



Rogue WiFi Monitoring

ROGUE WIFI MONITORING

Wireless capabilities are being built into tens of millions of computers and other devices. The convenience of being online anywhere has made the popularity of wireless transmitters, known as “access points”, soar. Wireless access points have very small footprints, are low cost, and can easily be set up. As such, it is increasingly likely that a wireless device will be placed in your office, without the consent of security management. It is equally likely that a neighbor will be broadcasting a wireless signal, allowing your employees to join an unauthorized network.

Because “rogue” wireless connections can bypass all security layers, they represent one of the biggest threats to enterprise network security. The locks on the computer room, the passwords put in place to gain access – even the firewall - can now be bypassed if a computer in your network locks onto the wireless network of the office or neighbor next door, or onto an unauthorized wireless network set up by an employee or contractor. Self-starting WiFi users in your company who set up their own access points may neglect to protect the device with passwords or keys, opening your network to anyone nearby. The over-the-air connection of 802.11 networks can be exploited by almost anybody who is within range of the access point.

Any comprehensive security architecture needs to include monitoring for ad hoc or unapproved wireless networks, including immediate quarantine upon detection of unauthorized connections.

CATBIRD'S SOLUTION: DETECTION AND RESPONSE

Catbird Network's Rogue Wireless Monitor is your first response to a WiFi threat. Catbird automatically sends an alert the instant a corporate computer logs onto an unauthorized wireless network. Catbird also monitors authorized wireless networks to ensure only authorized computers connect. Upon detection of Rogue WiFi activity, Catbird's quarantine – or “Penalty Box” - mechanism is automatically triggered. This Penalty Box automatically neutralizes the threat of the offending device through isolation – the host is simply prevented from accessing the network. Once IT administrators have identified the device and determined that it is safe, it may easily be reauthorized to join the corporate LAN.

When enabled, Catbird's Penalty Box will quarantine any rogue host that is on the same logical network as the Catbird internal agent. Once a rogue device is quarantined, all network traffic coming from that host is automatically

BENEFITS

Automatic and Immediate Threat Mitigation Catbird's WiFi Monitor detects rogue wireless activity and instantly prevents the offending device from harming the larger network.

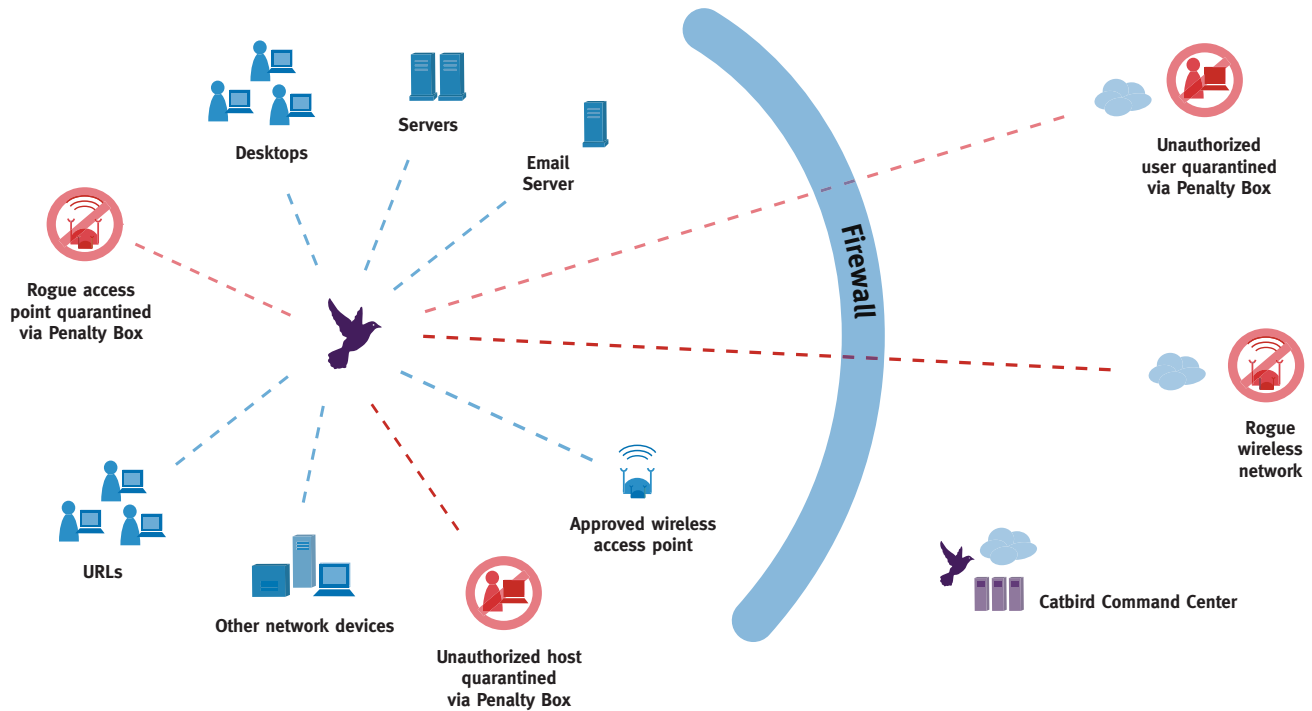
Stay on top of the latest security threat WiFi exploitation is the latest thorny problem in network security. Hackers are aware of this and taking advantage of the many “backdoors” WiFi introduces. Any comprehensive security architecture must address the vulnerabilities of WLANs.

Cost-effective Catbird's rogue WiFi monitoring provides enterprise-class protection with minimal expense.

Bullet-proof appliance Catbird's hardware agents are highly secure, allowing no inbound connections. Competitive devices allow access using web interfaces.

Rogue WiFi Monitoring

Catbird's comprehensive rogue wireless monitoring



directed to the Catbird internal agent, where it is discarded. By preventing communication between the unauthorized computer and the rest of the network, any potential threats are effectively neutralized.

All rogue wireless devices can be detected and quarantined by Catbird's Rogue Wireless monitor, including unauthorized access points, wireless laptops/devices/soft APs, peer-to-peer (ad hoc) communication and accidental associations with neighboring WiFi networks.

THE CATBIRD ROGUE WIRELESS MONITOR WITH PENALTY BOX WILL IDENTIFY AND STOP:

- Unauthorized users on the corporate WLAN
- Rogue Access Points set up by corporate employees
- New computers joining the corporate WLAN which have not yet been approved by IT staff
- Infected computers on the corporate WLAN

THE CATBIRD ROGUE WIRELESS MONITOR WITH PENALTY BOX WILL IDENTIFY:

- Authorized users on unauthorized WiFi networks

DEPLOYMENT

Catbird provides an internal agent which is placed onsite and in the same segment as the WLAN. This agent continuously watches the unlicensed spectrums on 2.4 GHz and 5.2 GHz and verifies that there is no activity contrary to the defined wireless policy. If a rogue wireless machine or access point is detected, it is quarantined within milliseconds. Then alerts are sent to the Catbird Command Center where administrators can view subsequent notifications and other relevant data.