USE CASE

Protecting Your Guest Wi-Fi

Executive Summary

Businesses continue to evolve as digital technologies reshape industries. The workforce is mobile, and speed and efficiency are imperative, necessitating dynamic, cloud-based infrastructures and connectivity, as well as unhindered, secure application access — from anywhere, on any device, at any time. Leaders must remove hurdles to progress, but new business initiatives and processes increase the attack surface, potentially putting companies at risk.

Many businesses are embracing a zero trust security model to meet these challenges head on. A zero trust architecture assumes that everything on the network is hostile; gone are the days of "inside versus outside" and perimeter security, as too is the mantra of "trust, but verify." In their place, organizations must adopt a "verify and never trust" outlook, authenticating and authorizing every device and user before delivering applications or data, and monitoring application access and network activity through logging and behavioral analytics.

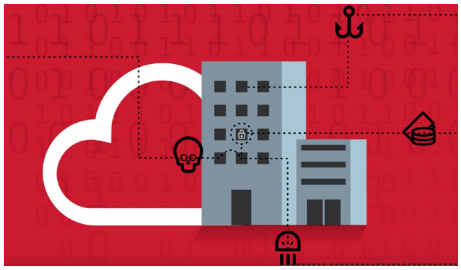
One of the many use cases associated with a zero trust security strategy is protecting guest Wi-Fi networks.

Protecting Your Guest Wi-Fi

At some point in the last decade, the question "Do you have Wi-Fi?" was superseded by the assumptive "What's your Wi-Fi password?" A connection to not just the Internet, but complimentary and performant Wi-Fi, accessible from an array of devices, often simultaneously, is an almost universal expectation, despite locale. We are connected at home, at work, on trains, at airports, at the local coffee shop, at our favorite retail destination, at stadiums, and even at 30,000 feet when traveling.

There are many benefits for the businesses and organizations that provide this connectivity via a guest Wi-Fi network, including improved brand perception, increased foot traffic, and superior customer experiences. But this differentiation doesn't come without challenges; customers, visitors, volunteers, or employees using your Wi-Fi network pose a significant risk if access is unfettered and unmonitored. Left unprotected, guest Wi-Fi networks are potential hotbeds for cyber threats and stolen data, as well as a massive brand liability.

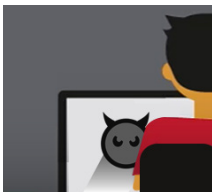
Inherent to users connecting their devices to your Wi-Fi network is understanding that you can have no expectation of the health of their machines, or the benevolence of their intentions. If previously compromised, their laptops, smartphones, connected wearable devices, and tablets may bring a barrage of malware and other advanced, targeted threats onto your network. If your network is unchecked, these infections will spread rapidly to other guest users and their devices. And given the volume and variety of activity on your guest Wi-Fi network, there will likely be requests made to malicious domains, whether accidental or deliberate.



Therefore, Internet requests that are unexamined and returned ubiquitously over the recursive Domain Name System (DNS) infrastructure are highly likely to carry a cyber threat back onto your network via a compromised endpoint. Once on your network, these threats will seek to connect with their command and control (CnC) framework. When this communication is established, sensitive and private information can be siphoned out of your network via DNS-based data exfiltration. This leakage might be the proprietary corporate data, the personal information, or the identities of your guest users.

Furthermore, unprotected and unaudited guest Wi-Fi networks are often misused by employees looking to bypass security measures on the corporate network. Whether these employees are looking to access content disallowed by the enterprise's Acceptable Use Policy or they are trying to skirt clumsy and frustrating security mechanisms that impede productivity, this bouncing between networks undermines your corporate security posture and creates gaps in your defense-in-depth strategy.

In addition to being an avenue for cyber threats that puts your customers, visitors, volunteers, and employees at risk, unprotected and unmonitored guest Wi-Fi poses a danger to your company's hard-earned brand reputation. In today's climate, where personal alignment with a company's values and actions often dictates consumer loyalty, this is arguably more important than ever before. As such, guest Wi-Fi users abusing your service to engage with inappropriate, unsavory, or even illegal content can be very detrimental to your brand reputation and ultimately, your earnings.



Beyond these violations of Acceptable Use Policies, those connecting to your guest Wi-Fi have an expectation of security. If, as discussed above, their devices or personal details are negatively impacted or leaked while connecting to your network, your brand image will undoubtedly suffer. Who's going to place their trust and future business in the hands of a company whose Wi-Fi unleashed crippling ransomware on their computer or exposed their credit card information?

Take Action: Implement Zero Trust

To responsibly and successfully furnish your customers, visitors, volunteers, or employees with a Wi-Fi connection, you must secure the network — protecting the users, their devices, and their information. And all of this naturally must balance against your bottom line; the cost of scaling secure guest Wi-Fi is often a limiting factor. Adopting a zero trust security model — simply authenticating and authorizing every device and user before delivering applications or data, while monitoring app access and network activity through logging and behavioral analytics — can easily help you protect your guest Wi-Fi.

Read "Moving Beyond Perimeter Security" to learn more about adopting a zero trust security model, or visit akamai.com/etp to learn more about Akamai's cloud-based, centrally managed, and easily scalable solution to securing your guest Wi-Fi.

Akamai