BLUE COAT

Security Empowers Business

TOP FIVE REQUIREMENTS FOR GUEST WI-FI ACCESS

SOLUTION BRIEF

Providing guest Wi-Fi access has become a must-have capability for companies in nearly every industry. Today, free Wi-Fi is ubiquitous in highly trafficked areas such as airports, coffee shops and hotels. However, guest Wi-Fi is not limited to retail environments; businesses in other sectors such as finance and healthcare also need to offer guest Wi-Fi to vendors and customers. However, these industries must ensure a high level of security and enforce company-specific acceptable use policies. And, depending on the industry and geographic location, businesses may also need to comply with country-specific regulations.

In addition to enforcing acceptable use policies, organizations need to optimize network performance and collect data that can be used to improve customer service and increase marketing opportunities, but without the burden of maintaining logs on non-essential traffic. For example, the widely used "captive portal" or guest login page could require users to register with their name, email and other demographic information that businesses can leverage for future communication.

Any company planning to deploy a guest Wi-Fi solution, or improve an existing solution with enhanced security and performance, should first consider these top five requirements:

① Separate guest and internal networks.

Network security is the first priority for any company looking to offer guest Wi-Fi access. Isolating guest and employee BYOD access from the rest of the enterprise network is a good practice to follow to ensure that the security and administration of the corporate network remains unaffected. Network segmentation can be achieved physically or virtually depending on the needs of the business.

Virtual segmentation, such as the routing of guest and BYOD access through a virtual LAN (VLAN), can offer a cost-effective solution by using the existing infrastructure. A small clinic, for example, may be able to use its on-premise security implementation to create a VLAN network for guest access. However, the additional traffic, which can include encrypted transactions and rich media, can impact the overall network performance.

Conversely, a distributed bank may decide to completely isolate their internal network from their guest Wi-Fi network to provide a logical as well as physical separation between them. Separation ensures that guest Wi-Fi can't impact the performance or the security of the bank's internal network. This type of deployment can be achieved with either an additional on-premise security solution or a cloud-based solution that can minimize deployment overhead and ensure all guest Wi-Fi traffic is secured through SaaS solutions.

② Enforce appropriate use.

If used for unauthorized purposes, guest Wi-Fi can have severe consequences for the enterprise. Objectionable and potentially illegal Wi-Fi traffic such as pornography and gambling can tarnish the corporate brand or even lead to legal action and fines.

Therefore, any guest Wi-Fi solution must be able to enforce the acceptable use policy because simply asking users to read and sign a lengthy policy is both unrealistic and insufficient. Enterprises must be able to enforce their own policies and block any questionable or illegal network use.

In addition, guest Wi-Fi opens the network to all types of devices ranging from traditional laptops to tablets and smartphones. As a result, the security solution must be able to enforce the acceptable use policy regardless of whether the user has a traditional browser, mobile browser or a specific app found on tablets and smartphones.

BLUE COAT

Security Empowers Business

SOLUTION BRIEF

③ Protect against malware.

Since many guest Wi-Fi solutions are offered at low (or no) cost to end-users, some enterprises assume end users are ultimately responsible for the safety of their device and personal information. While all end users should be diligent about mobile security, businesses must guard against negative press that can result from malware attacks and identity theft against users accessing their guest Wi-Fi network.

Incidents like these may suggest that the enterprise is not only indifferent to the security of their guests; public perception of the company's overall security may suffer as well. Enterprises in verticals such as financial, healthcare or even retail are especially vulnerable to the loss of consumer trust.

④ Enhance the mobile experience for customers and employees.

As previously mentioned, tablets and smartphones are more commonly used for guest Wi-Fi than traditional laptops. For this reason, enterprises need to ensure their acceptable use policy and security solution extends to these devices as well. This is often not the case.

Here's why: Tablets and smartphones typically leverage native apps or mobile web browsers instead of traditional browsers. These native apps and mobile web browsers are often different from those designed for traditional browsers. Therefore, common security and acceptable use policies designed for traditional browsers may not translate to tablets and smartphones.

This security gap can create vulnerabilities in the internal enterprise network because many companies simply open up their guest Wi-Fi network to BYOD employees. Therefore, a gap in guest Wi-Fi security can compromise employee devices and put both the employee and enterprise at risk.

⑤ Achieve total network visibility that supports business analytics.

Enterprises are quickly realizing the value of gaining visibility into all the traffic accessing their guest Wi-Fi network. With the right solution, administrators can identify common security hazards faced by the user and use this insight to improve both guest Wi-Fi and internal network security. For example, a rise in malicious links via Facebook "Likes" can alert administrators to review the security of their corporate Facebook page as well as employee social media use.

While some enterprises view guest Wi-Fi as a way to gather end-user or consumer intelligence, businesses must clearly identify and safeguard the information being gathered. For example, while it may be good business practice to assess the performance of an iOS or Android app on the guest network, logging other information such as email use may be considered an invasion of privacy.

Find the best guest Wi-Fi solution.

Organizations have a wide range of choices for deploying or expanding their guest Wi-Fi offering. Therefore, it's important to assess and prioritize the requirements outlined in this document in order to choose the best solution.

Blue Coat offers a wide range of solutions for guest Wi-Fi, including traditional appliances, virtual appliances and cloud services. All Blue Coat solutions offer common policy enforcement, so customers enjoy the same security and policy features regardless of which solution they choose.

Common policy enforcement also enables enterprises to deploy a combination of solutions that best meet their needs. Customers can easily extend their guest Wi-Fi network with additional appliances, use a virtual solution that leverages existing hardware or move to cloud services with essentially no on-premise hardware.

Learn more.

Find out more about Blue Coat solutions at www.bluecoat.com.

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000