Using cloud security to better protect Your organization
By 2020, Cisco Global Cloud Index estimates:

92% of global data center traffic will come from the cloud.
By 2021, Gartner estimates:

25% of corporate data traffic will bypass perimeter security.
Agenda

What’s happening in the market
Defining the Secure Internet Gateway
What sets Cisco Umbrella apart
The way we work has changed

Critical infrastructure
Amazon, Rackspace, Windows Azure, etc.

Business apps
Salesforce, Office 365, G Suite, etc.

Roaming laptops

Branch office

Workplace desktops
Users and apps have adopted the cloud, security must too

70% increase in SaaS usage
70% of branch offices have DIA
49% of the workforce is mobile
82% admit to not using the VPN

Security controls must shift to the cloud
Secure Internet Gateway

Your secure onramp to the internet, anywhere users go

On and off the corporate network
All ports and protocols
Open platform
Live threat intelligence
Proxy and file inspection
Discovery and control of SaaS
Cloud Access Security Broker

Protect the usage of business applications and critical infrastructure in the cloud

Discovery and control of SaaS

User & entity behavior analytics for compromised accounts and insider threats

Cloud DLP for data exposure and compliance violations

App firewall for cloud malware and shadow IT
## How a SIG compares to a NGFW

<table>
<thead>
<tr>
<th>SIG</th>
<th>NGFW</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main focus:</strong></td>
<td><strong>Main focus:</strong></td>
</tr>
<tr>
<td>Secure internet access, anywhere users go</td>
<td>Control inbound and outbound traffic and inspect threats at the perimeter</td>
</tr>
</tbody>
</table>
## How a SIG compares to a SWG

<table>
<thead>
<tr>
<th>Feature</th>
<th>SIG</th>
<th>SWG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open platform w/ bi-directional API integrations</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SaaS discovery and control; works w/ CASB</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Internet traffic enforcement for all ports &amp; protocols</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Cloud-delivered security to cover on and off-network</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web traffic enforcement for ports 80/443 and HTTP/S</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web application visibility and control</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Web content filtering</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web data loss prevention</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Web productivity and bandwidth control</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
How a SIG compares to a SWG

**SWG**

**Problem:**
Incomplete coverage of destinations and files

**HTTP/S layer**
- AV

**DNS and IP layer**
- VENDOR FEEDS
- RETROSPECTIVE FILE INTEL

**SIG**

**DNS and IP layer**
- PREDICTIVE DESTINATION INTEL

**HTTP/S layer**
- AMP

**VENDOR FEEDS**
- RETROSPECTIVE FILE INTEL

**TALOS AND AMP SUPPORTING ENTIRE CISCO SECURITY PORTFOLIO**

*Cisco Umbrella*
SIG works with your security stack

Secure Internet Gateway

Network and endpoint
- NGFW
- Netflow
- Proxy
- Sandbox
- AV
- AV

Network and endpoint
- Router/UTM
- AV
- AV

Endpoint
- AV
- ROAMING

First line

SIG
Safe access anywhere users go, even off VPN
First line of defense and inspection
Secure onramp to the internet
Cisco Umbrella

Visibility and protection everywhere

Enforcement built into the foundation of the internet

Intelligence to see attacks before launched

Enterprise-wide deployment in minutes

Malware
C2 Callbacks
Phishing

208.67.222.222
DNS
Overview

Domain registrar
Maps and records names to #s in “phone books”

Authoritative DNS
Owns and publishes the “phone books”

Recursive DNS
Looks up and remembers the #s for each name
Who resolves your DNS requests?

Challenges

- Multiple internet service providers
- Direct-to-internet branch offices
- Users forget to always turn VPN on
- Different DNS log formats
Using a single global recursive DNS service

Benefits
Global internet activity visibility
Network security w/o adding latency
Consistent policy enforcement
Internet-wide cloud app visibility
Gather intelligence and enforce security at the DNS layer

**Authoritative DNS logs**
- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains
- Related domains

**User request patterns**
- Compromised systems
- Command and control callbacks
- Malware and phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

---

Any device

Recursive DNS

Authoritative DNS

root.com.

domain.com.
Enforcement built into foundation of internet

Umbrella provides:

- Connection for safe requests
- Prevention malicious requests
- Proxy inspection for risky requests
Intelligent proxy

- Requests for “risky” domains
- URL inspection
  - Cisco Talos feeds
  - Cisco WBRS
  - Partner feeds
- File inspection
  - AV Engines
  - Cisco AMP
Intelligence to see attacks before launched

Data
- 100B DNS requests resolved per day
- Diverse dataset gathered across 85M users across 160 countries

Security researchers
- 250+ industry renown researchers across Cisco Talos and Umbrella
- Build models that can automatically classify and score domains and IPs

Models
- Dozens of models continuously analyze millions of live events per second
- Automatically score and identify malware, ransomware another threats

Cisco Umbrella
INTELLIGENCE

Statistical and machine learning models

Guilt by inference
- Co-occurrence model
- Sender rank model
- Secure rank model

Guilt by association
- Predictive IP Space Modeling
- Passive DNS and WHOIS Correlation

Patterns of guilt
- Spike rank model
- Live DGA prediction model
- Natural Language Processing rank model

Cisco Umbrella

2M+ live events per second
11B+ historical events
SIG Vision

Threat intelligence, cross-product analytics, APIs, and integrations

- DNS-Layer
- Proxy
- File inspection
- Sandbox
- 3rd-Party
- CASB controls
- App visibility and control*
- Inbound inspection*
- New product*

Leveraging a global footprint

*Future