NetworkChemistry™

INDUSTRY REPORT

Network Chemistry Wireless Threat Index™

Network Chemistry Wireless Threat Index Exposes Enterprises at Significant Risk for Data Loss

The Network Chemistry Wireless Threat Index is the first and only ongoing index to track and reveal trends that help enterprises and government organizations protect themselves from emerging wireless threats. The recently published index analyzes over 700,000 network connections across a wide range of devices – and warns that widespread use of unsecured mobile laptops and devices threaten organizations' networks, data and users. The report will be published on a quarterly basis.

Is Your Organization at Risk? Findings from the Wireless Threat Index

The explosion of wireless usage has enabled a new and dangerous vector for access to confidential data and can be used to damage the integrity of corporate networks and assets. The Network Chemistry Wireless Threat Index has been established to monitor these threats and assess the ongoing risk. Attacks on wireless LANs (WLANs) and breaches of 'no wireless' policies are a quick and easy way for hackers to steal data and enter the corporate network.

The wireless network has the same challenges as the fixed, wired network and organizations must have a pre-emptive plan of action to prevent wireless attacks and policy violations that can compromise an organization's data privacy and regulatory compliance. Security managers need to plan for, monitor, and mitigate potential wireless threats as well as react quickly when any breach occurs. The Network Chemistry Wireless Threat Index can be used by organizations as an early warning system to increase awareness of the growing threats and support investment in wireless security solutions.

Security Myths Disproved by the Data

The data for the analysis used in the Network Chemistry Wireless Threat Index was gathered from the thousands of laptops running the RFprotect™ Endpoint product and the hundreds of thousands of connections that they made in offices, on the road, and in homes from December 2005 to March 2006.

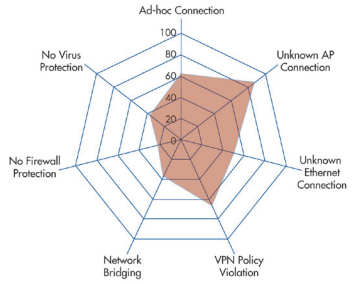
Based on the current analysis, a number of key reports were generated and the same data will be tracked over time. The findings also suggest that some pre-conceived notions about how laptops are used should be reevaluated.

The top four security myths disproved by the data are as follows: wireless connections are rarely made to unknown networks (36% of all wireless connections were with unknown APs), users do not connect to wireless and wired networks at the same time (37% of the endpoints analyzed had network bridging enabled), ad-hoc networks are seldom used (63% of endpoints had an ad-hoc connection turned on or tried to connect to one), and users actually use their VPN clients (68% of endpoints experienced violations of VPN policy).

This data provides excellent insight into how laptops are used once they leave the office and the importance of having security personnel apply and automatically enforce policies on what connections are allowed and how those communications should be secured. End users will inherently choose productivity over security and IT must transparently assure that the machines are being used in a safe manner that does not put the user or corporate data at risk.

Wireless Risk Profile

The data was analyzed to determine and report on the most significant risks and the likelihood that they would be exploited. The wireless risk profile chart describes the various types of wireless related threats that organizations and their endpoints face. The data represents the total percentage of endpoints that have experienced each type of threat. For example, 63 percent of all of the endpoints currently being protected by RFprotect Endpoint have or had the ad-hoc mode enabled.



TYPE OF THREAT	PERCENTAGE
Ad-hoc Connection	63
Unknown AP Connection	87
Unknown Ethernet Connection	52
VPN Policy Violation	68
Network Bridging	37
No Firewall Protection	23
No Virus Protection	38

- Each of the risks represented in this chart is significant and can be defined in the following ways:
- Ad-hoc connection - the endpoint has attempted to connect to an ad-hoc network
- Unknown AP connection - the endpoint has connected to an AP which is not previously known
- Unknown Ethernet connection - the endpoint has connected to an Ethernet network which is not previously known
- VPN policy violation - the endpoint has attempted to send network traffic across a connection when a VPN should have been used according to policy
- Network bridging - more than one interface on the endpoint was connected at once, e.g. by being plugged into the corporate LAN at the same time as being connected to a wireless AP or ad-hoc wireless network
- No firewall protection - the endpoint is not running a software firewall
- No virus protection - the endpoint is not running virus protection software

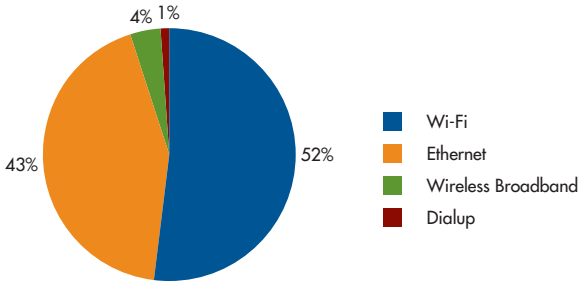
NetworkChemistry™

INDUSTRY REPORT

Network Chemistry Wireless Threat Index™

Connection Methods

Another area of focus for the index is on the type of connections used by endpoints. The following chart describes the usage of different interface types that were used when endpoints made a network connection. The analysis shows that wireless is now the preferred method of connectivity. The prevalence of wireless usage highlights the importance of ensuring secure connectivity practices to avoid loss of corporate data and/or misuse of resources.

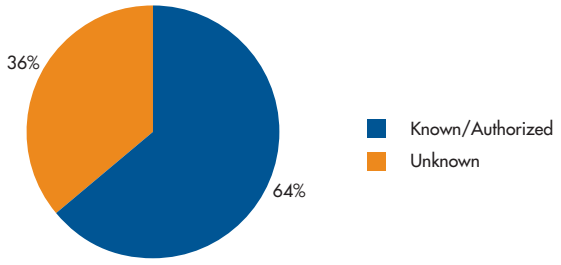


Known vs. Unknown Connections

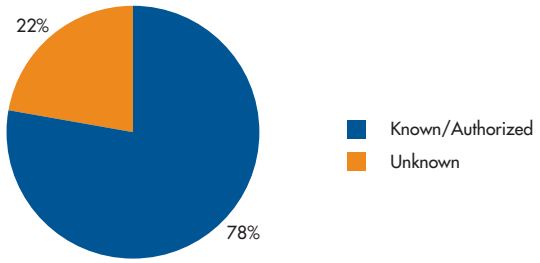
A critical piece of information for network and security personnel to understand is whether connections are being made to known and or safe networks. The analysis in this component of the index covers the percentage of connections to authorized verses unknown networks. It shows that 36% of all wireless access point (AP) connections were with an unknown AP while 22% of all Ethernet connections were with an unknown network.

In addition, users frequently connect outside of the enterprise which expands the network perimeter and risk of data loss. When connections are made with unknown APs or unknown Ethernet networks there are a number of risks including lack of encryption, evil twin, man-in-the-middle and phishing attacks.

AP Connections



Ethernet Connections



Summary

With the rapid expansion of mobile and wireless technologies, organizations are seeking more tools to help them assess risk and monitor potential threats, such as those coming from unsecured laptops, which leave a back door open to their networks. The Network Chemistry Wireless Threat Index provides a detailed, ongoing way for IT and security personnel to better understand and track emerging wireless threats, putting them in a position to mitigate any potential risks.

Look to the Leader

Network Chemistry is the industry standard for securing the mobile enterprise. The world's most successful enterprises and demanding government agencies trust Network Chemistry's wireless security solutions to prevent attacks, detect vulnerabilities, intrusions and policy violations, accelerate incident response, and conduct surveys for wireless LAN deployment planning. Network Chemistry offers the industry's only integrated platform for automating wireless threat protection, covering organizations' assets both inside and outside their facilities. Contact Network Chemistry today and put the wireless security experts to work to assure the protection of your critical data and assets.

Network Chemistry, Inc.
1700 Seaport Boulevard
Redwood City, CA 94063 USA
(650) 249-4300 Phone
(650) 249-4301 Fax

For More Information:
1-888-WLANIPS
www.networkchemistry.com