PANDA CLOUDINTERNETPROTECTION

Simply... Evolution

Overview

Cloud Internet Protection's in-the-cloud security services enable organizations to enforce business policy and mitigate risk, while providing every user with a rich Internet experience from any place and on any device. Cloud Internet Protection delivers twice the functionality at half the cost of current solutions through a multi-tenant, globally deployed infrastructure.

Emerging Web 2.0 Challenges

Most of today's security products—such as firewalls, VPN, IDS/IPS—protect corporate networks and servers from threats coming from the Internet. Newer threats such as bots, phishing and malicious active content attack users as they use the Internet and subsequently infect corporate networks. Other than deploying caching and URL filtering products, corporations have done very little to inspect web traffic and protect their users.

In addition, Web 2.0 applications such as social and business networking create both opportunities and challenges for today's organizations. They help create communities of interest for marketing, but can also create risks when users inadvertently download malicious content, or liability when employees publish inappropriate or confidential content on blogs and social networks. Road warriors and smartphone users further exacerbate this problem—their access to the Internet often bypasses all security controls.

Current solutions require the acquisition, deployment, and management of multiple point products at each Internet gateway—an expensive proposition.

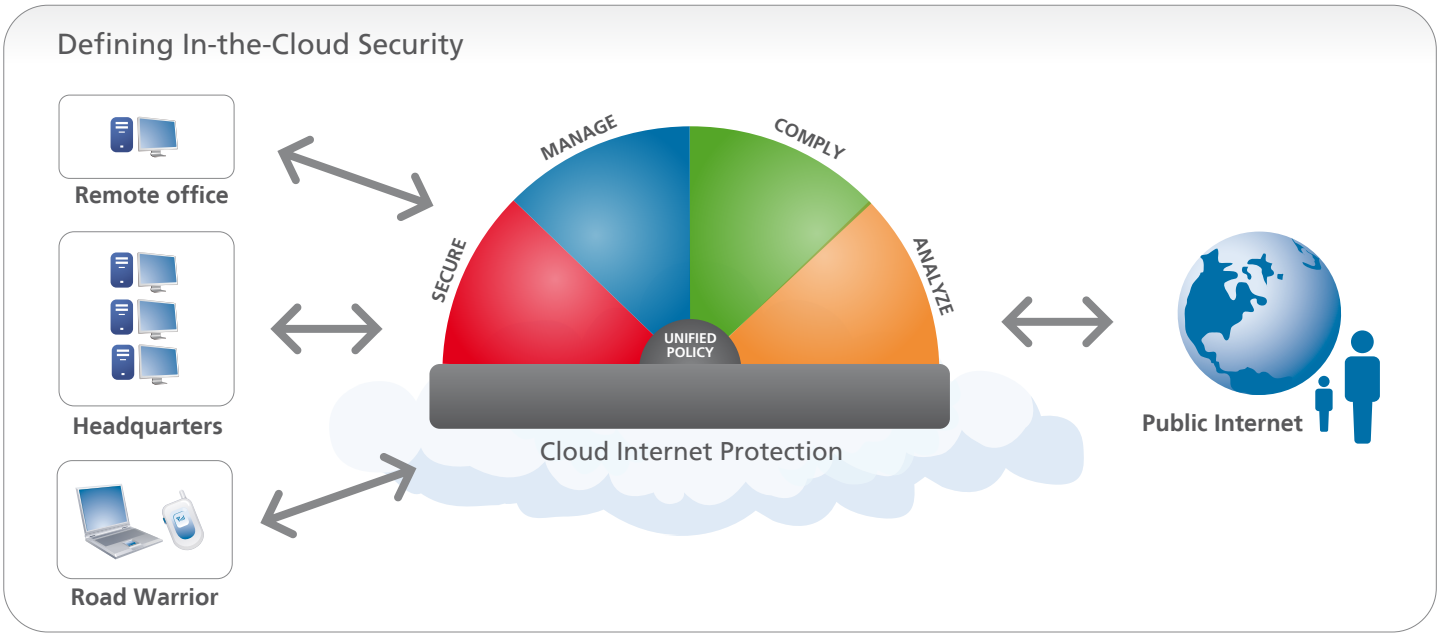
Cloud Internet Protection's in the-cloud service or Software-as-a-Service (SaaS) for the Internet-bound traffic is the best way to provide secure and managed access to users.

Defining In-the-Cloud Security

SaaS has been made popular by companies such as Salesforce.com, NetSuite, and Google. A major reason these companies have been successful managing tremendous growth and being cost-effective is that they developed platforms and applications specifically for SaaS.

Cloud Internet Protection has done the same for in-the-cloud web security. The Cloud Internet Protection Cloud is purpose-built to meet the latency, multi-tenant, global footprint, and reporting requirements that in-the-cloud security solutions demand. Traditional web proxies and reporting solutions designed for enterprise deployments cannot be repurposed to meet these requirements. The key driver of SaaS offerings are savings associated with not having to deploy or manage systems and software in an organizations network or end points. This is particularly challenging with web security since the web traffic has to be redirected to the service from both LANs and mobile devices (laptops, smart phones), users always need to be authenticated, and directory integration is necessary.

Cloud Internet Protection is in the unique position of being the only service that requires no on-premise hardware or client software to address these challenges. Cloud Internet Protection can redirect traffic and authenticate end users to properly report and apply user and group level policy for any device from any location.



Comprehensive, Integrated, and Best-of-Breed

Cloud Internet Protection provides an integrated, best-of-breed, and comprehensive functionality in four areas:

Secure
In addition to signature-based anti-virus and anti-spyware, Cloud Internet Protection offers protection against advanced threats such as bots, malicious content, phishing and peer-to-peer networks. PCloud Internet Protection's architecture provides inspection at forty times the speed of most competitive products, ensuring full protection without introducing the latency that afflicts current solutions.

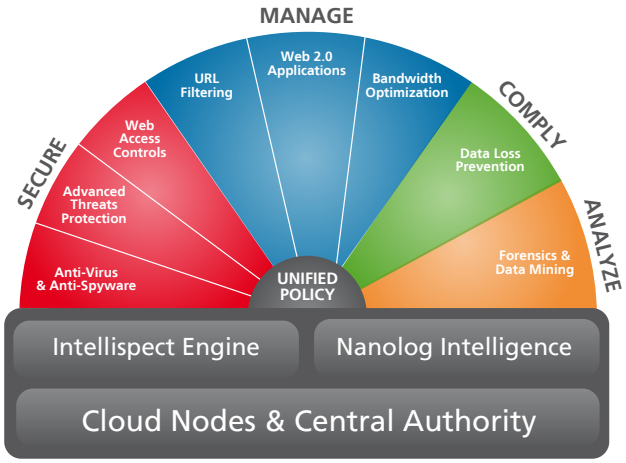
Manage
In addition to offering URL filtering, Cloud Internet Protection empowers organizations to provide managed access to Web 2.0 applications—such as social networking, blogging, streaming, Webmail, and IM. Cloud Internet Protection uses proprietary, patent-pending, dynamic content classification (DCCTM) to identify applications and control them.

Comply
Cloud Internet Protection detects and protects against data leakage through the HTTP/HTTPS channel (including Webmail, IM, file uploads) to enable regulatory compliance and secure company-sensitive information.

Analyze
Web logs from outbound Internet traffic require massive amounts of storage to retain. Due to a lack of good tools, organizations cannot use these logs to have visibility of traffic or perform investigations. Using patent-pending NanoLog technology, Cloud Internet Protection reduces storage requirements by a factor of fifty, provides rapid log analysis and offers forensics capabilities.

Revolutionary Technology and Performance

Like Salesforce.com's platform, Cloud Internet Protection's platform was purpose-built to support a multi-tenant SaaS architecture. The policy and log management is centralized, but the execution of policy happens at Cloud Internet Protection processing gateways that are deployed around the globe. Each gateway can handle 250,000 transactions per second, which is 50-100 times the throughput of other proxy servers. Its single-scan, multi-action (SSMATM) technology ensures accurate application identification without introducing latency.



Cloud Internet Protection service requires no upfront capital investment to purchase, deploy, or manage appliances or software. With Cloud Internet Protection infrastructure, IT administrators do not spend time managing and updating patches and signatures on multiple products; they can focus on policy enforcement. By providing integrated, best-of-breed and comprehensive functionality, Cloud Internet Protection delivers twice the functionality at half the price of current solutions.

Panda Security certifications and awards