



7 Requirements for Hybrid Web Delivery

Getting the best of both on-premises and SaaS

Traditionally, IT risk management has balanced security investment and the impact of the threat, allowing each business to make its own decision on the “right” security investment. However, when it comes to secure use of the web, the limitations of web security vendors have forced IT teams to make a hard choice between deployment platforms, security controls, and cost savings. The McAfee® Hybrid Service Delivery Architecture provides a blueprint for adopting any or all service delivery platforms—integrated appliances, virtual appliances, or hosted services—without scrimping on deployment flexibility, security, or savings.

Introduction

In web security, IT has had a choice of Column A or Column B: appliance-based or hosted services. The decision tree has been either/or, black/white, for two reasons: security concerns and cost models. Generally, high security concerns cause companies to stick with appliances. Some use virtualization to eke out higher utilization of compute resources. Shrinking budgets cause others to choose SaaS, accepting lower control over security and data privacy in exchange for lower upfront and operational costs.

Yet most businesses are neither black nor white, but some shade of gray: a mix of security sensitivity and cost sensitivity.

The McAfee Hybrid Delivery Architecture defines critical requirements that allow IT to apply traditional risk management to web security. This technical and business architecture starts with requirement zero: a firm foundation of strong security delivered in on-premises physical or virtual appliances or through the cloud as Security-as-a-Service. This secure foundation means that no matter which deployment path you pick, your users will be protected against web threats.

Once requirement zero, the baseline security concern, has been hurdled, other requirements help IT teams:

- Understand and overcome cost limitations
- Provide for best-of-breed service delivery
- Ensure service portability

This “hybrid” model lets IT staff efficiently protect their organizations against today’s emerging and morphing threats, while taking advantage of all available service delivery options: hardware and software integrated as appliances, virtualized appliances, and hosted service delivery platforms. Instead of concerning themselves with deployment trade-offs, IT can tune implementation according to specific business requirements, user community, and risk posture and get the right mix of security AND cost savings.

The Tradeoffs: Integrated Appliances, Virtual Appliances, and SaaS

Today, appliances lead the way in web security, with SaaS growing, and virtual appliances beginning to emerge. Each of these three models is attractive to IT security staff for valid and sometimes conflicting reasons. Let's examine the relative strengths and weaknesses of each of these models.

Model	Key Advantages	Key Concerns
Integrated HW/SW Appliance	<ul style="list-style-type: none"> • Performance • Fine-grained, hardware-accelerated security to cover specific risks • High configurability • Pre-tested and integrated solution • One call for support • Assets, data, redundancy, and availability protected and controlled within the organization 	<ul style="list-style-type: none"> • Up-front capital expense • Potentially unpredictable cost and disruption in order to upgrade or meet peak demands
Virtual Appliance	<ul style="list-style-type: none"> • Flex capacity on demand • "Green IT" • Higher utilization of existing compute resources • Assets, data, redundancy, and availability protected and controlled within the organization 	<ul style="list-style-type: none"> • Extra layer of infrastructure to manage • More policies to configure • Two calls for support • Virtualized infrastructure introduces extra risk • Hypervisor overhead and tuning requirements
Hosted SaaS	<ul style="list-style-type: none"> • Typically lower start-up costs • Lowest administrative costs • Seamless capacity growth • Maintained 24/7/365 by security and availability experts • Convenient activation • One call for support 	<ul style="list-style-type: none"> • Latency • Least IT control over security and data privacy required for compliance

The McAfee Hybrid Delivery Architecture: Next-Generation and Flexible

From this comparison, it is apparent that no single model is a panacea. Many businesses apply protection based on the use case, SaaS for remote offices and appliance gateways (physical or virtual) for corporate headquarters. Within any given organization, there are times when a combination of models offers the best solution. Over time, an organization—or a part of an organization—may desire to move from one service-delivery model to another. However, this type of flexibility and portability cannot be bolted on; it must be designed into a solution from both business and technical perspectives.

While many vendors have announced availability of web security solutions on more than one platform, the solutions are parallel systems. With parallel environments, mixing models means paying twice. Instead, the McAfee Hybrid Delivery Architecture allows organizations to achieve security and cost savings, mixing and matching deployment models across all platforms. These requirements go beyond basic deployment of parallel systems. They support a "platform-agnostic" foundation that adapts to changing business needs, rather than forcing a business to adapt to a vendor's technology limitations.

The McAfee Hybrid Delivery Architecture rests on seven design pillars:

0. A strong foundation of best-of-breed, proactive security
1. Flexible deployment options: integrated hardware and software, virtualized, and hosted
2. Single price for multiple deployment options
3. Fully portable security services
4. Support for splitting services across delivery platforms
5. Common policy definition and administration
6. Unified reporting

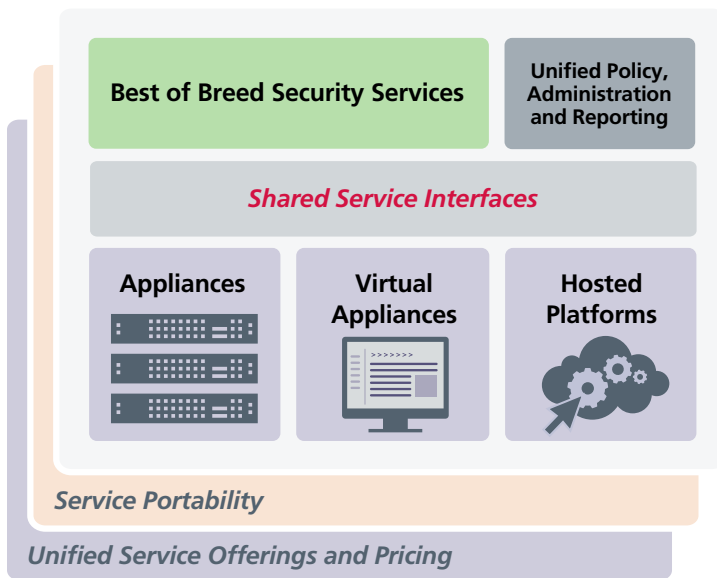


Figure 1. The McAfee Hybrid Delivery Architecture.

Requirement 0: A strong foundation of best-of-breed, proactive security

The first hurdle to adoption of SaaS is confidence that the security practices at the cloud will protect users and sensitive data the way on-premises appliances do, so that wherever users are accessing the web they are covered with similar protection. We know security, like other technology programs, blends people, processes, and technology. Not all SaaS services secure equally. Security standards for each of these elements will vary between providers. With SaaS, you also have to factor in trust, embodied in your service level agreement and informed by the vendor's past performance. ISO certification is one aspect to look into when it comes to managing datacenter controls, such as the ISO/IEC 27001:2005 certification.

Certain core capabilities are baseline requirements for web security in this age of drive-by downloads and malicious content. The below list looks at the most important capabilities that are typically available in appliances and represent the ones IT users should require in any web security offering:

- *Anti-malware signatures*—This is a minimum protection, some vendors have their own researchers, some import signatures from a third party which could be an indication of lower quality, as well as a lag in protection, and some provide both their own in addition to third party options
- *Real-time anti-malware scanning and analysis*—In addition to using signatures, some vendors will perform dynamic assessment of malware on websites and in content files; when heuristics are used to evaluate intent, experience and research investment affect the heuristics' accuracy of detection
- *Reputation*—Some vendors maintain a reputation database of websites, IP addresses, and registrants and use these reputations to block communications with risky sites; dynamic URLs and the ever-changing threat landscape require perpetual vigilance and advanced technologies to not only keep up with changing threats but predict and protect against future threats
- *URL filtering*—Categories such as adult content, gaming sites, and social networking sites may need to be blocked to support corporate policies

McAfee delivers all of these capabilities in a single suite: McAfee Web Protection. Powered by McAfee Global Threat Intelligence from McAfee Labs and the proactive McAfee Gateway Anti-malware Engine, McAfee Web Protection includes all the features of the McAfee Web Gateway on-premises solution and McAfee SaaS Web Protection in a single priced offering. You can deploy it on premises, in the cloud, or both, for maximum flexibility and high availability.

Requirement 1: Flexible deployment options: integrated hardware and software, virtualized, and hosted

As discussed above, each service-delivery model has unique benefits, and one size may not fit everyone. There may be times when each is right for only a part of an organization. A complete web security solution makes all three of these platforms available. In addition, each platform puts unique technical and business requirements on the solution provider.

- A wide range of integrated appliances must be available to meet varying capacity and performance needs
- Virtual appliances should come with documentation and guidance on the resources needed for adequate performance when running on a hypervisor under load
- Hosted services must be more than simply a pool of hosted appliances, but be built as a true multi-tenant secure architecture

Where some vendors steer companies to the solution their technology implements best, McAfee offers IT true freedom. McAfee already provides well-respected, proven web security applications on all three of these service-delivery platforms.

Requirement 2: Single price for multiple deployment options

There is no doubt that IT is moving to a service delivery model. To remove any constraints around service quality and features when making deployment choices, the McAfee Hybrid Delivery Architecture recommends all delivery platforms have a single price. With pricing independent of deployment decisions, IT can deliver the right services based on requirements, strengths, and weaknesses—not cost.

For the ultimate deployment flexibility and future proofing of investments, McAfee offers all features of the McAfee Web Gateway and McAfee SaaS Web Protection solution in a single suite: McAfee Web Protection. With comparable security and a single price, you can deploy on premises, in the cloud, or both for maximum deployment flexibility and high availability.

Requirement 3: Fully Portable Security Services

Service portability is an especially important business companion of price consistency. There must be no loss of protection, compliance, or continuity when users' service provisioning moves from one platform to another. Without both portability and consistent pricing, any system will fail to deliver the promised benefits. For example, make sure you understand what technology is being used with each deployment option. Are both on-premises and SaaS options using the same anti-virus engine? Are they both providing the same granular categories for web filtering and the same anti-malware engine, or are they using completely different systems that will result in varying efficacy?

McAfee delivers service portability by abstracting the delivery platform from the security services. The same anti-virus and anti-malware secure users of both McAfee SaaS Web Protection and McAfee Web Gateway. The security services also apply the same URL categorization database. Although the underlying technologies are consistent, we optimize the technologies for the type of deployment. For instance, we allow IT to apply more fine-grained policies and controls for the appliance and leverage streamlined policies for SaaS.

Requirement 4: Support for splitting services across delivery platforms

A natural extension of the availability of multiple delivery platforms is the ability to "hybridize" services across platforms. By "hybridize," we mean custom implementations where some services might use one platform, some another. The goal is to enable organizations to use various delivery options to meet their environment and requirements. For instance, security services might be split to keep known threats away from the corporate office, or traffic that is normally filtered by an on-premises appliance might be redirected to fail over to a SaaS platform if a peak threshold (such as 90% utilization) were reached on the appliance. The ability to add capacity on the fly allows IT to ensure it meets service level agreements without jettisoning security and compliance.

McAfee supports split services in several ways. You might divide processing so that McAfee signature-based malware scanning was performed with the McAfee SaaS Web Protection platform and intent-based analysis was performed locally with McAfee Web Gateway, allowing more control, granularity, and auditing. Or, a rule on the Web Gateway, such as a utilization threshold, can push traffic to SaaS when needed for seamless service.

Requirement 5: Common Policy Definition and Administration

Whenever services are deployed across multiple systems, common policy definition and administration streamline operations. An administrator should be able to define policy and deploy it for enforcement independent of the service-delivery platforms being used. The administrative interface should abstract the service-delivery platform from the user for whom the policy is applied. The McAfee Hybrid Delivery Architecture emphasizes the importance of a unified policy definition and administration across integrated and virtual appliances and SaaS delivery platforms. Classic shared policies are URL filtering and anti-malware screening for all web traffic. As with any product and service integration, administration gets better over time.

McAfee is investing in common policy definition and administration for the McAfee Web Protection solution. Although initially these processes may require separate configuration steps, we deliver common protection levels and increasingly integrated configurations.

Requirement 6: Unified Reporting

Every business has different audiences: executives, compliance officers, forensic investigators, and IT security managers. Though they may want separate views based on business requirements, there should be a core, common reporting infrastructure. Each of these users should have the same level of reporting available across service delivery platforms, without requiring manual aggregation of reports. Specifically, reporting should collect service activity across all platforms and allow flexibility to create audience-specific reports.

McAfee aggregates data regardless of delivery platform to provide the instant information and forensic tools needed to: illuminate how organizations use the web, comply with regulations, identify trends, isolate problems, document inappropriate web activity, and tailor filtering settings to enforce web usage policies.


Case Study One: Distributed Sites

Organization A is looking at replacing their antiquated web filtering software with a modern web security solution. Ideally, they would like control, low costs, configurability, and flexibility. The company has a large datacenter at their headquarters and prefers to deploy as much of their computing infrastructure as possible on dedicated appliances and reserve VMware for testing and high availability. In addition, they have three regional headquarters with significant staff at each facility, but limited IT management capacity. Lastly, about 20 percent of their total staff works out of home offices.

The Web security team has evaluated integrated and virtual appliance models and hosted services. They discovered for themselves the difficult tradeoffs discussed earlier in this paper. Then they found that McAfee offered all three delivery models with McAfee Web Protection. This implementation allows them the control they desire, plus the ability to effectively serve and add remote users to the solution. McAfee Web Protection allows them to have the best of all three models for web security, without sacrificing service quality or flexibility.

Case Study Two: An Acquisition

Organization B uses McAfee Web Protection with McAfee Web Gateway appliances to deliver robust web security to their organization. However, they have just acquired a company, and the entire IT staff of the acquired company has been terminated. Due to the flexibility of the McAfee Web Protection deployment option, the Web security director simply signs up the acquired company to the McAfee SaaS Web Protection offering. As the acquisition matures, the company knows that it can reallocate



hybridized service features as appropriate, perhaps ending up with desktops configured to go directly to the SaaS, perhaps ending up with a fully appliance-based deployment. Most importantly, IT is able to deploy and enforce policy and provide integrated reporting to compliance and management teams from day one.

The McAfee Hybrid Delivery Architecture—the Best of All Worlds

These scenarios and many others are enabled by the McAfee Hybrid Delivery Architecture vision, embodied in seven requirements:

0. Best-of-breed, proactive security services that deliver a strong security foundation
1. Flexible deployment options: integrated hardware and software, virtualized, and hosted
2. Single price for multiple deployment options
3. Fully portable security services
4. Support for combining services across delivery platforms
5. Common policy definition and administration
6. Unified reporting

By adopting these requirements, IT organizations will be able to mix and match integrated appliances, virtualized appliances, and hosted service delivery. Instead of trading off security and cost, IT can adopt and adapt easily as their business demands.

While others tout multiple platforms, McAfee is building this robust business and technical architecture into its McAfee Web Protection solution to deliver next-generation security on the next-generation platform. With unified pricing and services, we make it easy for both security-sensitive and cost-sensitive organizations to deploy advanced web security. To learn more about McAfee's platforms, solutions and vision, visit www.mcafee.com/websecurity.

About McAfee, Inc.

McAfee is the world's largest dedicated security technology company. Delivering proactive and proven solutions and services that help secure systems and networks around the world, McAfee protects consumers and businesses of all sizes from the latest malware and emerging online threats. Our solutions work together, integrating anti-malware, anti-spyware, and virus protection with security management features that deliver unsurpassed real-time visibility and analytics, reduce risk, ensure compliance, and help businesses achieve operational efficiencies.

