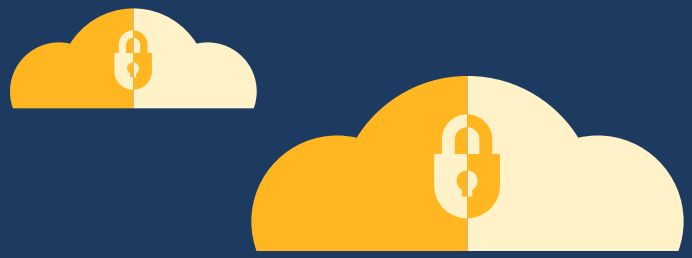
No Network Perimeter?
Now What?

When cloud apps, mobile devices and remote workers eliminate the concept of a network perimeter, it's time to think outside the security box.

Symantec™

CHAPTER 1

Secure the Cloud Generation



Beat back today's perfect storm of security challenges with network protection created for the Cloud Generation.

How do you secure mobile users, remote offices, and cloud apps? How do you meet your evolving compliance obligations... while battling endless and increasingly sophisticated cyber security attacks?

Backhauling sends branch and remote internet traffic to the corporate data center, where security and threat protection policies are applied. This model is fading in popularity as companies move their operations to the cloud because backhauling traffic over private multiprotocol label switching (MPLS) links is very expensive, and because backhauling creates latency issues that impact offsite employees trying to get to cloud apps and the web. Alternatively, employees can access cloud-delivered security services directly, eliminating backhauling; security policies are applied as traffic directly goes to the web and cloud applications.

In 2017

1 in 13

URLs analyzed at the gateway were found to be malicious.

That's up from 1 in 20 in 2016.

Suggestions:

- Make a cloud-based secure web gateway the foundation of your security infrastructure—it will protect your users and data wherever they are located
- Gain the security you need without sacrificing network performance or affordability
- Ensure you have industry-leading threat protection technologies
- Protect on-premises and remote/mobile users with unified security policies
- Select a comprehensive solution for effective and seamless protection

When hidden in encrypted traffic, malware can penetrate and overwhelm traditional network defenses. Most internet traffic today is encrypted, and bad actors increasingly use encryption to spread malware.

CHAPTER 2

Build Your Defense Around an Advanced, Cloud-delivered Secure Web Gateway

The Cloud Generation requires a secure web gateway (SWG) that covers more than just the web and cloud application security basics.

Secure web gateways (SWGs) speed secure data flow to web and cloud apps, uniquely scanning traffic—even when it is encrypted—for malware and information security compliance violations. This is why a SWG is the perfect foundation for your network security stack. An advanced, cloud-delivered secure web gateway goes beyond traditional basic functions (such as enforcing your company's acceptable web use policies). It uses threat intelligence data to assess the risk of URLs, so your employees don't end up on risky sites, and it incorporates inspection technologies to check traffic for cyber-threats, and data loss. And some SWGs are incorporating innovative technologies like web isolation to add additional threat protection for your users. A full-featured SWG can provide the comprehensive capabilities you need to solve the critical security and compliance challenges you face. Best of all, when it is delivered in the cloud, you can route your users' traffic through it at all times, making sure they are protected wherever they are and on whatever device they are using.

Suggestions:

- **Selectively inspect encrypted traffic to accurately scan content for malware and compliance violations.**
  - Quickly and securely inspect SSL/TLS encrypted traffic to get the protection your organization needs and the performance your users demand. Most internet traffic is now encrypted, so it's critical your network security decrypts traffic and orchestrates it to security and data compliance inspection engines. Protection from an emerging class of threats targeting your user's web browsers directly is also a critical requirement.
- **Give employees protected access to potentially risky websites. Safely access URLs embedded in emails and prevent corporate access credentials from being entered into phishing sites.**
  - Use web isolation to keep threats targeting your user's web browsers and phishing attacks away from employee devices. Web isolation executes web sessions away from endpoints, sending only safe rendering information to users' browsers thereby preventing any website delivered zero-day malware from reaching your devices.

CHAPTER 2

Build Your Defense Around an Advanced, Cloud-delivered Secure Web Gateway

- **Automatically apply your data privacy and protection policies to all web traffic, encrypted or not, and use dashboards and online reports to monitor activity.**
  - Send decrypted SSL/TLS traffic to any Data Loss Prevention (DLP) system for accurate and fast analysis. Support regulatory compliance and protect data.
- **Accurately identify the cloud apps in use, evaluate their risks, and control access to them by user, group, location, and more.**
  - Secure cloud apps, and protect data that interacts with public clouds, via cloud access security broker (CASB) controls. Gain visibility into all cloud applications used by employees, "known" clouds like Office 365 as well as "Shadow IT" clouds (provisioned by employees themselves) to ensure they comply with company cloud usage policies.
- **Integrate your cloud SWG with on-premises and mobile endpoint protection.**
  - Get complete multilayered network-to-endpoint protection and simplified mobile device app management by integrating network security with endpoint-installed security. Create a multitiered defense protecting all enterprise endpoints including mobile and remote users connecting directly to the internet.
- **Connect remote/branch office employees to the network while taking advantage of SD-WAN performance and flexibility.**
  - Easily secure remote office and mobile employees with optional SD-WAN (and similar) devices that route remote traffic to cloud security. Get started as easily as changing the configuration on your firewall or proxy, or by making a lightweight adjustment on users' devices.

CHAPTER 3

Get High Security and Performance Without High Cost

Use Network Security as a Service delivered in the cloud to gain all of the capabilities you need to protect your employees.

Consistent policies will be enforced for users wherever they are located on whatever device they are using. Best of all, since its a full network security stack that is cloud delivered, comprehensive security is available at cloud-speed and simplicity. Everything you need is integrated into one cost-effective service, and you can scale your deployment over time as needed by simply adding additional subscriptions for new users.

Direct-to-net efficiency

Cloud-delivered security can deliver great performance for your offices and mobile users, since your employees connect to the security service on their way to the web location or cloud app they are trying to get to – it's called "direct to net" security. Also look for services that have integrated SD-WAN offerings that make it simple to connect your offices to the cloud.

Efficient SSL/TLS-encrypted scanning

Don't let critical SSL/TLS traffic inspection create unwelcome latency and devour computing resources. Using an ill-suited device, such as a next-generation firewall, can severely degrade performance.

Single-agent network security access

More employees are connecting to the network via a growing collection of remote and mobile devices. Why add an additional agent to allow each to connect to a cloud-delivered network service? A single lightweight agent that provides comprehensive endpoint security and additionally re-directs your web traffic to your network security stack in the cloud should do the trick.

CHAPTER 4

Gain Visibility, Minimize Risk, Maintain Compliance for Apps like Office 365

Use CASB controls to accurately identify the cloud apps being used, evaluate their risks, and control access to them by user, group, location, and more.

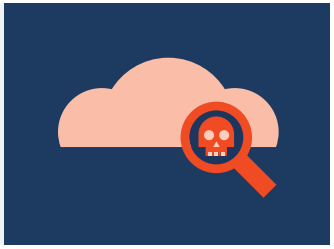
Complying with regulations requires visibility into, and command of, sensitive data—wherever it resides. That includes data in documents shared in cloud applications, even in apps adopted by employees without IT approval (so-called Shadow IT). CASB capabilities protects data that interacts with public cloud applications like Office 365.

Accurately identify applications in use

Gain deep visibility into user activity across a broad range of cloud apps and services, and enforce granular content and context-based policies. Continuously monitor cloud app usage and detect when sensitive data is being shared. Ensure employees comply with cloud usage policies.

Evaluate cloud app risks

Examine dozens of attributes for every cloud your employees are using. Identify risky activity, malicious behavior, and malware threats—and block them in real time to protect information.



Control cloud app access

Set access and control policies by user, group, location, and more based on cloud attribute data. Identify and classify critical compliance-related data and monitor how that data is being uploaded, downloaded, or shared in cloud apps.

CHAPTER 5

Unify Security Policy Management for Simplicity and Consistency

Quickly define and implement policies across on-premises and cloud environments as you adapt to fast-changing regulatory requirements and corporate mandates.

Face it, changing your security infrastructure can become operationally complex. If you don't plan ahead you may end up with cloud and on-premises platforms that require different policies and you'll be stuck maintaining two separate systems. Make your life simpler by selecting a solution that allows you to deploy similar capabilities on-premises and in the cloud with the ability to manage both with a single set of policies. If you are moving to 100% cloud, look for a solution that will let you migrate your existing security policies to your cloud network security service with the push of a button.

Simplify the transition to cloud-based security

Designate the on-premises policies you want to automatically migrate to your new cloud-delivered security.

Create and manage consistent policies

Create new policies by defining them once and pushing them to all your secure gateways, gaining consistent enforcement in hybrid on-premises and cloud security environments.

Maximize your existing investment

Take advantage of your in-place security systems where you can. Leverage your investment in DLP, but now extend it to the cloud. Maintain an on-premises SWG in your main data center(s) if that makes sense, but move your branches and mobile users to the cloud. And manage any environment—from private to public, physical, virtual, or cloud—or any mix in-between, from a single administrative console.

CHAPTER 6

Bottom Line: No Perimeter? No Worries. Cloud-Delivered Network Has You Covered

Symantec's cloud-delivered Web Security Service protects central locations, branch offices, remote and roaming users, and company data wherever they reside, using robust enterprise-class security capabilities delivered in a high-performance global cloud service.

Unequaled network security capabilities

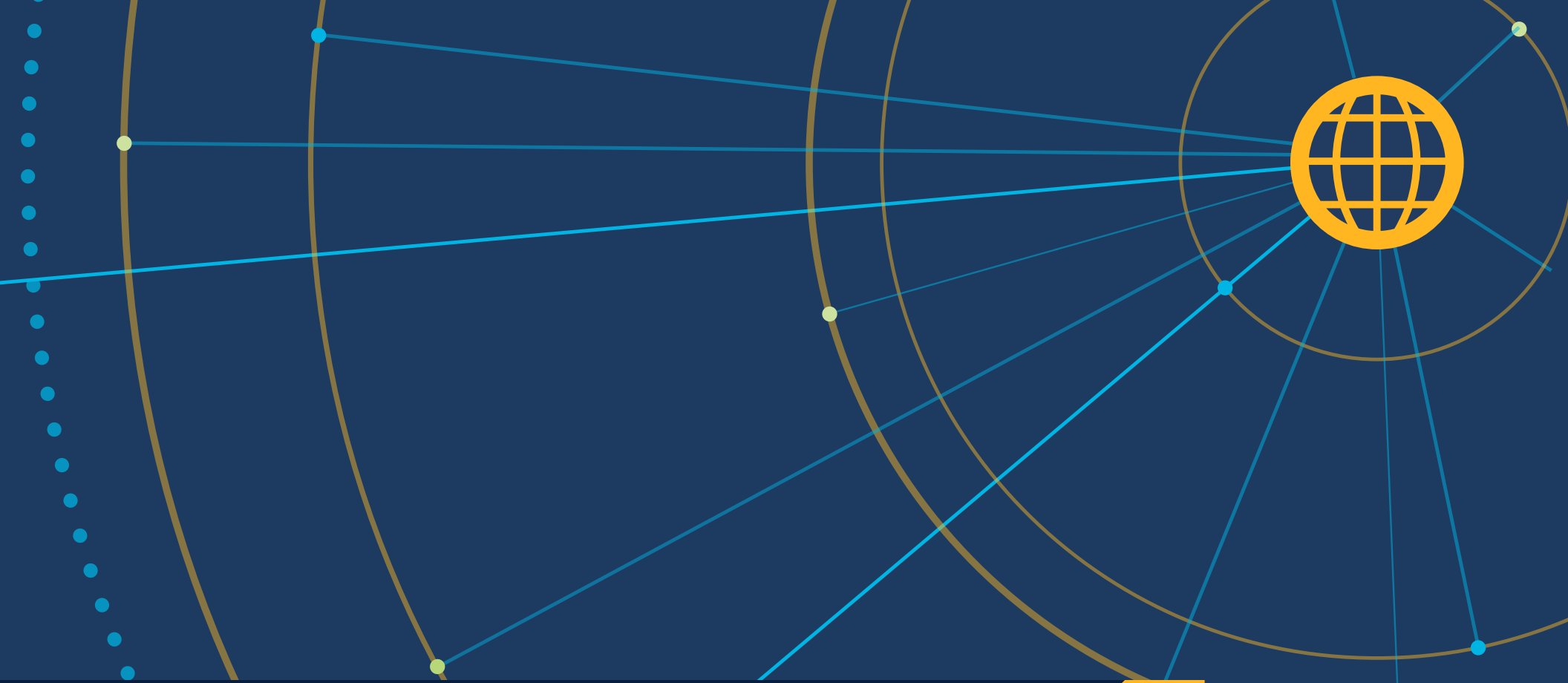
The cloud-delivered Web Security Service runs on the same advanced proxy technology as Symantec ProxySG—a Leader in Gartner's Secure Web Gateway Magic Quadrant for the last 11 years. It's the foundation for a full stack of network security: an advanced Secure Web Gateway at the core plus malware analysis, sandboxing, web isolation, cloud application controls (known as CASB), Data Loss Prevention, integrated SD-WAN and more—all powered by unique threat intelligence that determines the risk of every website your employees try to visit.

Global cloud network: Proven performance

We offer "five 9s" (99.999 percent) uptime SLAs thanks to our distributed and resilient global cloud datacenter infrastructure. We optimize performance with, for example, network peering connections with Microsoft, Amazon, Google, and others, and TCP window optimization that speeds large files as they move between cloud storage apps.

Integrated protection that simplifies your operations

We realize that you also need to deploy security solutions on your endpoint. This is why we integrated our award-winning Symantec Endpoint Protection (SEP) with the Web Security Service. So when you use the products together, you have one less agent to install and manage on your endpoints. SEP can be configured to route web traffic to the Web Security Service so network security policies can be enforced. This delivers a unique endpoint and network security defense-in-depth service from Symantec, designed to keep your users safe in a world without perimeters.



For more information, please visit
symantec.com/products/web-and-cloud-security

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec™

19C210137_SB_VANISHING_PERIMETER_EN