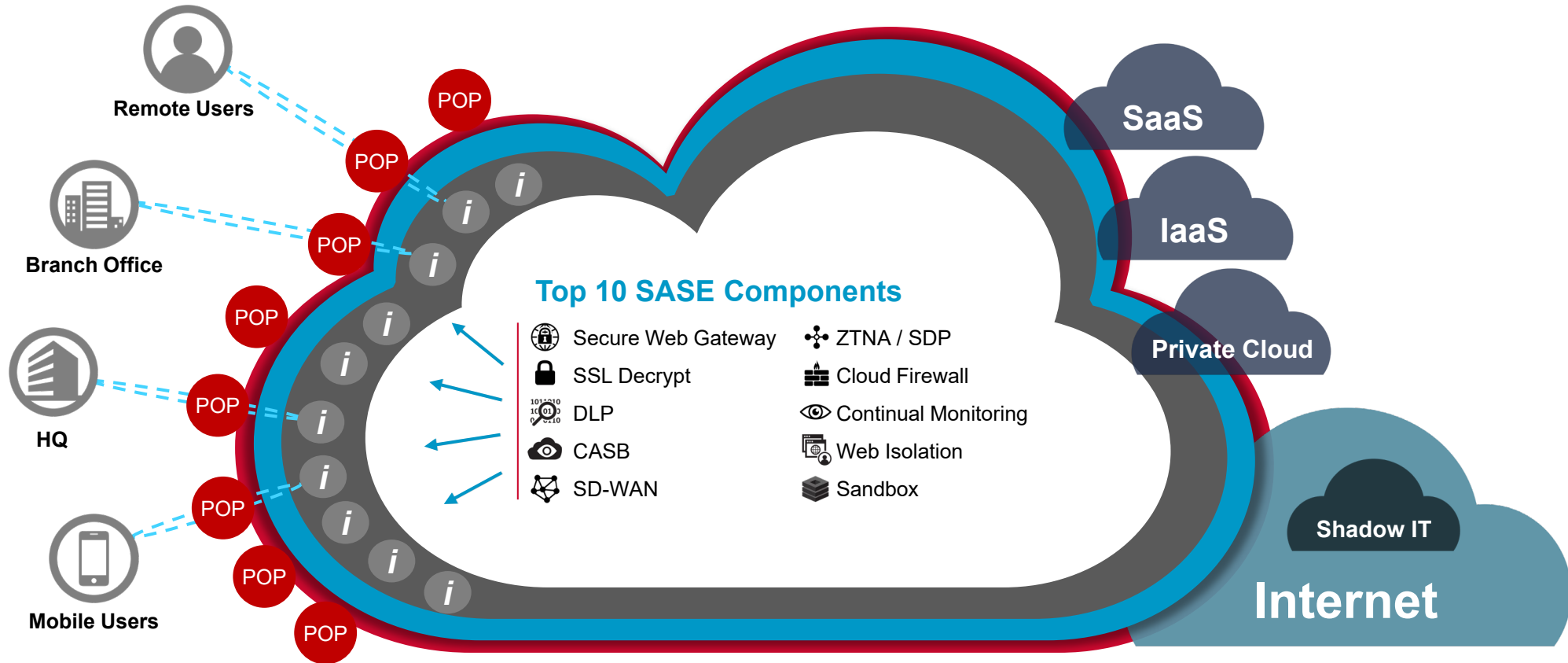
- Context Aware
- Threat Prevention
- Identity

Gartner®

Connecting Endpoints	<i>“Digital transformation and adoption of mobile, cloud, and edge deployment models fundamentally change network traffic patterns, rendering existing network and security models obsolete”</i>	Securing Endpoints
SD-WAN		Secure Web Gateway
QoS		SSL Decryption
CDN		Data Loss Prevention
WAN Optimization		CASB
Network-as-a-Service		ZTNA / SDP
Bandwidth Aggregators		FWaaS
Policy Based Forwarding		Web Isolation

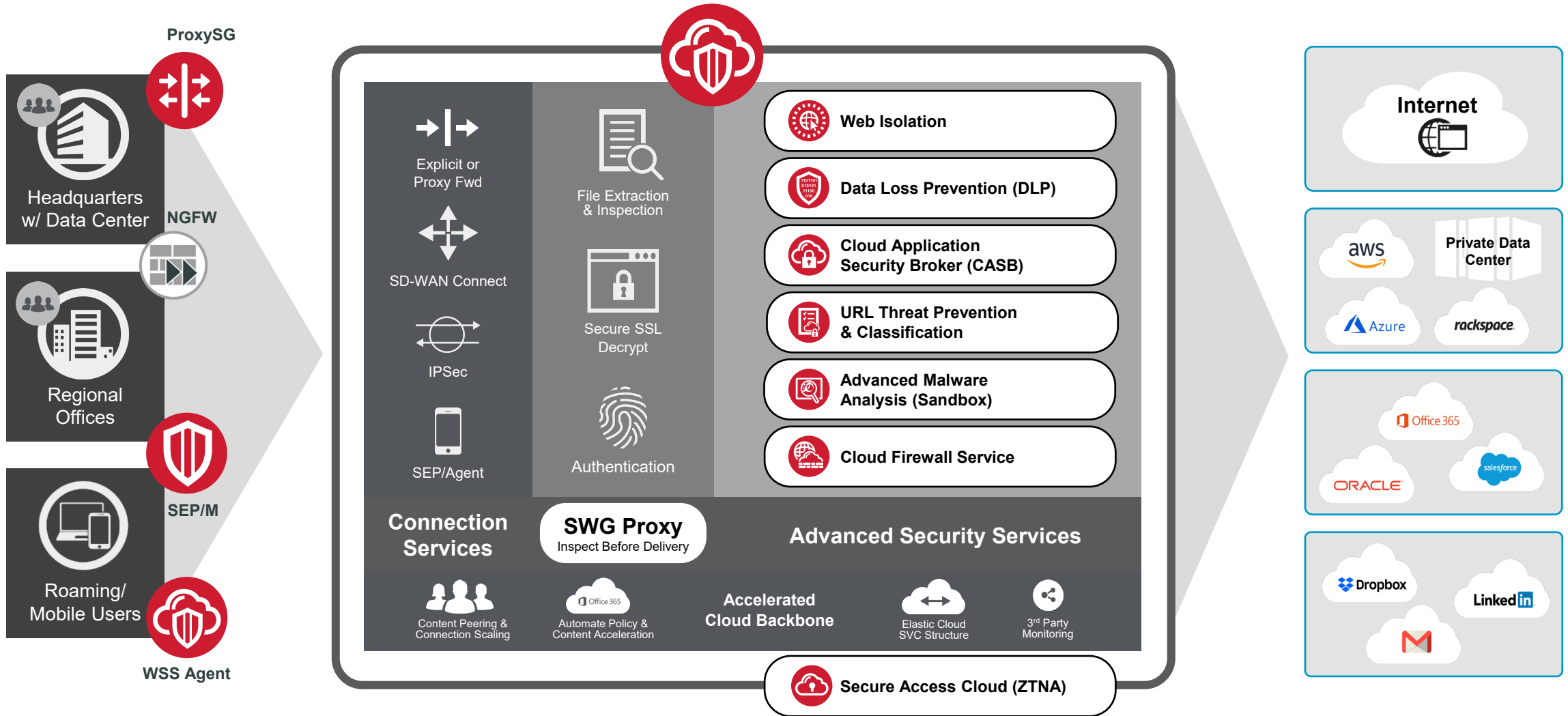
SASE Framework

Pushing simple, fast, flexible, and scalable security to the service edge



Symantec Web Security Service

Providing a foundation for our SASE solution



Customer Win – Large Multinational Insurance Company

- **Customer Challenges**

- Needed secure web activity for all employees
- Wanted multi-layer content inspection and sandboxing to identify advanced threats and data loss
- Protection from malware and phishing attacks

- **Why We Won**

- Strong Partner advocated Symantec
- Symantec offered solution for every desired deployment option
- Hybrid deployment model helped mitigate decision risks

- **Competitors**

- None (Stringent requirements in RFP excluded competition and locked in Symantec)

Symantec Solutions

ProxySG

Content Analysis

Web Isolation

Global Customer Care Solutions Company

- **Customer Challenges**

- Global company running 23 data centers must protect customers' sensitive information
- Competitor's threat gateway solution was going EOL

- **Why We Won**

- Customer favored on-premises solution for compliance
- Required anywhere, anytime support
- Symantec beat all competitors in "real world" POC

- **Competitors**

- Cisco, Zscaler

Symantec Solutions

ProxySG

Endpoint Protection

DLP



Thank You





BROADCOM®

connecting everything®



Thank you for downloading this Symantec guide! Carahsoft is the reseller for Symantec Fed and Sled solutions available via Navy BPA, DIR-TSO, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Symantec’s solutions, please check out the following resources and information:



For additional resources:
carah.io/Symantec-resources



For upcoming events:
carah.io/Symantec-webinars



For additional BlackBerry solutions:
carah.io/Symantec-remote-solutions



For additional FED and SLED solutions:
carah.io/Symantec-solutions



To set up a meeting:
symantecteam@Carahsoft.com
703-871-8539



To purchase, check out the contract vehicles available for procurement:
carah.io/Symantec-contracts