



Secure Web Gateway: The Power of Proxy

Tim Balog, CISSP

Solution Engineer Manager
Federal Sales

June 13, 2018



Agenda



- 1 Symantec Today
- 2 Role of the Proxy
- 3 Symantec Secure Web Gateway (SWG)
- 4 SWG Platform
- 5 Web Security Service
- 6 SWG Integrations
- 7 Summary



Symantec Today

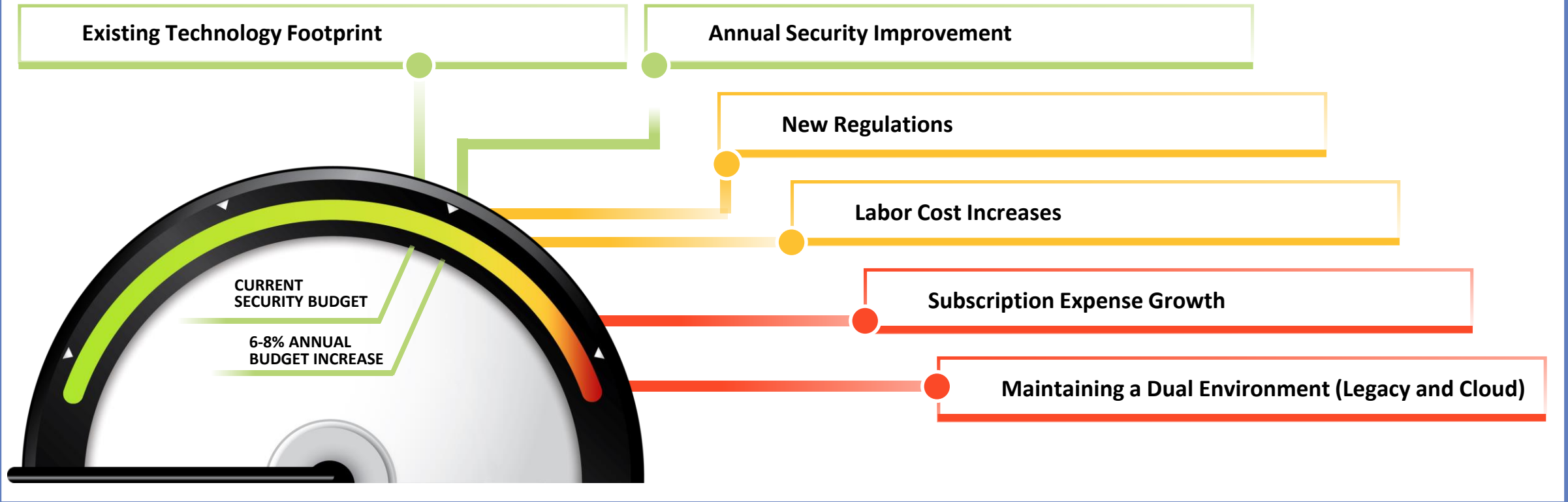


Fiscal Crisis


The Industry Faces a Looming Fiscal Spending Crisis



\$🔒 SECURITY OPERATING COSTS




Symantec | At a Glance



175M
endpoints under protection



\$5B+
FY18E revenue



2100+
patents



Leader in 5 Gartner MQs
CASB, SWG, EPP, DLP and MSS



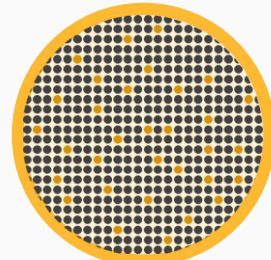
350,000+
customers worldwide



~3,500+
company wide R&D

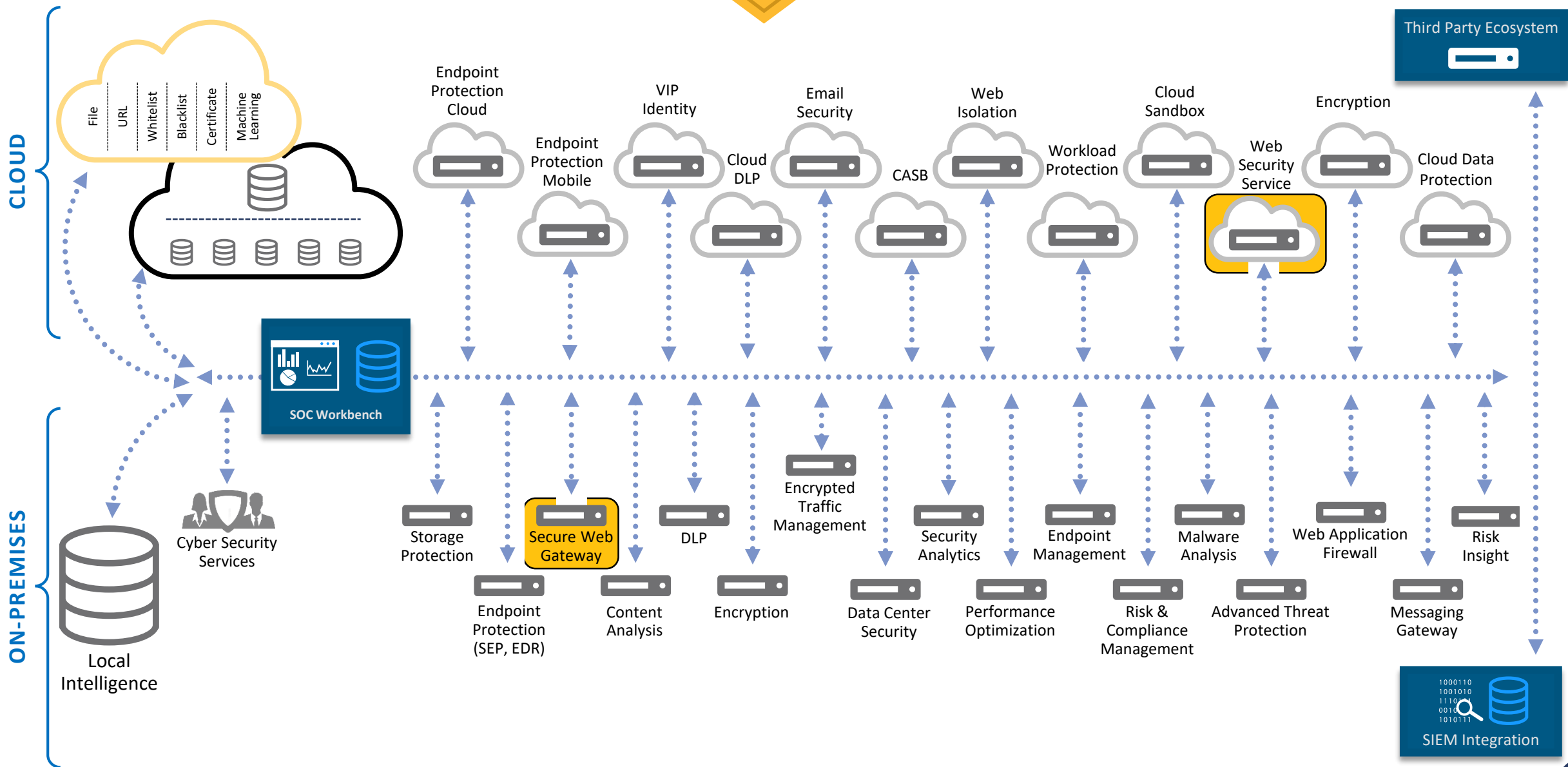


9 SOC
threat response centers



9 Trillion
telemetry points

Hybrid Cyber Defense Solutions



Broad Portfolio of Cyber Security Solutions



Protection & Security



ZIMPERIUM
McAfee
KASPERSKY
SOPHOS
CROWDSTRIKE
TREND MICRO
CYLANCE
Symantec

Endpoint

FireEye
NIXSUN
RSA
Symantec

Forensics & Recording

bitglass
CipherCloud
Trust in the Cloud™
Vaultive
Symantec

Encryption & Tokenization

DIGITAL GUARDIAN
FORCEPOINT
McAfee
Symantec

Real-Time Bi-Directional DLP

netskope
skyhigh
Microsoft
Symantec

Reporting & Audit

tripwire
Bit9+ CARBON BLACK
ARM YOUR ENDPOINTS.
McAfee
Symantec

Device / IoT

Compliance & Governance



Web Protection

Symantec
CISCO
McAfee
FORCEPOINT
zscaler
Menlo Security

Advanced Malware

Symantec
CORE SECURITY
FireEye
lastline

Analytics & Intelligence

Symantec
CISCO
netskope
ORACLE
exabeam
splunk>

Integrated Cloud Data Analysis

Symantec
CISCO
netskope
skyhigh

Access & Authorization

Symantec
skyhigh
bitglass

Visibility & Discovery

Symantec
Microsoft
netskope
paloalto NETWORKS
skyhigh

Messaging

Symantec
proofpoint
mimecast
Barracuda
FireEye
TREND MICRO

Managed Security



Content-Aware DLP



Secure Web Gateway



Endpoint Platforms



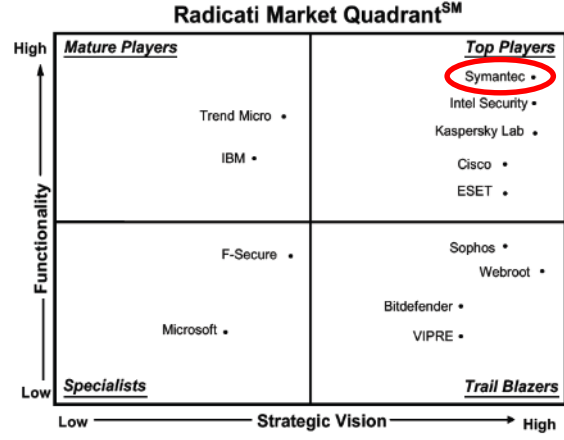
Content-Aware DLP



CASB



Endpoint Platforms



Endpoint Platforms

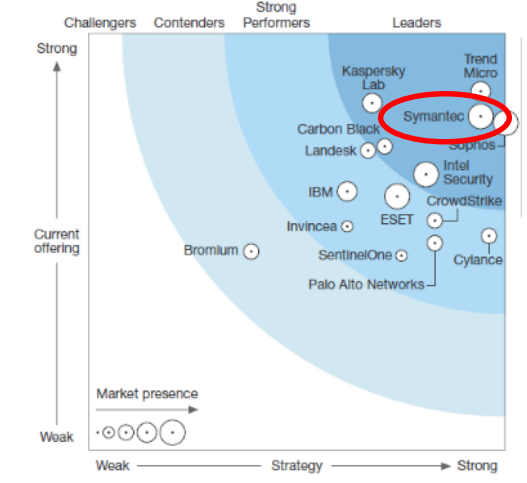
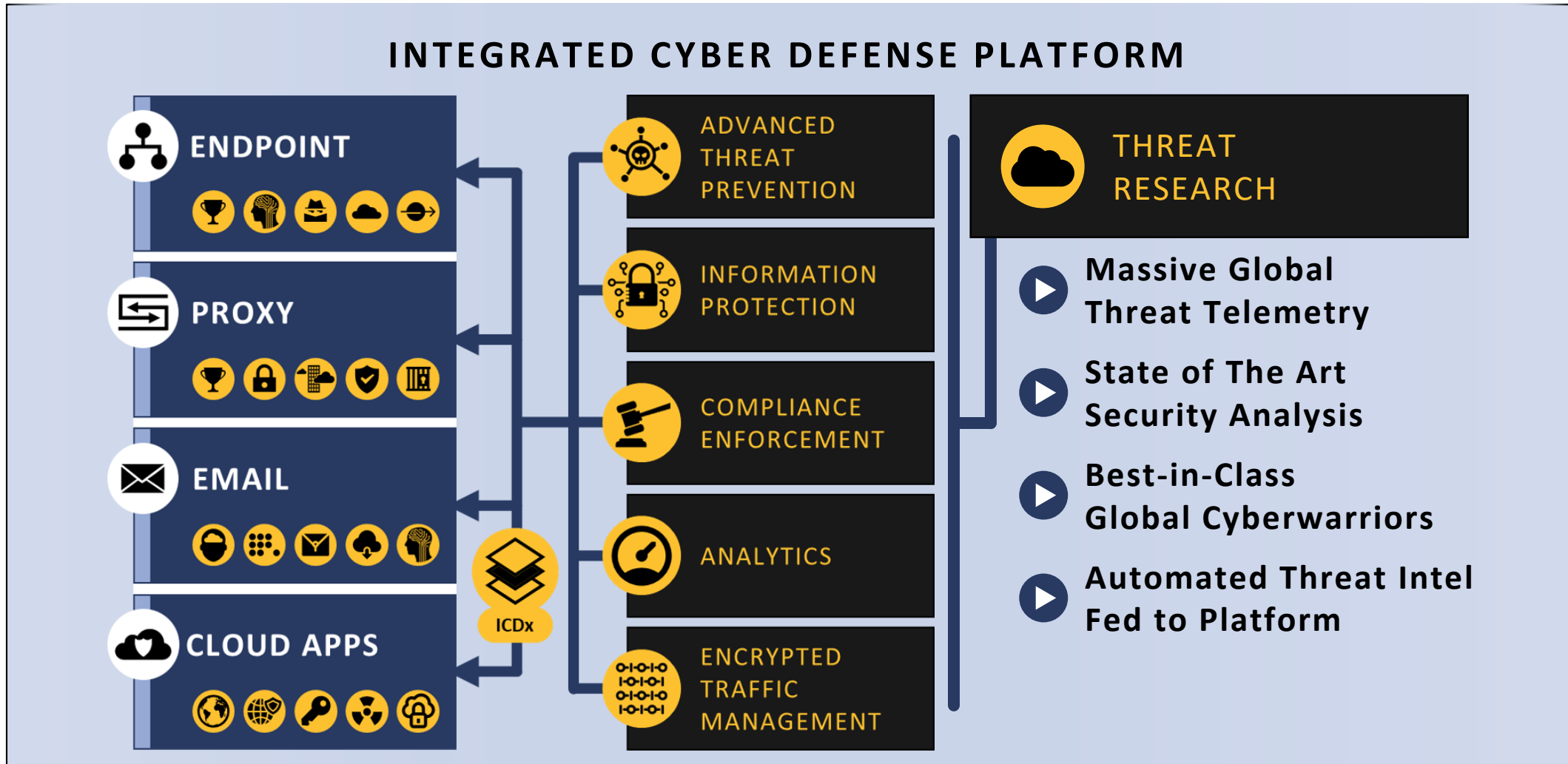


Figure 2: Endpoint Security Market Quadrant, 2016

Most recent published release from Gartner, Forrester Wave, and Radicati

Delivering Protection in The Cloud Generation



Role of the Proxy



The Power of a Proxy in Security



proxy 

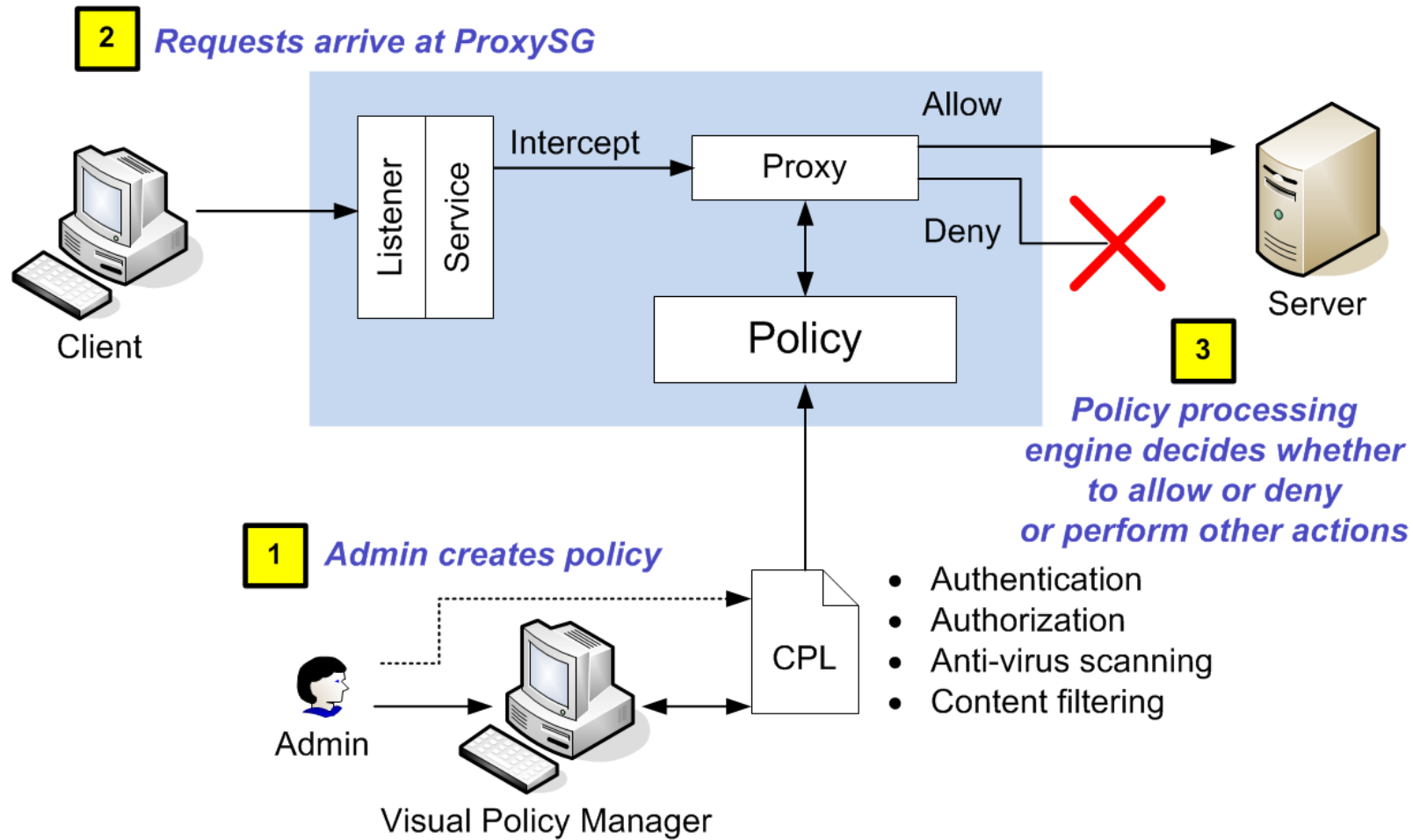
noun | \ˈprāk-sē\

: a person who is given the power or authority to do something (such as to vote) for someone else

: power or authority that is given to allow a person to act for someone else

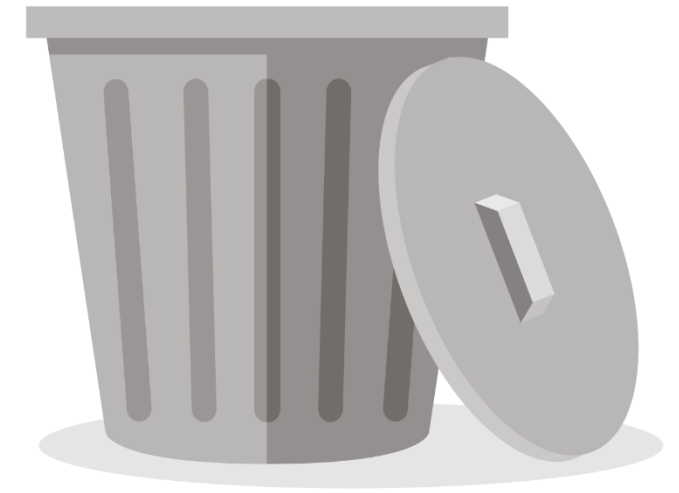


How Proxies Work



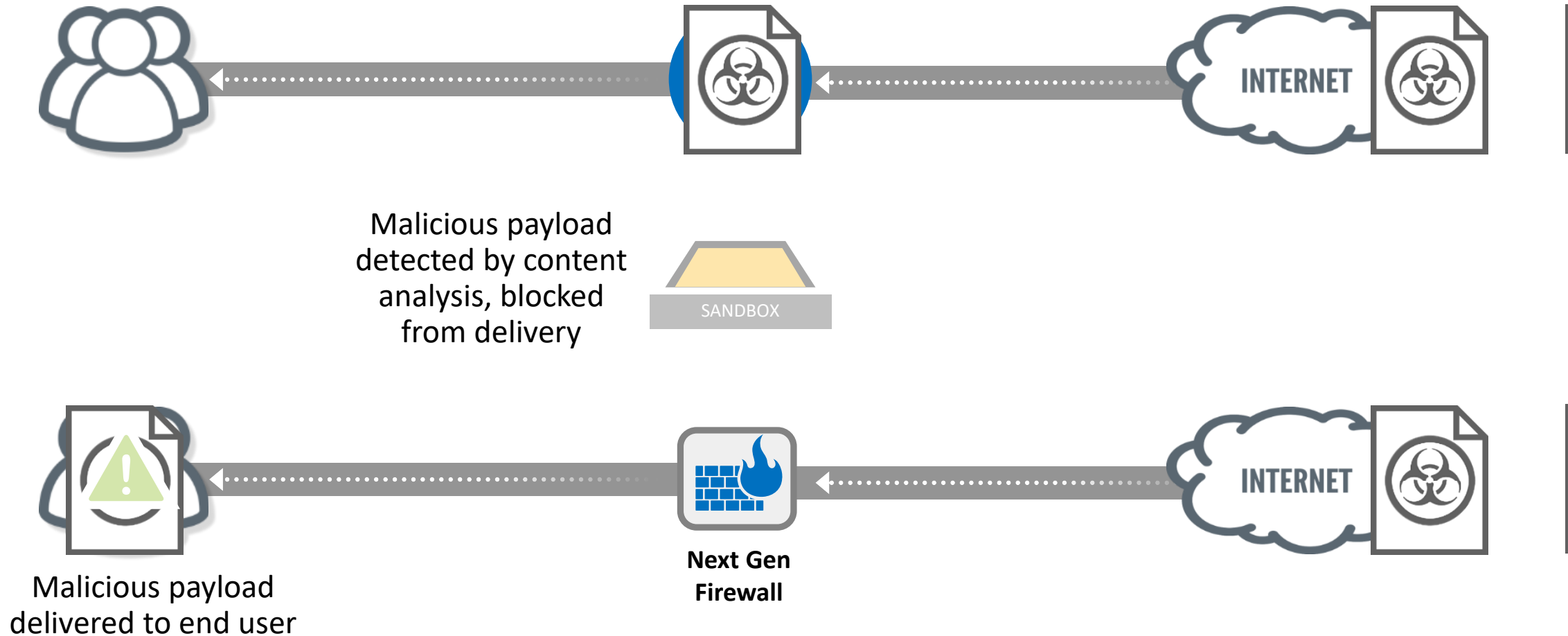
Traditional Network Platform

Proxy-Based Architecture-Full Picture



Effective Prevention

Proxy Architecture Compared to Next Gen Firewall

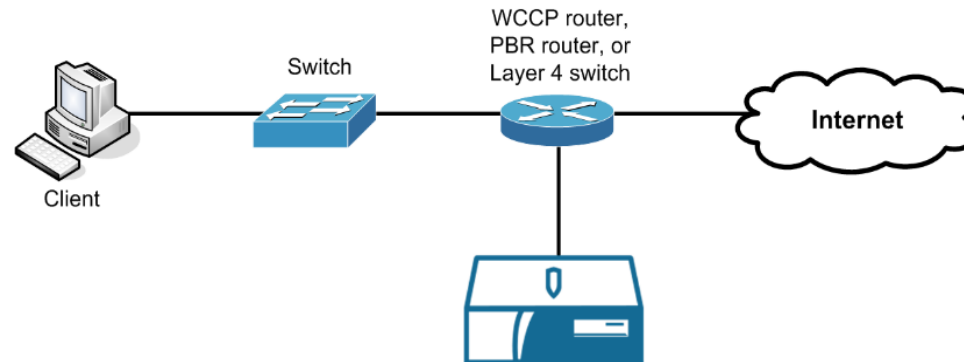


Deployment options

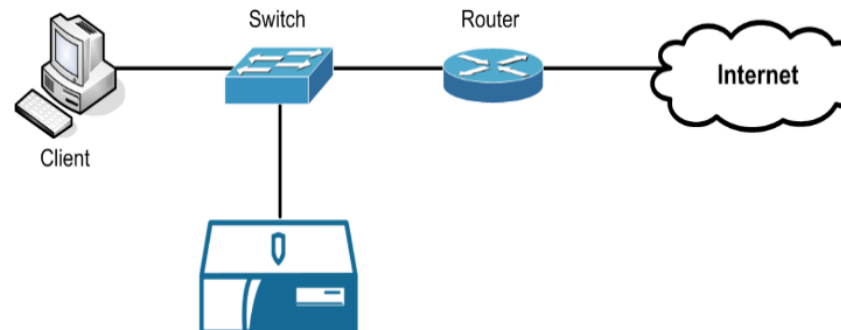
- Physically inline



- Virtually inline



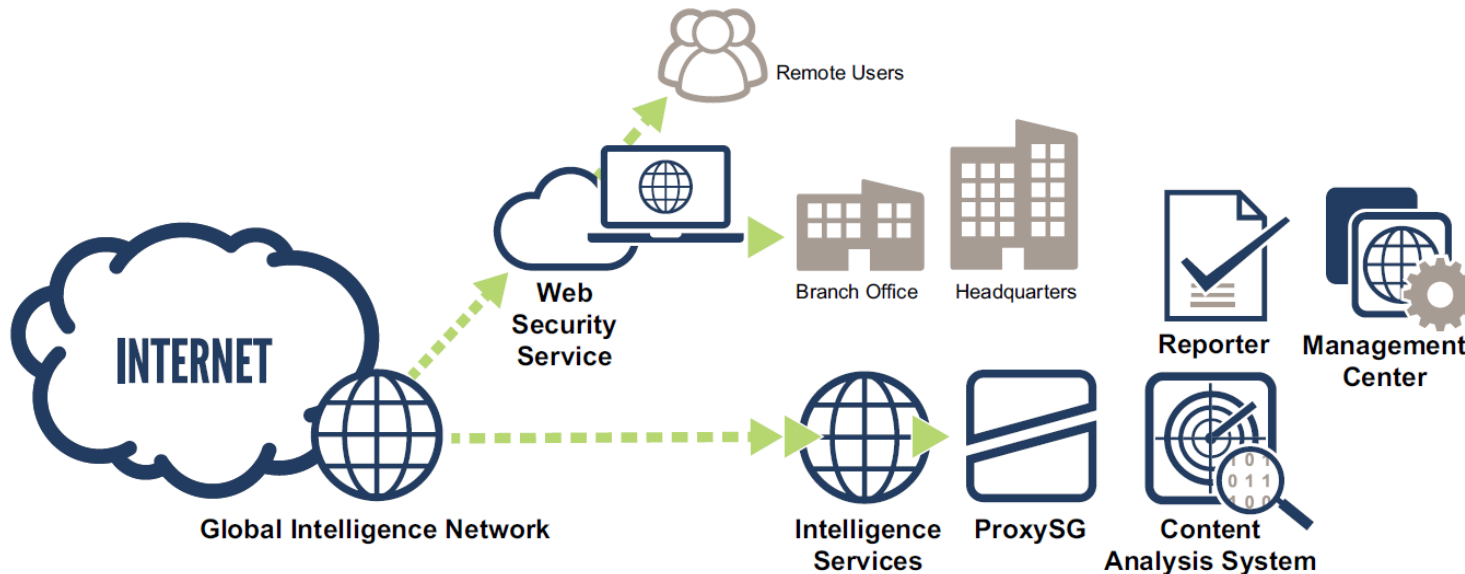
- Out-of-path



Symantec Secure Web Gateway



Symantec Secure Web Gateway



Symantec SWG Delivers:

- Negative Day Threat Defense
- Hybrid Delivery Model
- Strong User Authentication
- Visibility Into Encrypted Traffic
- Integration with ATPs Across Industry
- Control Over Web & Cloud Usage
- Performance & Reliability
- Accelerated Cloud App Performance
- Scalability & Lower TCO



ProxySG

Description

Physical or virtual appliance SWG solution delivering an advanced set of technologies working together to protect your organization in the cloud, across the web, social media, applications and mobile networks.

Differentiators

- Market leader (Gartner, Forrester, Radicati) for over a decade; 15K global enterprises depend on SG
- Cloud deployment for branch offices and remote users, centrally managed with Universal Policy
- Demonstrably superior results for threat prevention and information security/compliance
- Best in Class SSL inspection - received only “A” rating for secure inspection (recent 3rd party report)
- ICD outcomes – reduced effort to remediate threats between network and endpoint, improved

Key Customer Issues / Pain Points Solved

1

Web, cloud, mobile has all collapsed onto http/https, exposing NGFW limitations; need strong security control point to protect enterprise (threats and infosec)

2

Complicated web/cloud AUP enforcement and logging requirements to satisfy corporate, regulatory and data privacy mandates

3

SSL/TLS encryption “blind spots” creates vulnerabilities

4

Poor existing gateway threat prevention architecture leaves enterprise exposed to advanced threats

5

Use of unsanctioned cloud apps creates risk of loss of compliance sensitive data

Symantec is Named a Leader in 2017 Gartner Magic Quadrant for Secure Web Gateways: A Leader for the 10th Time*



Figure 1. Magic Quadrant for Secure Web Gateways



Source: Gartner (June 2017)

*This is a reflection of the Blue Coat (Now Symantec) ProxySG.

Source: Magic Quadrant for Secure Web Gateways, Lawrence Orans, Peter Firstbrook, 12 June 2017, Gartner, Inc.

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Symantec. Gartner does not endorse any vendor, product or service depicted in our 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.

Radicati Market Quadrant 2018



Corporate Web Security – Top Player 11 times running

Corporate Web Security - Market Quadrant 2018

MARKET QUADRANT – CORPORATE WEB SECURITY

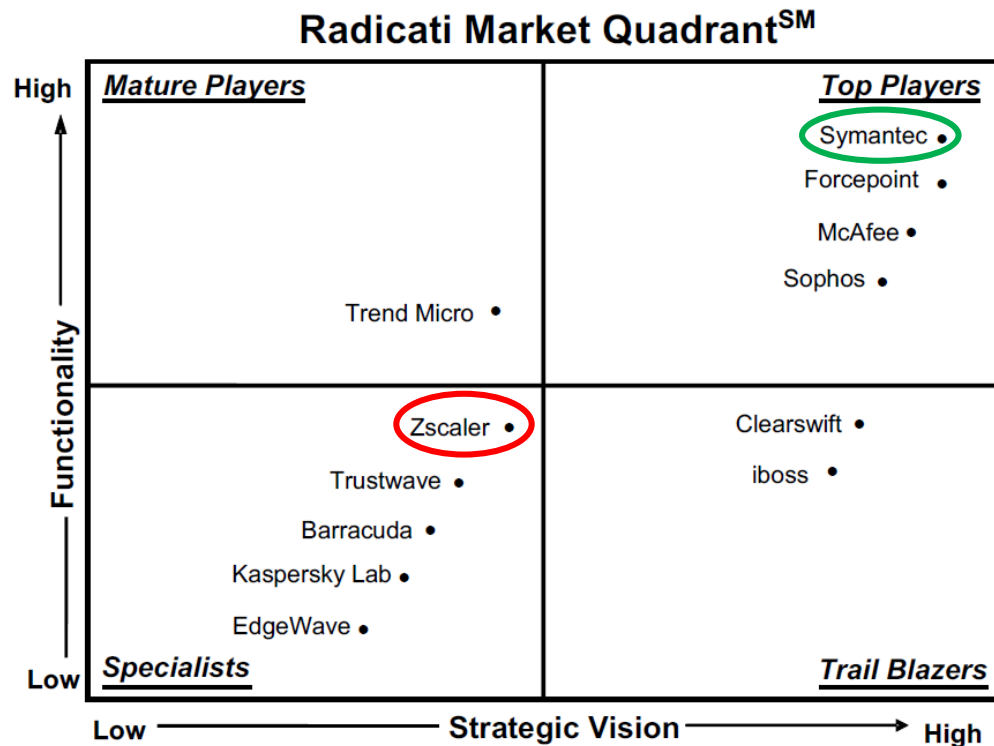


Figure 3: Corporate Web Security Market Quadrant, 2018*

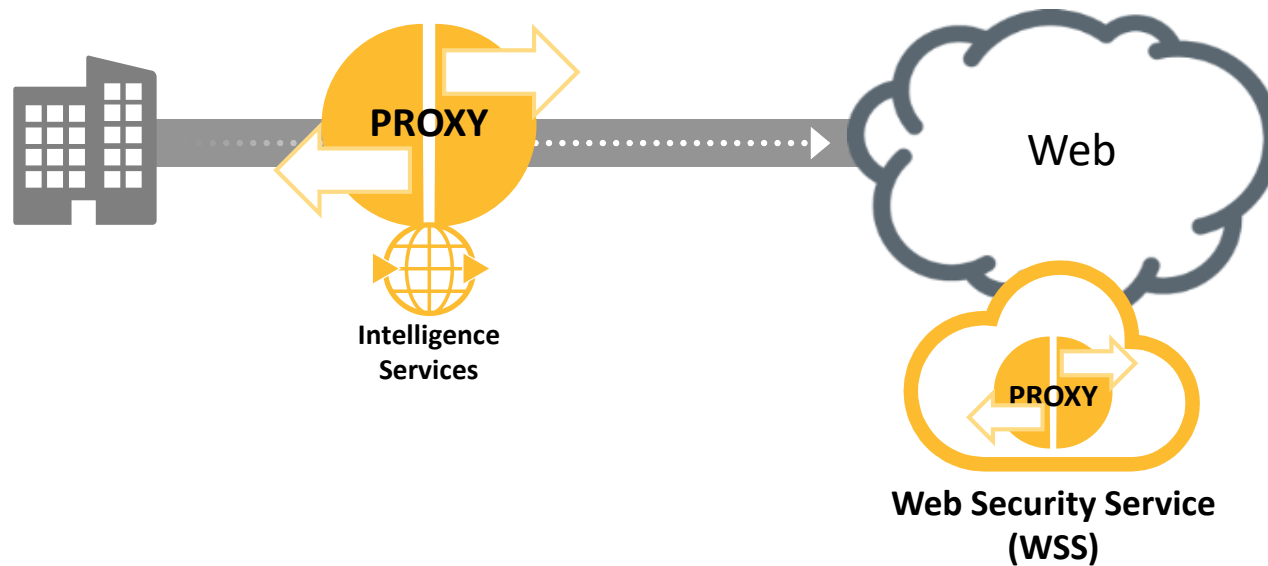
Zscaler WEAKNESSES

- DLP, bandwidth control, Web 2.0 controls, and other advanced features are only available on higher-priced packages of the Zscaler Web Security solution.
 - Zscaler no longer offers email security as part of its service portfolio, which may disappoint customers looking to source both web and email security from a single vendor.
 - Zscaler offers a cloud-based firewall service as an add-on to its SWG service. The firewall service, however, is not intended as a replacement for enterprise firewalls or UTM appliances, it is primarily suitable for small businesses, branch offices, roaming laptops or kiosks.
- Zscaler customers have reported instances of performance degradation, which have affected user satisfaction with the solution.
- Zscaler customers reported scaling issues and faulty functioning of VPN functionality as affecting their deployments.

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

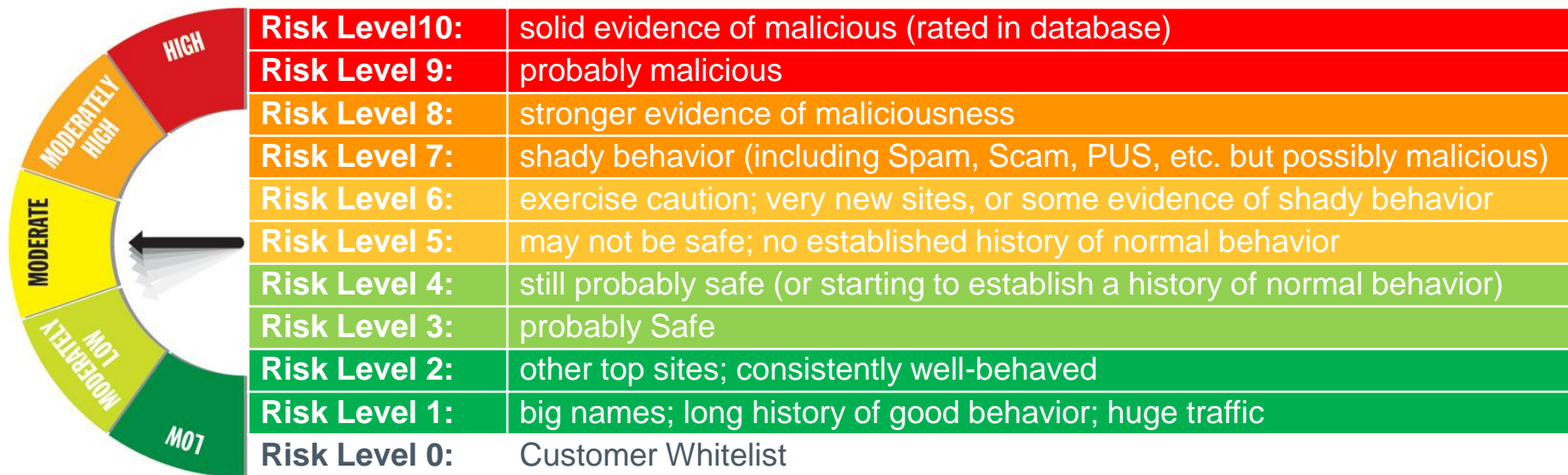
**Web Access Governance &
Threat Protection**

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

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

URL Threat Risk Levels

Eliminate The Riskiest Traffic Without Over-Blocking



Categorize and rank 1.2 billion of Web/URLs requests Per day

Provide granularity with 11 Risk Levels

Block 99.9% and over 50M malware threats daily

Categories, Intelligence Services, and Threat Risk Levels



Blue Coat Category Descriptions

- Abortion
- Adult/Mature Content
- Alcohol
- Alternative Spirituality/Belief
- Art/Culture
- Auctions
- Audio/Video Clips
- Brokerage/Trading
- Business/Economy
- Charitable Organizations
- Chat (IM)/SMS
- Child Pornography
- Computer/Information Security
- Content Servers
- Controlled Substances
- Dynamic DNS Host
- E-Card/Invitations
- Education
- Email
- Entertainment

DATA FEED

CONTENT CATEGORIES

SECURITY CATEGORIES

URL THREAT RISK LEVELS

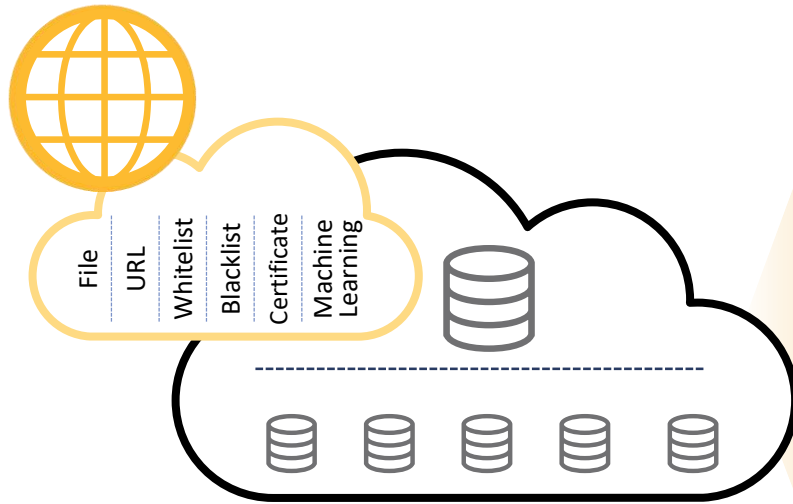
GEO LOCATION

BASIC WEB APPLICATION

CONTROLS



Global Threat Intelligence Network



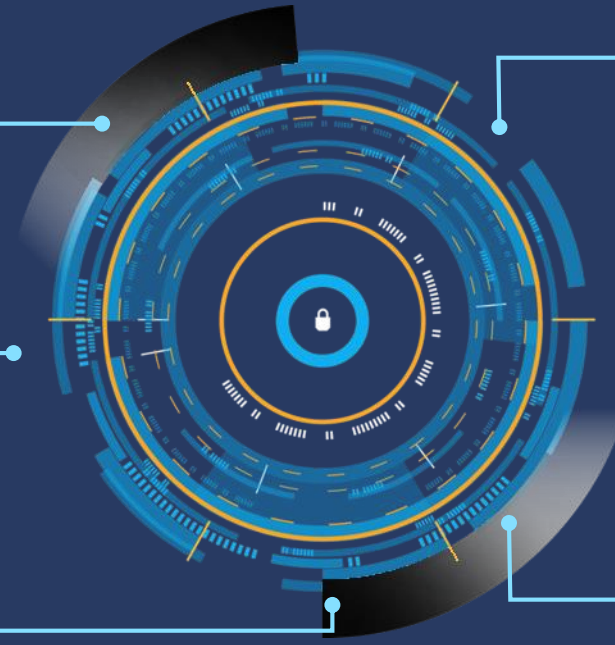
Discovered **430 million** new unique pieces of malware last year

1B malicious emails stopped last year

228M social engineering scams blocked last year

23,000+ Cloud applications discovered and protected

40B web attacks blocked last year



CLOUD GLOBAL INTELLIGENCE SOURCED FROM:



1.1 Billion previously unseen web requests scanned daily



2 Billion emails scanned per day



175M Consumer and Enterprise endpoints protected



9 global threat response centers with **3500+** Researchers and Engineers

Secure Web Gateway



ProxySG and Advanced Secure Gateway

Proxy All Endpoints

- Terminate and decrypt traffic
- Emulate all device types
- Extract content for inspection
- Integrate authentication



Control Web & Cloud Governance

- Discover & control shadow IT risk
- Block web-borne threats
- Enforce access policy & audit usage of web & cloud

Prevent Threats & Orchestrate Content

- Pre-filter sandbox with advanced content inspection
- Send content to DLP, sandbox, analytics, etc.
- Open integration architecture to quickly add new services

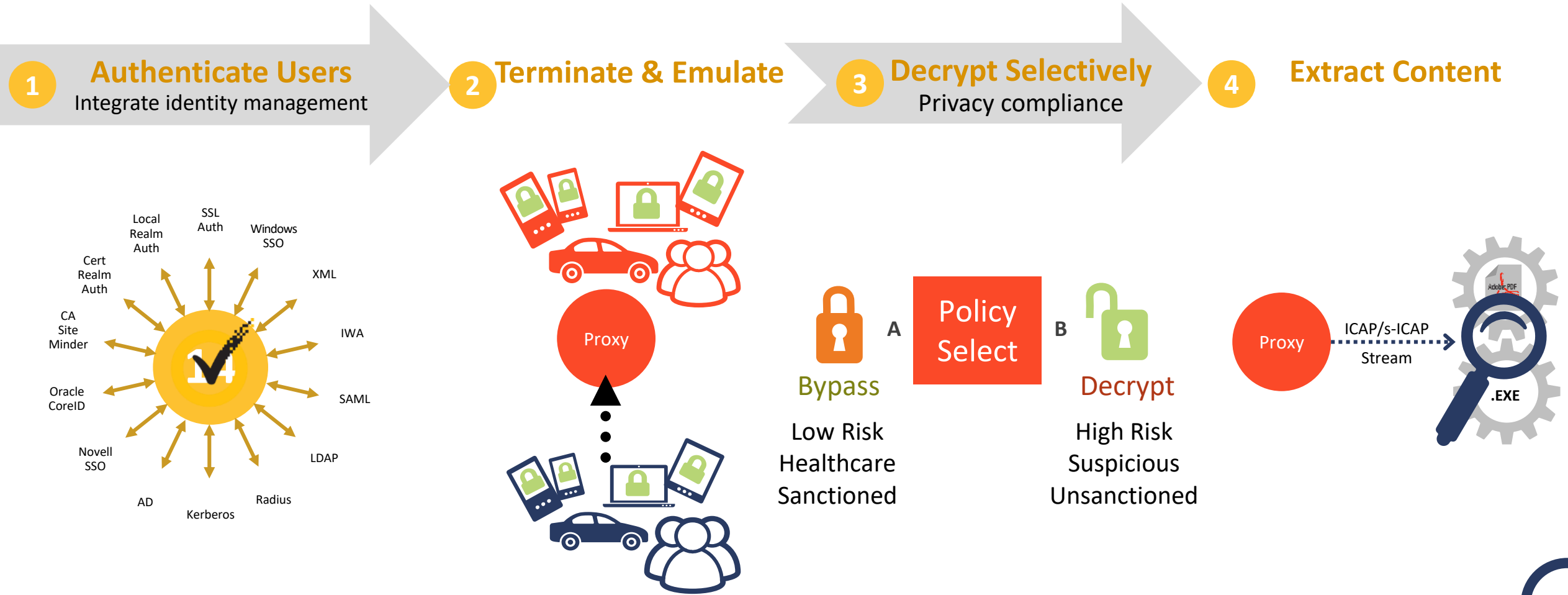
Enhance the User Experience & Performance

- Video Acceleration and Split Tunneling
- Asymmetric Caching of Content
- Optimized Protocol Support

Proxy All Endpoints



Architecture for Content Extraction and Device Emulation



Control Web and Cloud Access



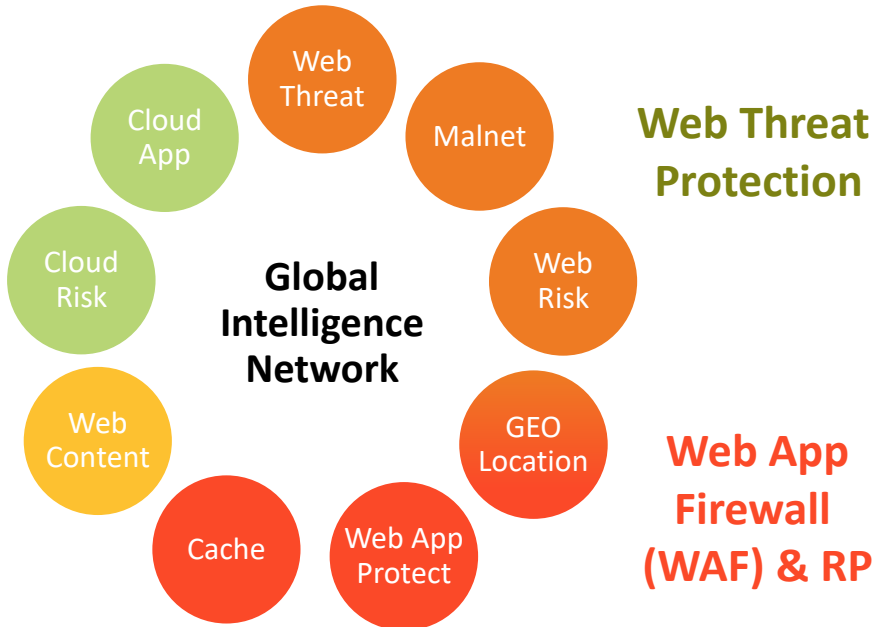
Access Governance and Policy Enforcement

- 21,000+ Cloud apps
- 60 attributes of risk and business readiness
- Drive Shadow IT control policy on Proxy/SWG

- 84 Total categories
- Across 55 languages
- Dynamic, real time rating

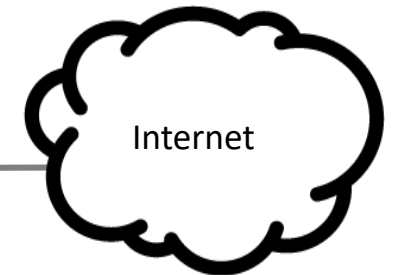
Cloud Access Security (CASB)

Acceptable Use



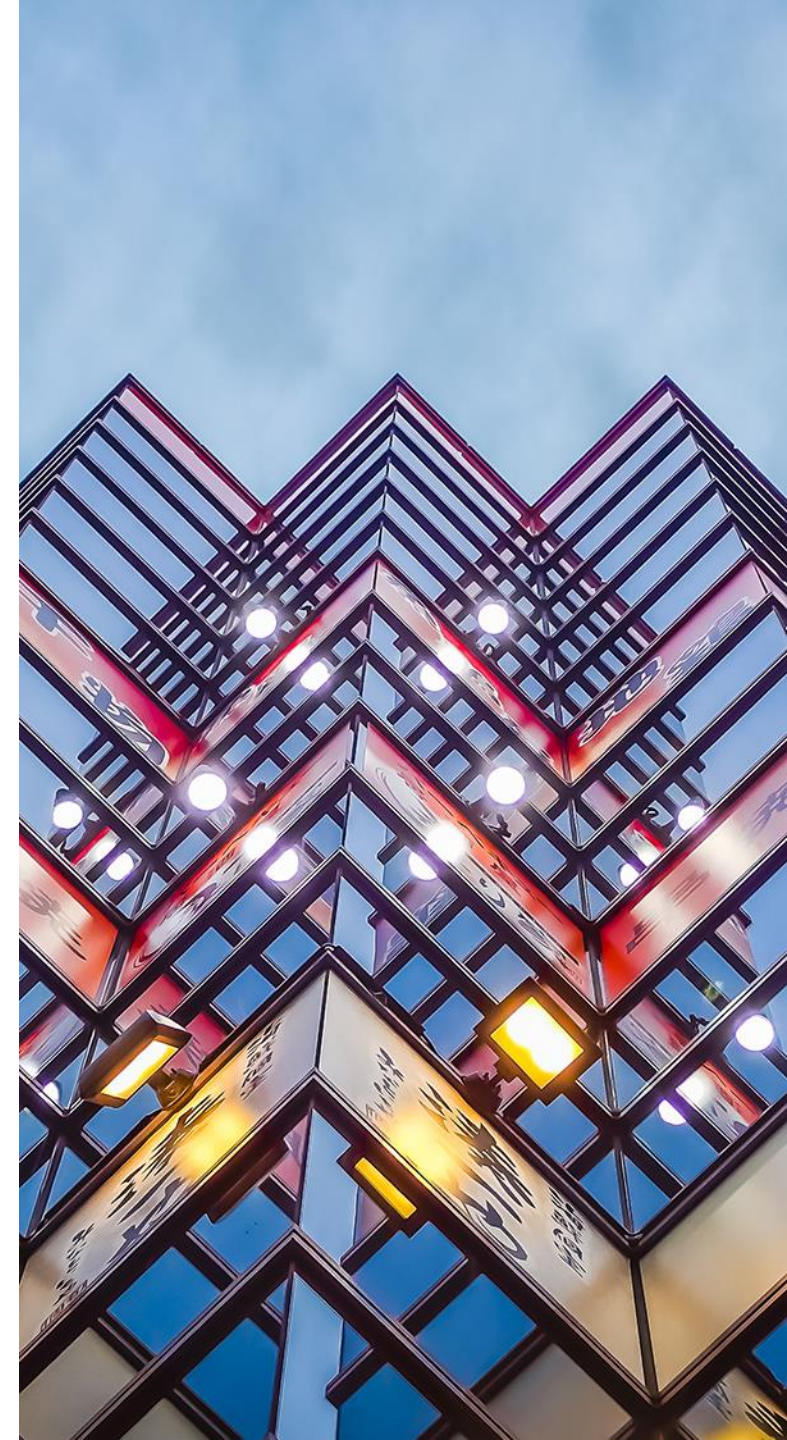
- 12 Security categories to block 90% of all threats
- Malnet stop zero day exploits
- URL Threat Risk – increases security without over-block

- OWASP Top 10 application protections
- Dynamic intelligence to maximize cache



SWG Platform

Providing Advanced Threat Protection



The Cloud-Generation SWG Strategy



Build Superior Advanced Threat Protection

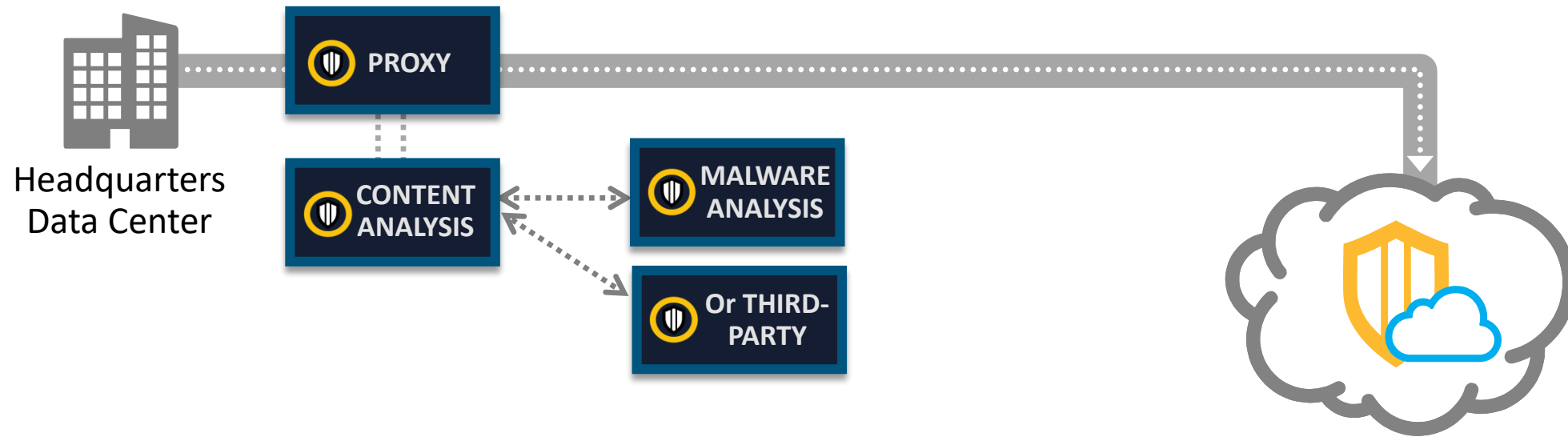
- Pre-filter & integrate sandboxing with Content Analysis (CA)
- Simplify ATP Architecture with Advanced Secure Gateway (ASG: Proxy + CA)
- Link malware detection and endpoint remediation (EDR) to simplify incident response
- Deploy an inline, active Web App Firewall to scale application protection
- Increase web security and simplify policy with URL Threat Risk

**Move to Cloud
Security**

**Scale True Hybrid
Deployments**

**Decrypt SSL-TLS
Responsibly**

Passing files to other devices



On Prem:

- **ProxySG** – decrypt, extract content, send via iCAP
- **Content Analysis**– pre-filters files (dual AV, WL, predictive), API to (any) Sandbox
- **Malware Analysis**– targeted emulation / virtual detonation

Cloud Service:

- **Web Security Service** – cloud proxy
- **Malware Analysis Service** – cloud sandbox

Content Analysis / Malware Analysis (Sandboxing)



Product Profile



Content Analysis/ Sandboxing

Description

Symantec Content Analysis leverages extensive threat intelligence and protects against advanced threats through file reputation matching, multiple anti-malware and analysis techniques, and sophisticated sandbox detonation.

Differentiators

- Multiple layers of threat inspection (Hash reputation, Advanced Machine Learning, Dual Antimalware engines)
- Adds centralized inspection to Proxy, SMG, SEP and ATP
- Dynamic, customizable sandboxing (Emulation/Virtualization) on-box or cloud
- Key reason Symantec is “Top Leader” in Radicati’s APT Protection Market Quadrant report

Key Customer Issues / Pain Points Solved



Need centralized, sophisticated and customized inspection beyond Proxy, email, endpoint



Too many security tools and too many alarms lead to missed attacks and high costs

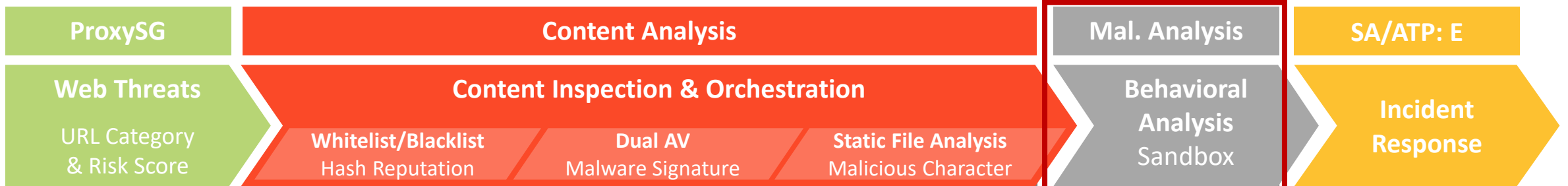


Have some inspection capability of “known” threats, need custom sandbox to find “unknowns”



I have FireEye, I need to improve accuracy and reduce the number of alerts and reduce cost

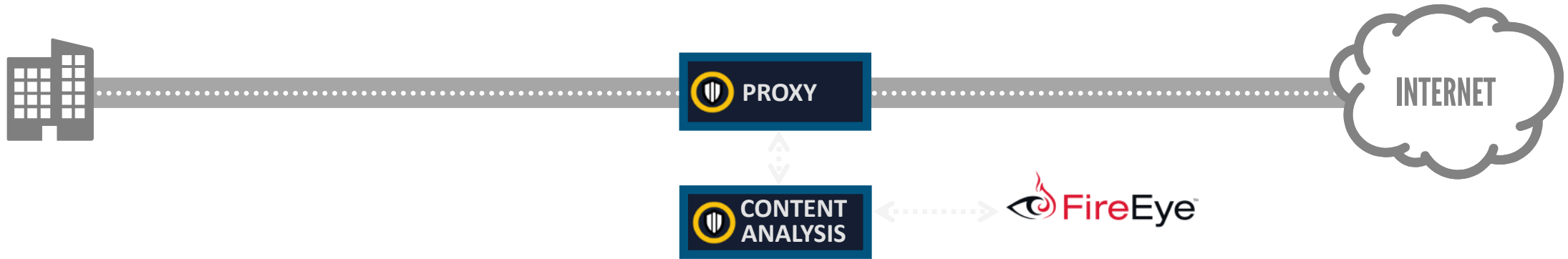
Reducing the Incident Response Queue



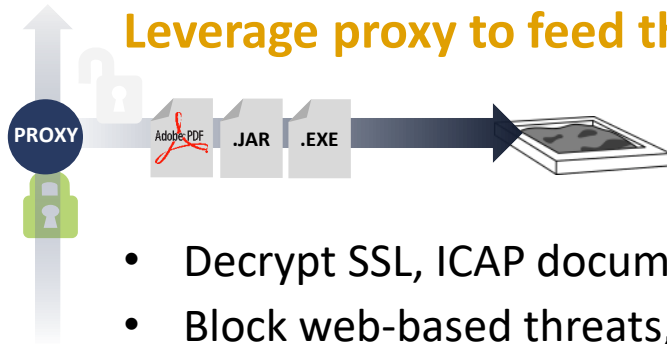
Content Analysis



Improve detection, reduce sandbox capacity requirements

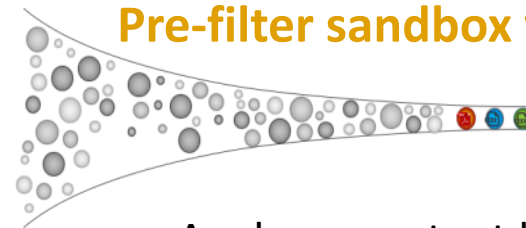


Leverage proxy to feed the sandbox



- Decrypt SSL, ICAP documents to sandbox
- Block web-based threats, C&C traffic
- High availability, inline, active blocking
- Enables centralized sandboxing

Pre-filter sandbox with content analysis

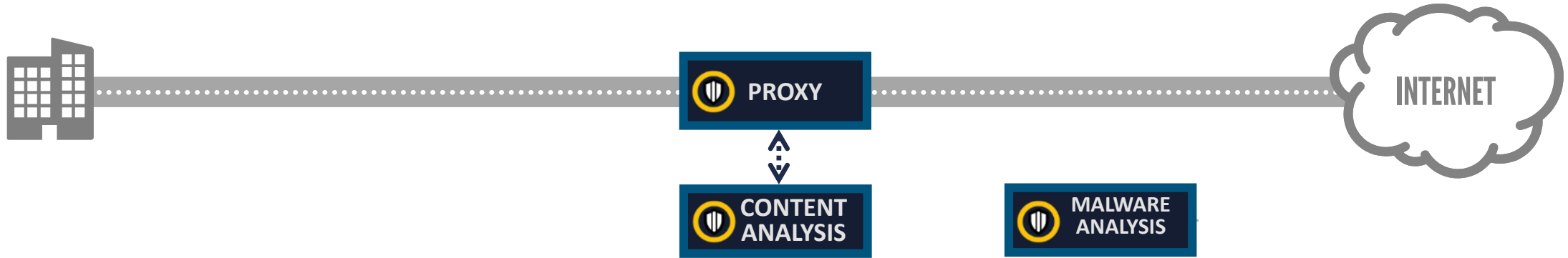


- Analyzes content before delivery to sandbox via API
- Applies multiple AV engines, white list
- File code analysis with machine learning finds zero-day threats

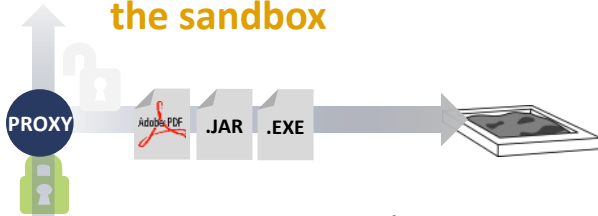
Symantec Malware Analysis



Add Emulated and Virtualized Detonation to Battle Advanced Threats

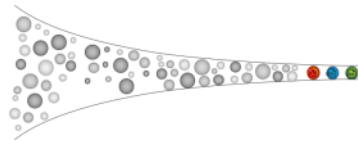


Leverage proxy to feed the sandbox



- Decrypt SSL, ICAP documents to CA
- Block web-based threats, C&C traffic
- High availability, inline, active blocking
- Enables centralized sandboxing

Pre-filter sandbox with content analysis



- Analyzes content before delivery to sandbox via API
- Applies multiple AV engines, white list
- File code analysis with machine learning finds zero-day threats

Target sandbox detonation for faster results

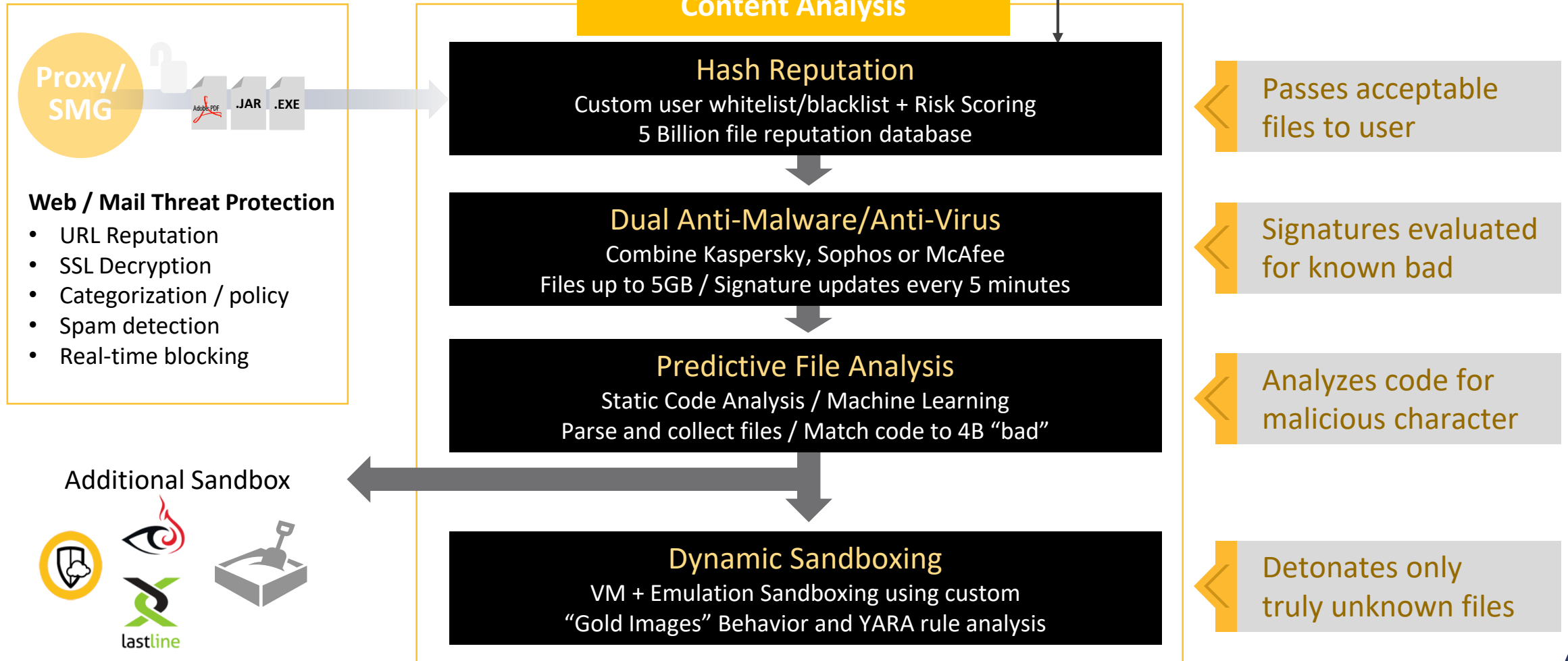


- YOUR standard OS images
- Faster analysis, with lower required CPU/memory
- Work with proxy to delay delivery until cycle completes

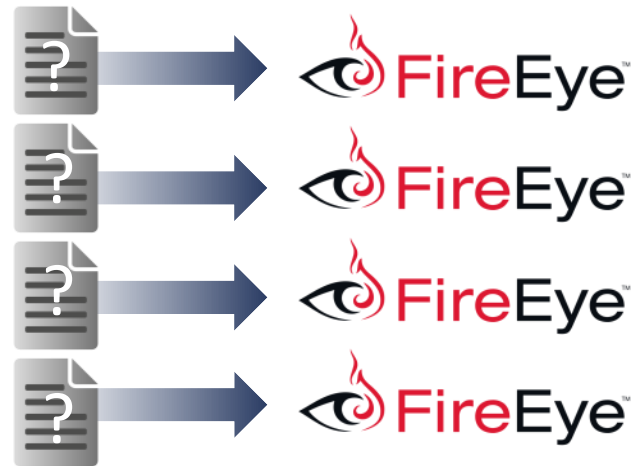
Content & Malware Analysis



Thorough Inspection = Better Protection

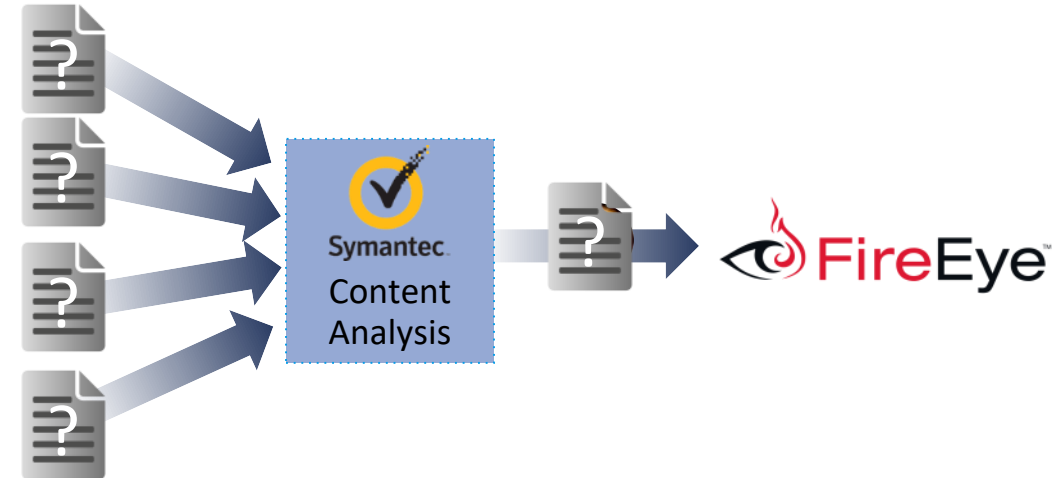


Dramatically Reduce Sandboxing Costs



50% Reduced Sandbox Cost

- Reduce sandbox capacity 75%
- Dramatically fewer samples to process
- Centralized architecture “pools” sandbox
- Lower capital acquisition costs



90+% Savings on Incident Response Costs

- 4x better detection
- Trusted inline proxy position
- Prevents malware delivery
- Dramatically reduced alarms

Advanced Secure Gateway - ASG



Simplify Your ATP Architecture



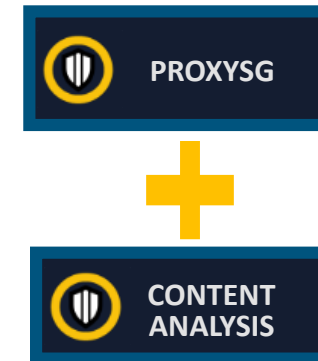
**Advanced Secure Gateway
(ASG)**

Authenticate, Enforce, & Log
See and Control Shadow IT
Block Web Threats & ATP C&C

Decrypt SSL, extract documents
ICAP documents
Prevent delivery based on verdict
Stream decrypted data to forensics

**Unify Access
Governance**

**Extract &
Orchestrate Files**



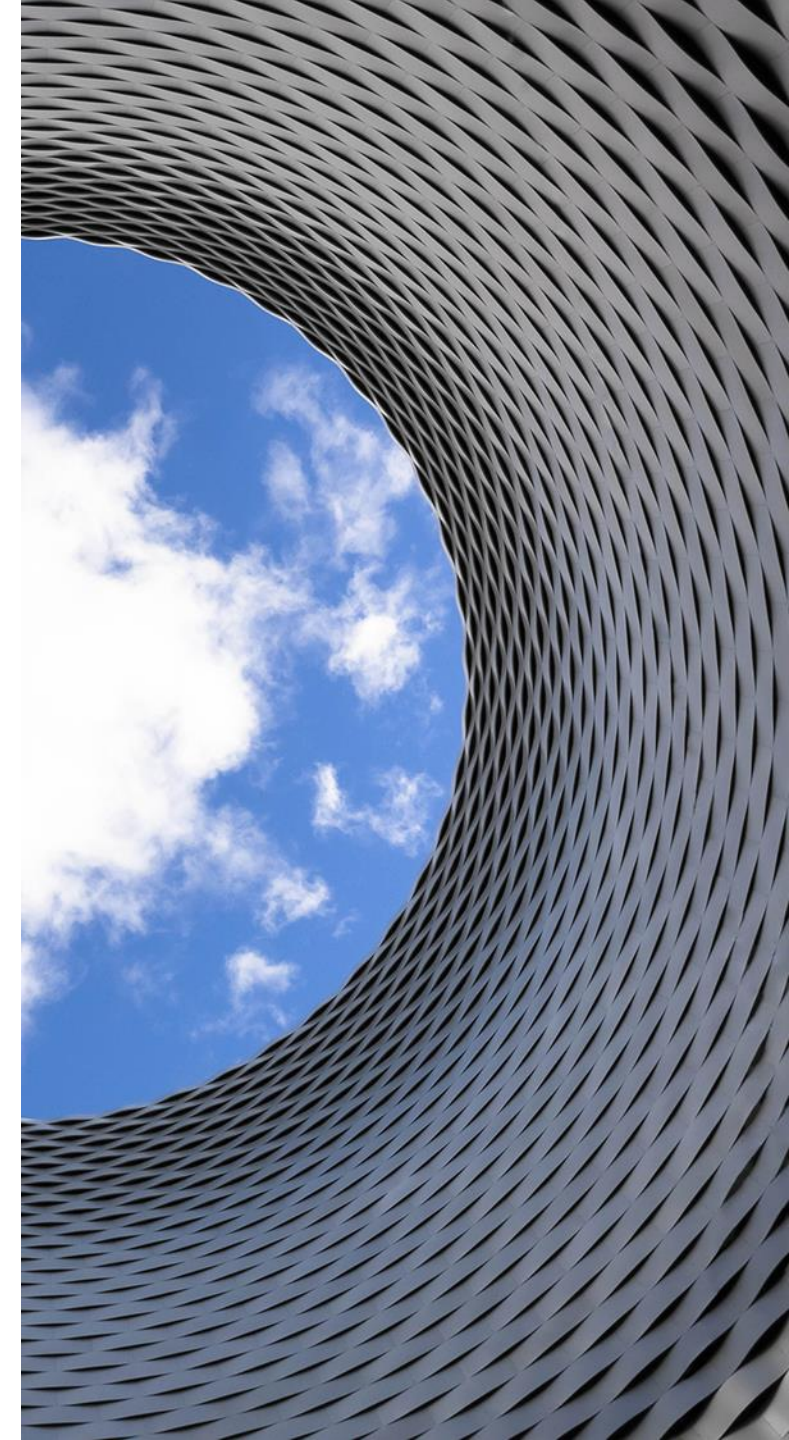
**Inspect Files to Prevent Malware
& Advanced Threats**

Whitelist/blacklist
Dual A/V Signatures
Static Code Analysis
Filtering Sandbox Broker



Web Security Service

Proxy From the Cloud - For the Cloud



Web Security Service



Product Profile

Description

Complete advanced network security stack delivered as a cloud service, including SWG and firewall services, content analysis, sandboxing, web isolation, DLP, and CASB capabilities.



Web Security Service

Differentiators

- Most complete set of advanced network security services (SWG, FW, DLP, ATP, Isolation, CASB, SD-WAN)
- Performance/Uptime/Accessibility of global network with simple connectivity (SEP redirect, SD-CC)
- Best in class threat prevention (A rated SSL inspection, better detection 10X few false positives (Tolly Report), Web Isolation, CASB controls)
- Best in class DLP (always top of MQs and Wave reports)

Key Customer Issues / Pain Points Solved



Poor user performance & increasing cost of backhauling internet network traffic



Operational complexity and capex acquisition costs of full network security stack



SSL/TLS encryption “blind spots” creates vulnerabilities



Poor existing gateway threat prevention architecture leaves enterprise exposed to advanced threats



Complexity of managing a hybrid gateway deployment

Adoption of Cloud App Challenges



Headquarters Data Center



How Do I Move to Cloud Security to...

- › Protect my users from ubiquitous threats?
- › Secure data & comply with legal regulations?
- › Effectively manage new devices and mobile users?
- › Transition to cloud speed while maintaining flexibility?

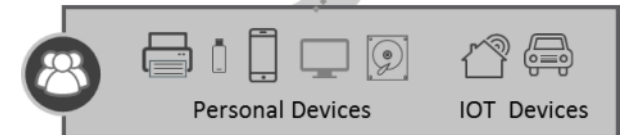
...With the capability, reliability, performance of on-prem security systems



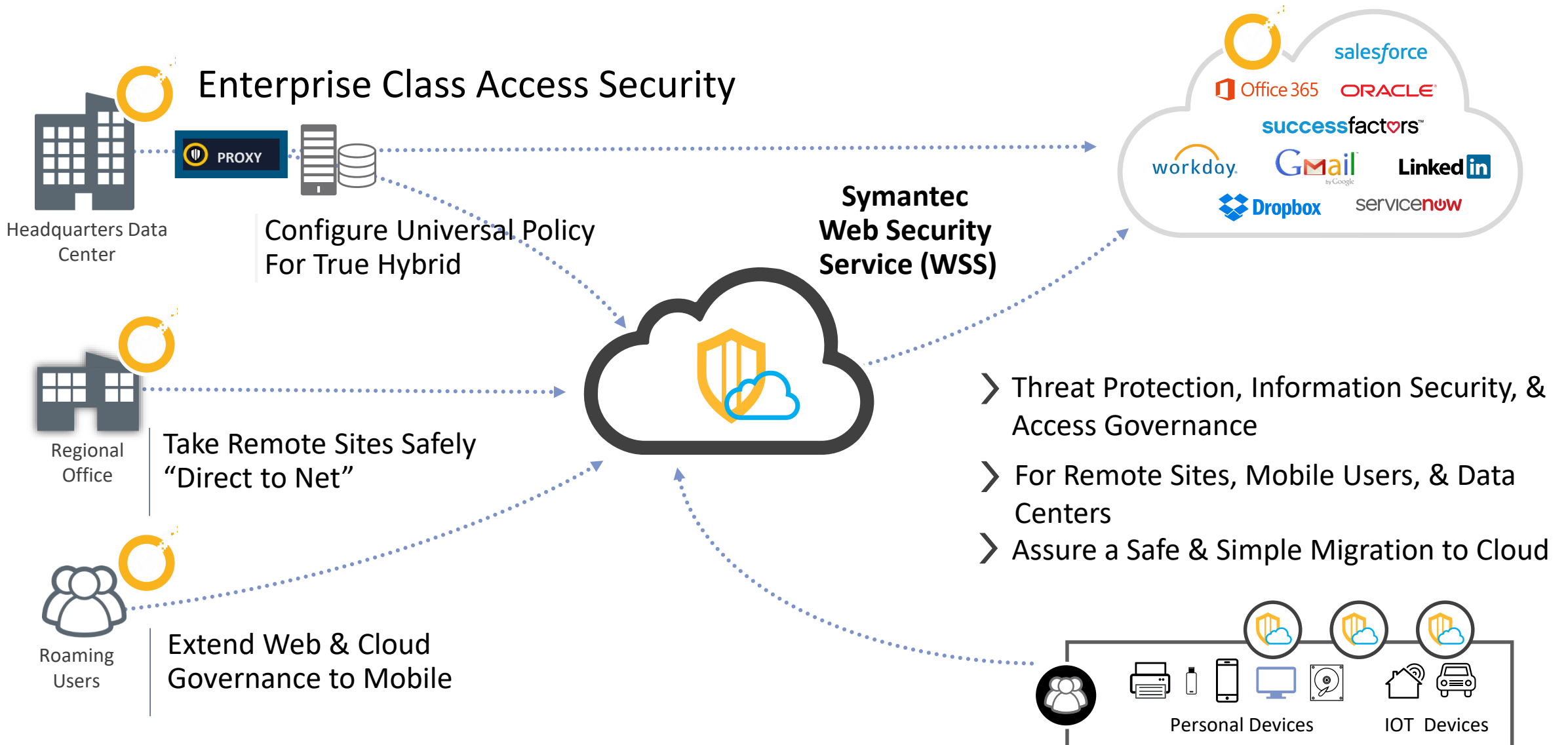
Regional Offices



Roaming Users



Symantec Web Security Service



Symantec Web Security Service



Full Security Stack in the Cloud

**Malware Scanning
& Analysis**



**Information
Protection**

Cloud delivered ProxySG Secure Web Gateway <

Set granular policies to control web usage <



**Symantec Web
Security Service**

> Cloud-only or mixed model (cloud & HW)

> Market-leading enterprise-class feature set

**Unified Management
(Cloud & Premise)**



CASB

SWG Integrations

Leveraging Proxy's Central Role in Cyber Security

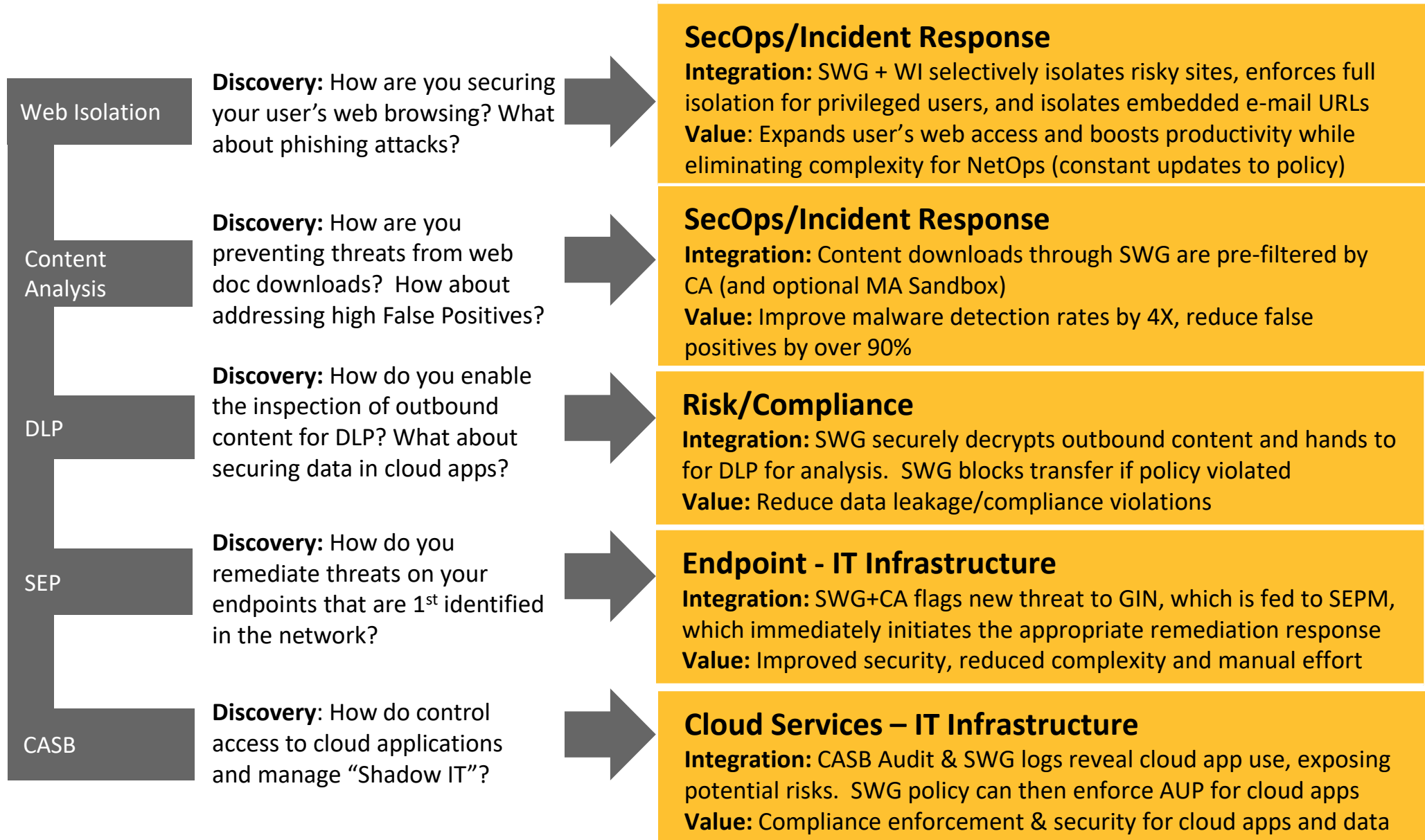


Using Integrations to Bridge Organizations



SWG

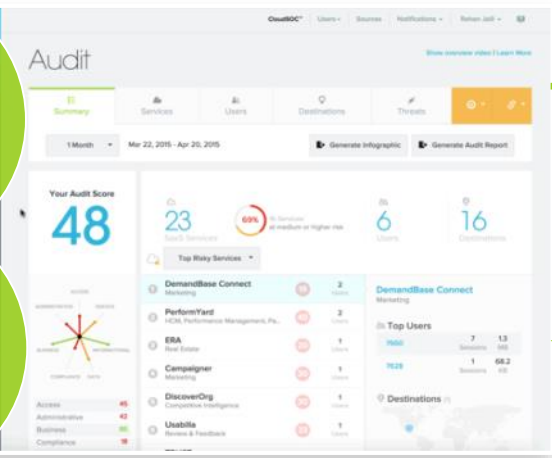
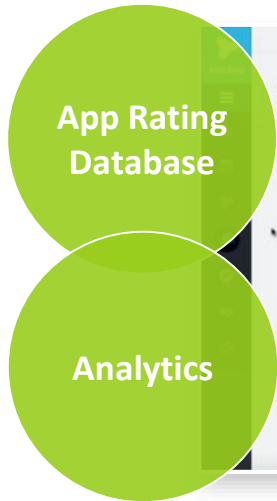
Network IT
Infrastructure



CASB - Cloud & Web Access Governance



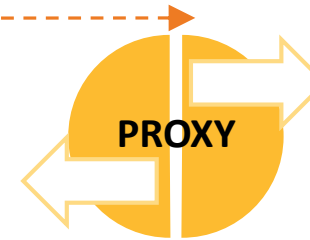
Web Security Service Policy Integration



Audit – AppFeed



GIN



PROXY



Symantec Web Security Service

Logs



Intelligence of 23,000+ Apps

Shadow IT Visibility

Scalable Proxy Policy to Control & Manage Risk



Roaming/
Mobile Users

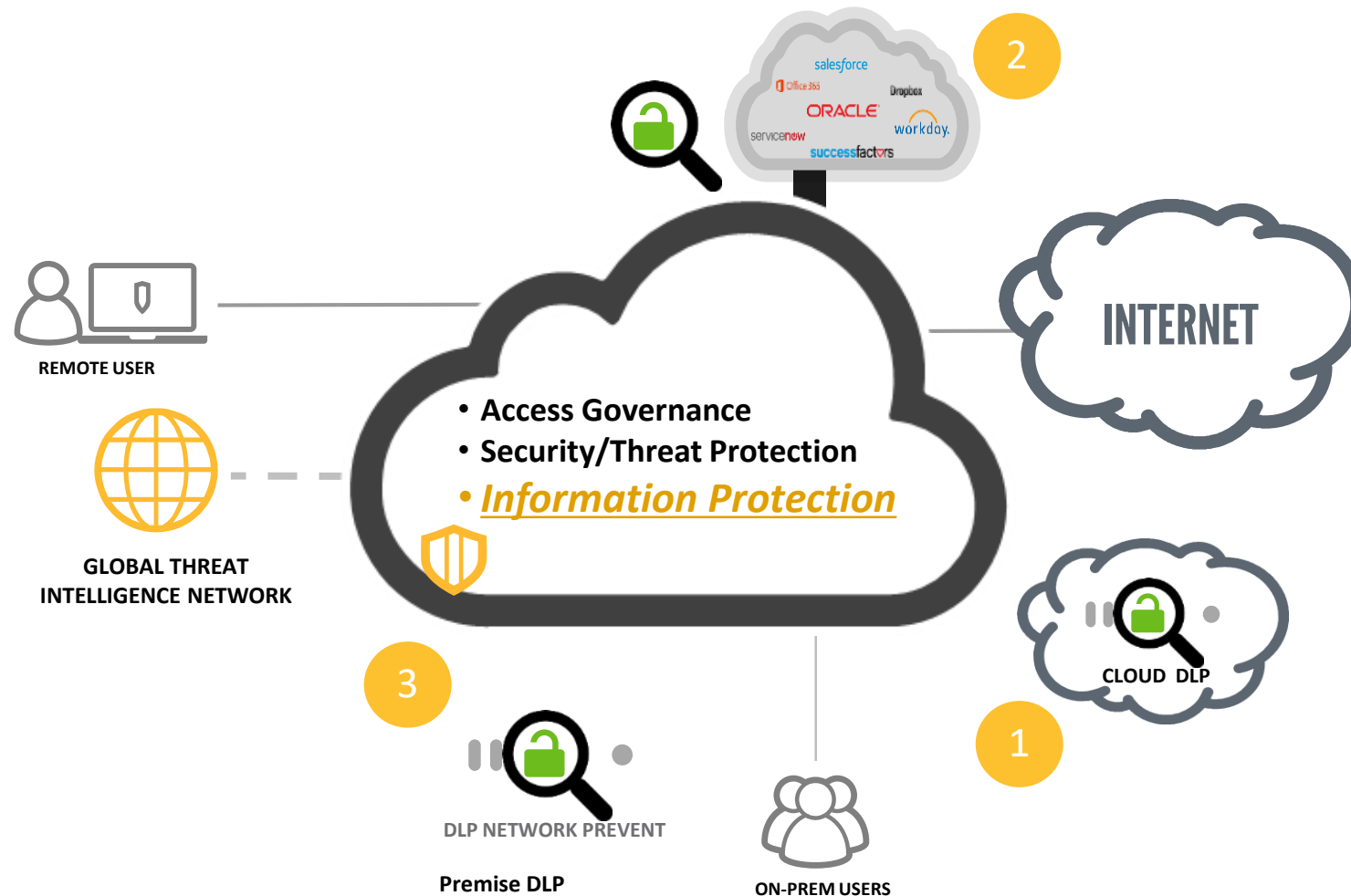


Offices

Web Security and Information Protection



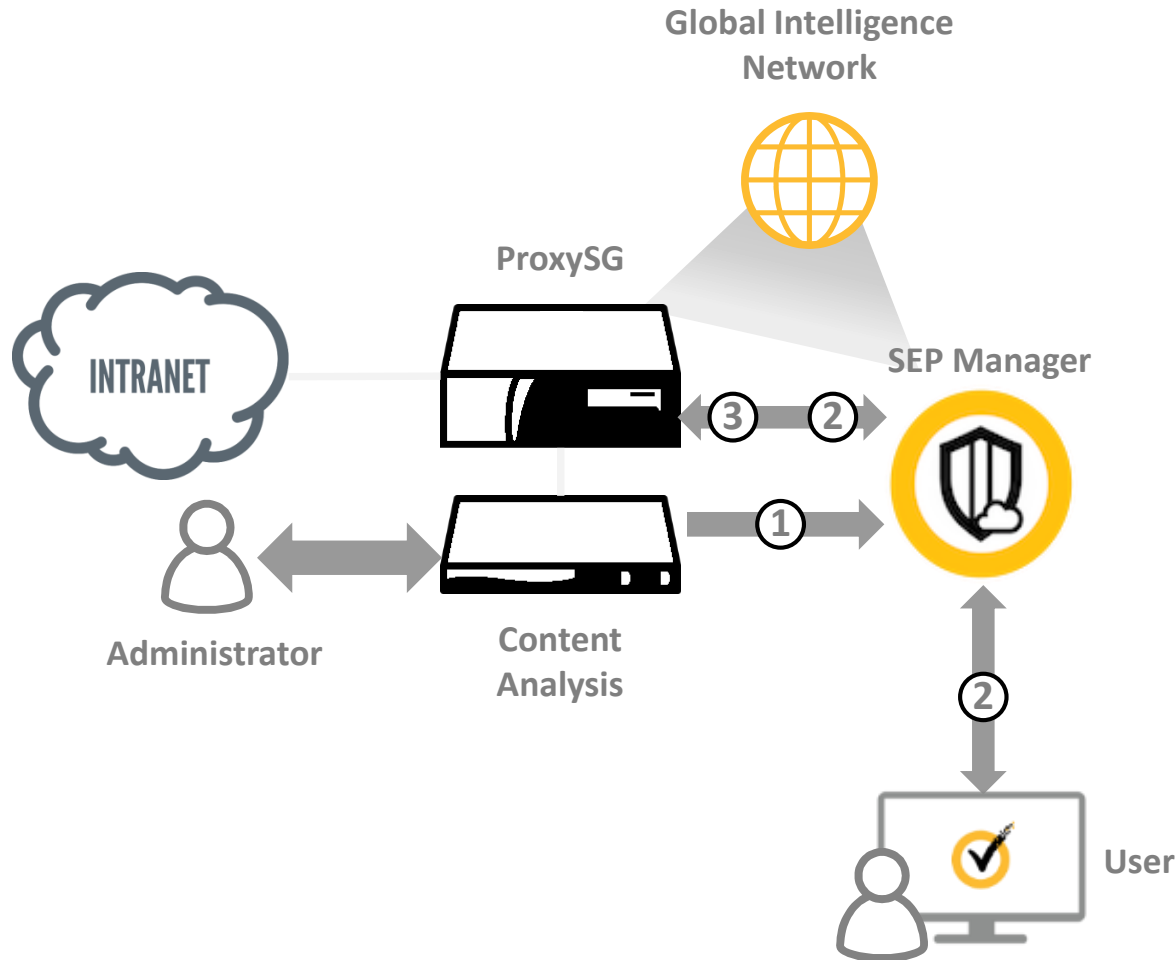
Extend Data Loss Prevention (DLP) Coverage to Cloud, Mobile, & Branch Users



- 1 Remote users? Direct to Net Branches? Leverage Cloud DLP with WSS.
- 2 Using Cloud SaaS Apps? Use CASB with Cloud DLP.
- 3 Have on-premise DLP already in place? Use it. One policy, effective everywhere

Integrate EDR with Gateway ATP Sandbox

Content Analysis with Symantec Endpoint Protection (SEP)



1. Content Analysis identifies potential threat using information from the Global Intelligence Network and sent to Symantec Endpoint Protection(SEP) Manager to verify
2. SEP Manager checks with endpoints to identify which are infected and responds to ProxySG
3. Remediation: blacklist communicated to
 - ProxySG / Content Analysis
 - SEP Manager

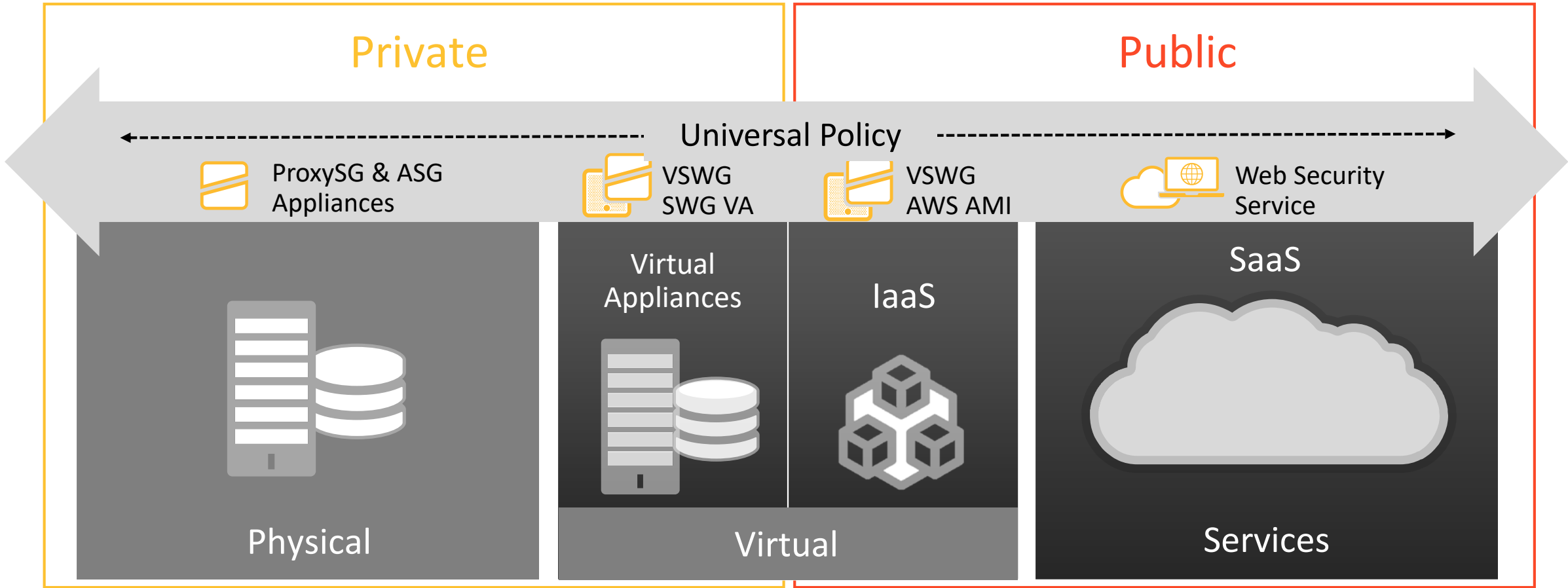
Summary



True Hybrid Security



Deploy to Match Your Needs



ProxySG appliance models



S200



S400



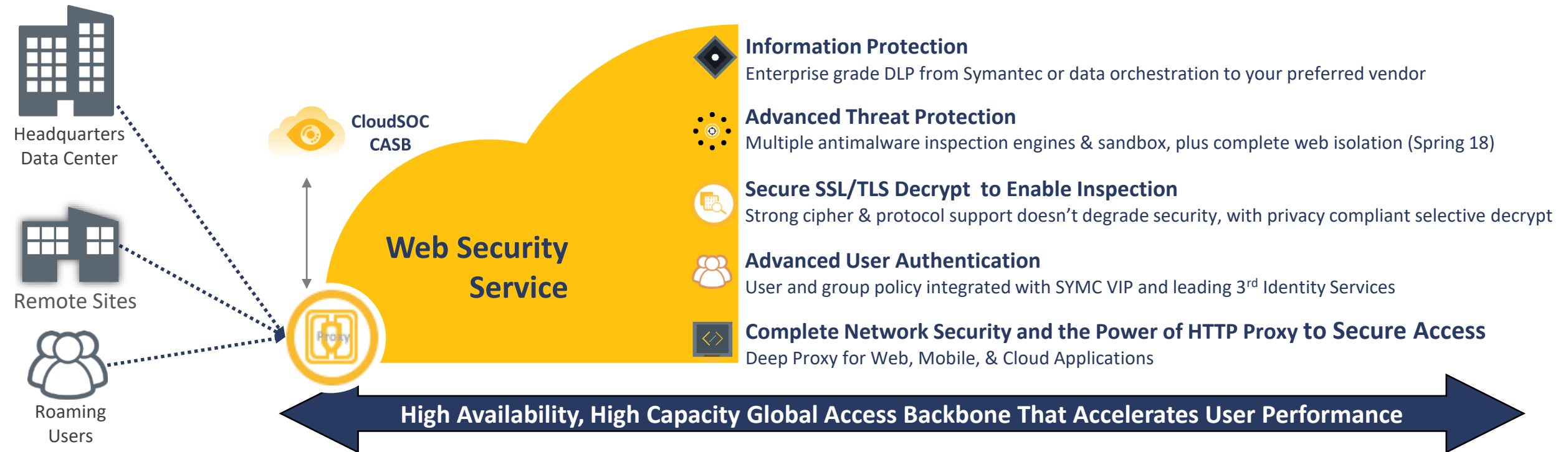
S500

ProxySG	SG S200-10	SG S200-20	SG S200-30	SG S200-40	SG S400-20	SG S400-30	SG S400-40	SG 500-10	SG 500-20/30
License Capacity									
Recommended Employee Count	500	1200	2600	5000	6000	14,000	25,000	30,000	50,000
System									
Disk Drives	500GB SATA	2 x 500GB SATA	2 x 500GB SATA	2 x 500GB SATA	3 x 1TB SAS ²	6 x 1TB SAS ²	8 x 1TB SAS ²	8 x 1TB SAS ²	16 x 1TB SAS ²
Boot Device	Single 16GB SSD				2 x 16GB SSD (dual redundant)				
RAM	6GB	8GB	8GB	16GB	16GB	24GB	32GB	64GB	128GB
Onboard Ports ¹	(2) 1000Base-T Copper ports (with bypass) (2) 1000Base-T Copper ports (non-bypass) (1) 10/100Base-T Copper, BMC Management Port							(2) 10Gb Base-T Copper ports (with bypass) (2) 10Gb Base-T Copper ports (non-bypass) (1) 1000Base-T Copper, System Management Port (1) 1000Base-T Copper, BMC Management Port	
Optional NICs	4x10/100/1000Base-T (Copper with bypass capability) 4x1GbE Fiber-SX (with bypass capability, full height slot only) 4x1GbE Fiber-LX (with bypass capability)				4x10/100/1000Base-T (Copper with bypass capability) 4x1GbE Fiber-SX (with bypass capability, full height slot only) 4x1GbE Fiber-LX (with bypass capability) 2x10Gb Base-T (Copper with bypass capability) 2x10Gb Base-T (Copper non-bypass) 2x10Gb Fiber (SR with bypass capability) 2x10Gb Fiber (LR with bypass capability)				



Web Security Service

A Full Network Security Stack Delivered In the Cloud



New Virtual Appliances: GEN 2 SG VA's



Scale to 1.6Gbps on Vmware ESX

- On-demand Proxy Capacity
- Forward Proxy and Reverse Proxy / WAF



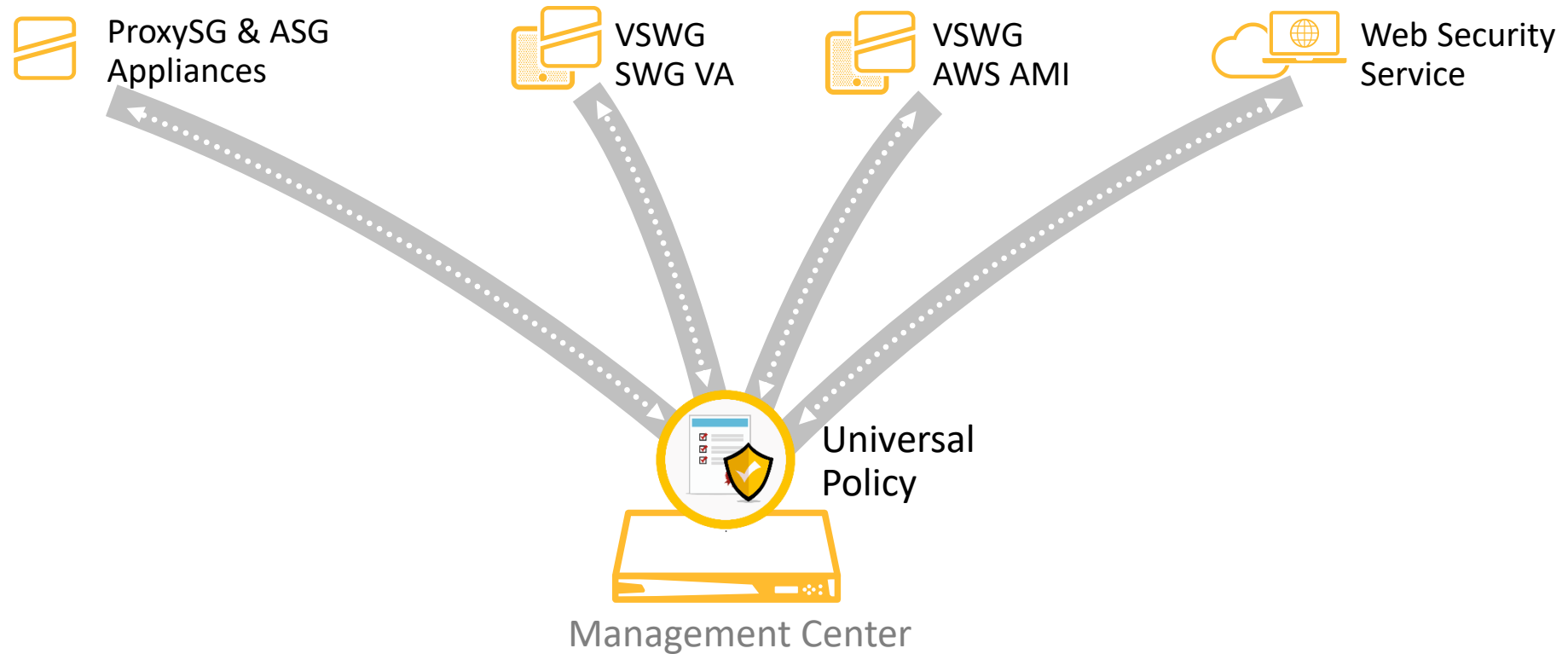
Gen 2 SWG VA SCALE ESX



Gen 1 SWG VA Multi-platform

Max Throughput	100M-1.6Gbps	100Mbps
Max Conns	250,000	10,000
Pricing Base	CPU-based pricing	Users
Pricing Options	1, 2, 4, 8, or 16 cores S, M, L Connection Capacity	25, 50, 100, 500, 1000, 2500 Users
BCWF/BCIS	Not included	Included
SKU Stub	SG-VA-SE	VSWG
Platforms	ESX	ESX, Hyper-V, AWS

Seamless Hybrid with Universal Policy



**Simply Extend Policy to Cloud
Web Security Service**

**Consistent Policy for On-Prem,
Mobile Users, Virtual**

**Centralize Reporting, Admin, & 55
Policy with Management Center**

Management Center/Reporter

Product Profile



Description

Protects websites from the OWASP Top 10 threats blocking known attack patterns with both signature-based, and signature-less content nature detection engines.

Differentiators

- Symantec integrations offer reporting and management from a single pane-of-glass and enable Unified Threat Reporting combining multiple threat intelligence sources.
- Pre-built and custom reporting capabilities with advanced filtering and analysis tools
- Improves the scalability, security and cost effectiveness SYMC network protection deployments

Management Center/Reporter

Key Customer Issues / Pain Points Solved

1

Need to manage an increasingly complex, growing infrastructure with a fixed budget and no additional headcount

2

Need to improve the consistency of devices and policy, which can become fragmented with a growing stack and our move to the cloud

3

Increasing load on web and cloud traffic makes uptime of my security stack a mission critical requirement



Thanks.

