SOLUTION BRIEF

Top 10: Connect to the Cloud for Security

Discover, assess, and remediate cloud threats

Both the way we work and the security landscape are in a state of constant change. Employees work from anywhere, and the traditional network perimeter is removed when a laptop leaves the building. A cloud edge that provides ubiquitous security, regardless of location, is emerging to replace it. Can security at the cloud edge solve your security problems?

Problem 1: Employee access to the web and cloud services is no longer confined to the network perimeter, creating a gap in visibility and protection when users roam off network.

With a web gateway delivered as a cloud service, users can roam off network and use their managed endpoints at locations such as coffee shops or airports and always maintain the same web security policy.

Problem 2: Threats such as malware are often missed when an employee is off network because security is reduced or different.

McAfee uses the same technology in the cloud as with its on-premises web gateways, providing equal levels of security, including protection against zero-day malware. This lowers costs and provides greater flexibility for IT operations by reducing the volume of incidents stemming from off-network users.

Problem 3: Detecting the most sophisticated malware is expensive and means purchasing a dedicated network sandbox.

Using a cloud-based sandbox is dramatically less expensive than an appliance, works whether the user is on or off network, and, with McAfee, is managed enforcing the same policies as the cloud-delivered web gateway.

Problem 4: Cloud applications are being used by nearly every department, and we don't know what's out there or if they're introducing risk to our security posture.

All cloud application traffic, even over secure sockets layer (SSL), can be investigated through a free cloud visibility service provided to McAfee® Web and Data Protection customers. This service uncovers Shadow IT and allows you to explore the risk associated to cloud applications along with the classification of data sent outside the organization.

Problem 5: Cloud access security broker (CASB) technology requires manual steps to make use of log data for application visibility.

This seems like a waste of time for our team, who is already stretched thin. By using a cloud-delivered web gateway on the same platform as cloud visibility, log import occurs natively, meaning there are no additional steps needed, avoiding the hassle of "store and forward" methods. It just works.

Problem 6: The use of cloud applications happens everywhere, but we can only control access to them when the user is in the office.

With a cloud-delivered web gateway, functionality such as the ability to upload documents to an application can be controlled wherever the endpoint travels since it is always connected to the cloud enforcement point.

Problem 7: There are multiple management consoles that we switch between to manage our security functions.

This causes us to spend a lot of time mastering each interface and remembering workflows that are never the same. All cloud services from McAfee, currently including a cloud-delivered web gateway, sandbox, and cloud visibility service, all share a common policy and management console to keep your workflows in one place.

Problem 8: Parts of our security infrastructure are very expensive to buy and maintain, such as our web proxy and sandbox appliances.

With McAfee, you can deploy a web gateway and sandbox as 100% cloud services, meaning no more appliances and a much lower TCO.

Problem 9: We pay for multiprotocol label switching (MPLS) circuits and (virtual private network) VPN tunnels just to scan our web traffic from remote sites at our data center.

This seems like wasteful spending. With a cloud-delivered web gateway, you can immediately reduce the cost of MPLS circuits and VPN tunnels by sending all public-facing web traffic through the cloud for processing, while maintaining limited MPLS or VPN tunnels for internal traffic only.

Problem 10: It is time-consuming to roll out new software to every endpoint. Why do I have to do that for endpoint and web security?

Web gateway routing and authentication functionality can be deployed together with McAfee Endpoint Security. Your endpoints are ready to turn on the connection to the cloud for web security, sandboxing, and cloud visibility immediately.

Check it out for yourself. **Sign up for free trials of all our cloud services here.** For more information on cloud services and endpoint technology mentioned here, visit the following pages:

- McAfee Web Gateway Cloud Service
- McAfee Cloud Threat Detection
- McAfee Cloud Visibility—Community Edition
- McAfee Endpoint Security

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

2746_0617
JUNE 2017