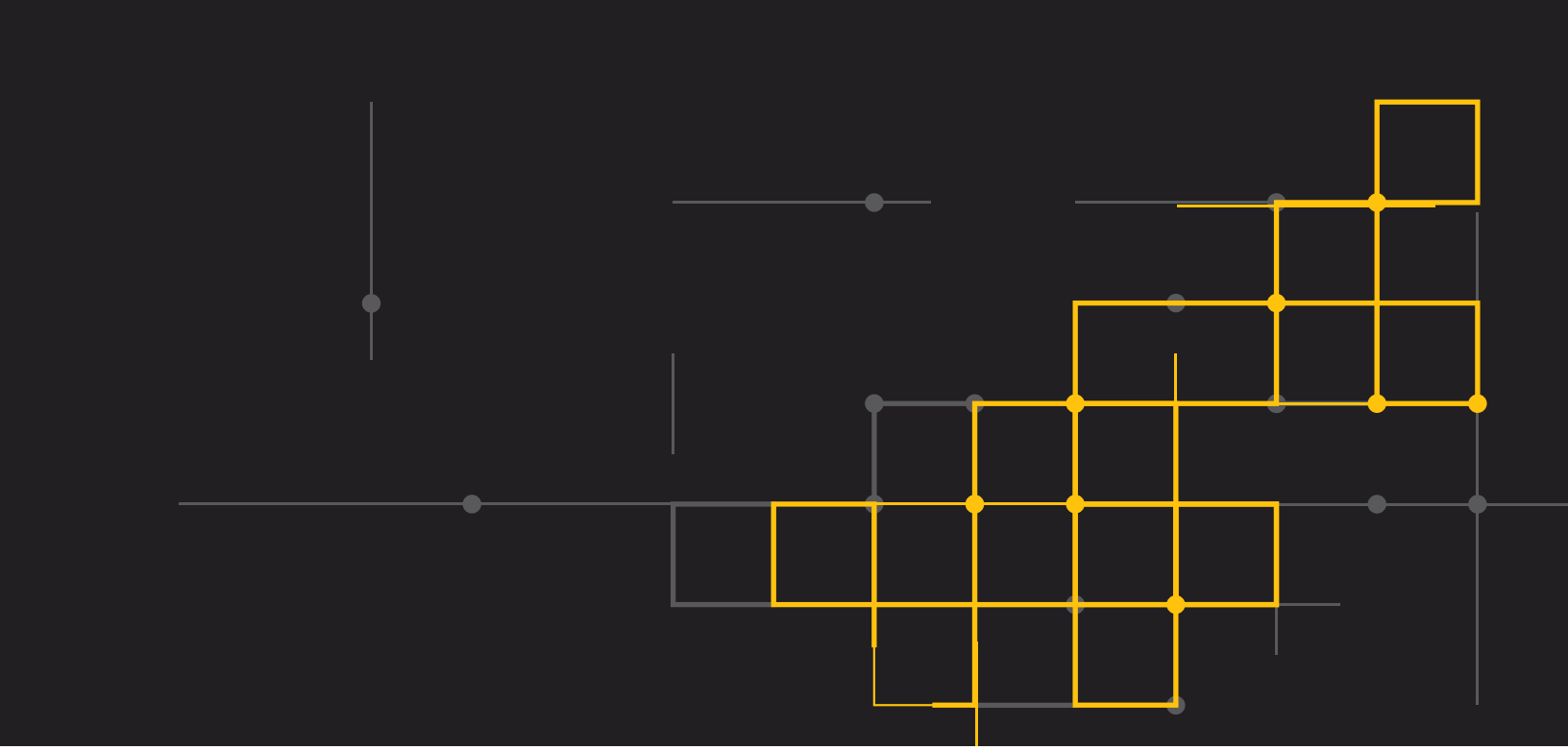


Extending Threat Protection and Control to Mobile Workers

Cloud-Based Security Services Protect Users In Any Location Across Any Network

It's a phenomenon and a fact: employees are always on today. They connect to the network whenever they want, from wherever they happen to be, with laptops, smartphones and tablets. Securing smartphones and tablets is a challenge, but laptop computers, still the most vulnerable of all endpoint devices, present the biggest mobile threat to corporate security. Laptops today are far more numerous than other mobile devices, and are more tightly integrated into the enterprise infrastructure. They are prime targets for malware attacks.

Symantec

Protecting laptops from these threats in branch offices, in home offices, and on the road is increasingly critical – and challenging. As mobile users leave the corporate network, they leave corporate policies and security behind. They're exposed to web-based threats that lurk in search engines, social networking sites and email.

In this environment, businesses need to extend consistent protection, policies and reporting to mobile workers in any location across any network. Businesses are now using cloud-based security services for that purpose.

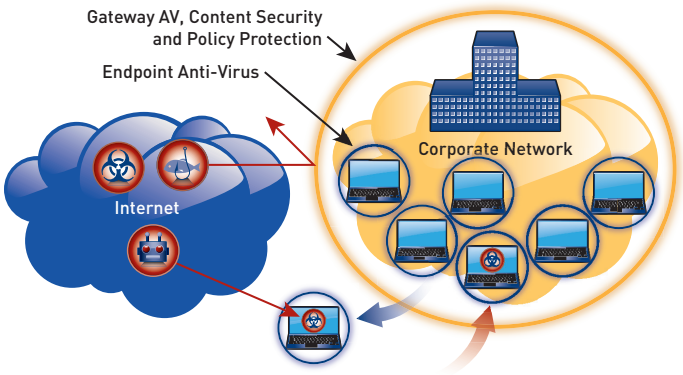
Cloud-based security allows businesses to create a seamless secure experience for all mobile employees, whether they're connecting from the corporate network, from captive hotel portals, or from Wi-Fi logon pages. They receive all the benefits of up-to-date protection without sacrificing portability, flexibility or agility. Businesses can be assured that when mobile laptops access the corporate network they're not infected with malware.

Why Laptops are the Weakest Security Link

According to Forrester Research, more than 60 percent of businesses issue laptops to sales reps, executives, heavy travelers and IT staff as standard practice. Laptops will continue to be the dominant PC platform for the foreseeable future; they're forecasted to account for more than 43 percent of PC sales through 2015, declining only slightly despite the growth in tablets. At the same time, the population of mobile workers is expected to reach 1.19 billion in 2013, accounting for 34.9 percent of the workforce according to IDC.

Despite the convenience of smartphones and tablets, laptops are the dominant platform for mobile workers because they're exceedingly efficient, particularly for long sessions or complex tasks. The problem is that although the laptop is a critical business tool, it's also used for personal activities. Workers visit vulnerable web sites, access social networks, and expose personal data.

Traditional Enterprise Boundaries Leave Mobile Users Vulnerable



Step 1 – Elevated Threat Risk

Desktop AV only - no content security and no policy enforcement. Mobile users risk infection when Enterprise policies are unable to follow.

In fact, many users surf the web much more aggressively when they're off the corporate network, exposing their laptops to greater risk of infection. Their ubiquity, and the ways mobile workers use them, make these endpoints – and, in turn, corporate networks – very vulnerable to a dynamic threat landscape that saw a 240 percent increase in malicious sites in 2011 alone. According to the Symantec Systems 2012 Web Security Report, the average business now faces more than 5,000 security threats every month, and nearly half of these threats originate in the most popular places on the internet – search engines and social networks.

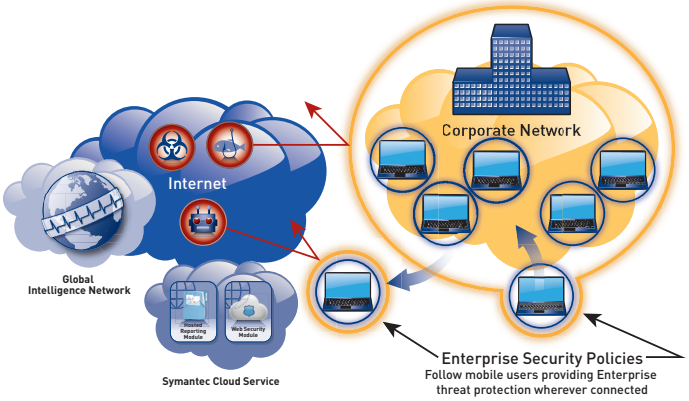
Criminals may also target laptops because they know workers are far more likely to use them (rather than smartphones or tablets) to store and access sensitive corporate data.

Cloud-Based Security is the Answer

Cloud-based security lets IT and security professionals extend protection and control seamlessly to mobile workers, particularly when the solution is tightly integrated with on-premise appliances to deliver unified policy management and monitoring. Securing the laptops of mobile workers through a cloud-based service allows IT to achieve the following goals:

- **Reduced Threats**: Cloud-based security services seamlessly extend threat and malware protection to mobile workers who are left unprotected when they're off the corporate network. By integrating multiple defenses into a single service offering, a cloud-based security solution can deliver more effective protection than traditional desktop solutions. For businesses, the extension of this protection ensures that mobile workers don't introduce infected endpoints into the corporate network, where they can steal sensitive data.
- **Reduced Complexity**: With a cloud-based security solution, the IT organization can quickly and easily provision new laptops or even remote offices from corporate headquarters. Policy management can be centralized, eliminating the need to create additional policies to cover mobile use. Reporting can also be centralized to provide a single view of user behavior on and off the corporate network.
- **Reduced Cost**: Cloud-based security services represent an operational expense rather than a capital expense, giving businesses budget flexibility. The consume-as-you-go model allows businesses to purchase just enough licenses to cover existing users – then scale as needed. And there are more savings at the branch office: with centralized management and deployment, IT no longer needs to staff branch offices or be on-site to provision new services.
- **Better User Experience**: In addition to reducing bandwidth pressure on the corporate network, a cloud-based security service can help improve laptop performance. Clean internet is delivered to the laptop; unwanted content is blocked. This reduces processing overhead for content screening and inspection and makes more power available for users' applications. With a cloud-based service, users simply log on and access their content anywhere, anytime – safely.

Adding Cloud-Based Security to Extend Policies



What a True Enterprise-Class Cloud Solution Requires

When it comes to delivering a cloud-based security service, some solutions are more robust and powerful than others. Knowing the difference is important for successful implementation. To deploy maximum protection and control without sacrificing the user experience or compromising the security of the corporate network, businesses need enterprise-class features and performance.

When evaluating any cloud-based security solution, therefore, IT organizations should make sure that it includes these essential features:

- A Robust Global Network: This is of great importance in any evaluation of vendor solutions. It's not enough to look at 'dots on a map.' To deliver the reliability that users expect, the solution must guarantee 99.999 percent availability through an infrastructure that utilizes only enterprise-grade data centers. This standard requires that the network be fully meshed in SSAE 16 or ISO 27001-approved data centers with both local and global redundancy for disaster recovery.
- Tight Integration with Existing Solutions: Tight integration enables IT organizations to easily deploy a cloud-based security service into an existing security and network infrastructure without disrupting services or the user experience. To do that, the solution must include two key elements:
  - » **Robust Connection Methods**: All cloud-based security services require web traffic to be redirected to the cloud. This redirection typically occurs at the corporate internet gateway where appliance-based security solutions, such as firewalls or proxy devices, are deployed. To guarantee encryption and resiliency, a universal capability like IPsec VPN is required. For mobile workers, redirection should take place at the device level. Mobile workers often connect over public connections, so redirection must also be secure. A tamper-resistant software client that communicates over SSL and encrypts traffic regardless of connection type is the most secure option for mobile workers and the laptops they use.
  - » **Universal Directory Support**: Ensuring that directory authentication is seamless for both employees and administrators is especially important with mobile workers. Support for Active Directory and Security Assertion Markup Language (SAML) allows the IT organization to deliver a single sign-on (SSO) experience for its users.

- Consistent Threat Protection: Businesses can't afford to settle for good-enough threat protection against today's dynamic threat landscape. A cloud-based security service must be able to deliver the same protection seamlessly to all employees, regardless of their location or the network they're using. For enterprise-class protection, that means a combination of defenses, including web filtering, anti-virus scanning and real-time analysis of all web content. And the defense must be able to analyze encrypted traffic, because more and more businesses are adopting cloud-based applications. The HTTPS connections used by these applications can circumvent traditional web security solutions.
- Flexible Policy Management and Reporting: Addressing the security needs of mobile workers as they move from the corporate office to remote locations requires flexible controls that allow IT to set situational policies. These policies should be managed centrally and enforced seamlessly as users move across networks, devices and locations. Supporting and managing these policy capabilities demands real-time reporting insight into all web behavior. The ability to monitor and report on threat activity is increasingly important, particularly for advanced persistent threats and botnet activity on the corporate network. Mobile workers using laptops have the same performance and policy requirements as desktop users – but are exposed to greater risk. With the right cloud-based security service, a business can extend protection and control from the corporate office to any location and give all users the same secure experience.

Choosing the Right Cloud-Based Security Solution

The Symantec Cloud Service is built on technology used by 85 percent of the FORTUNE Global 500. It delivers the enterprise-class performance, security and reliability that businesses need to extend security perimeters to mobile workers. Symantec has architected its Cloud Service to ensure instant operability with existing network infrastructures.

Here's what it delivers:

- **Enterprise-Class Reliability and Performance**: The Symantec Cloud Service is built entirely on enterprise-class Tier 1 data centers that guarantee five-nines uptime. The multi-tenant architecture is purpose-built with a fully meshed network of global data centers that delivers consistent, high-availability access to users at any location. The advanced security and performance technologies used in Blue Coat's ProxySG and ProxyAV appliances are the foundation of the Cloud Service. They deliver a robust and proven architecture that scales to the capacity requirements of the most demanding enterprises.
- **Secure Client**: The Symantec mobile client enables a secure, authenticated implementation through the cloud for mobile workers on laptops. It is tamper-resistant and can only be uninstalled by administrators, which is extremely important for laptops and mobile devices. Additionally, the Symantec client is location-aware, which ensures that mobile workers' traffic will be forwarded to the nearest data center. The location-aware client can uniquely sense when it's behind a ProxySG appliance on the corporate network, and will conform to the policies enforced by the appliance. When the user leaves the corporate network, the Symantec Cloud Service becomes the primary source of protection and policy enforcement.
- **Secure Connectivity**: The Symantec Cloud Service offers the most robust and secure connection options available to enterprises. It is the first security service to offer IPsec VPN connection to the cloud. With an IPsec implementation, organizations can leverage existing equipment to connect to the Cloud Service and avoid filtering on firewalls, which slows down performance. Since the Cloud Service uses open standards to ensure interoperability with gateway devices and clients' existing capabilities, it works well with laptops and mobile devices.
- **Global Threat Protection**: The Symantec Global Intelligence Network delivers threat intelligence across Blue Coat ProxySG appliances and the Symantec Cloud Service, ensuring consistent protection for all users, regardless of location. The Global Intelligence Network utilizes advanced analysis and ratings techniques to protect more than 75 million users worldwide from 3.3 million threats daily, including calls to command-and-control servers from infected endpoints. Symantec Security Labs continually assesses the threat landscape and adds new defenses to the Global Intelligence Network. For example: Symantec recently added a Negative Day Defense that tracks the malware networks (malnets) that are responsible for nearly two-thirds of all attacks – and blocks those attacks before they launch.
- **Granular Control**: The Symantec Cloud Service provides granular Web and mobile application controls that allow IT organizations to manage the applications on their network and the way users interact with them. These granular controls help businesses manage the risks and bandwidth impact of web and mobile applications. For example: an IT organization could create a policy that allows read-only access to Facebook, mitigating the threats of data loss, reduced productivity and malware attacks.
- **Actionable Reporting**: These controls are strongly supported by unified real-time reporting capabilities that provide a single view of all web activities across the organization. This intelligence enables 'actionable reporting' – triggering a policy action based on a reporting threshold. Actionable reporting also works in real time with the Global Intelligence Network, immediately identifying infected laptops that have been blocked from calling home to command-and-control servers. IT can then quickly remedy the problem.

Symantec Cloud Service: The Clear Choice for Security in the Cloud

Mobile workers create challenges for security-minded businesses. Smartphones and tablets occupy mindshare, but the widespread deployment of laptop computers creates the greatest security challenge to IT.

It's clear that neither the challenges nor the laptops are going away anytime soon. Finding a solution is critical. Cloud-based security services provide a seamless way to address the security, policy and performance challenges. The right solution can help enable mobile workers without compromising the security of the corporate network. Symantec Cloud Service is the comprehensive, field-proven answer.

Learn how you can benefit from enterprise-class security in the cloud.

About Symantec

Symantec Corporation World Headquarters

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

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, 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 suite of products for protection at home and across all of 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.

SYMC_wp_Threat_Protection_Mobile_Worker_EN_v2a