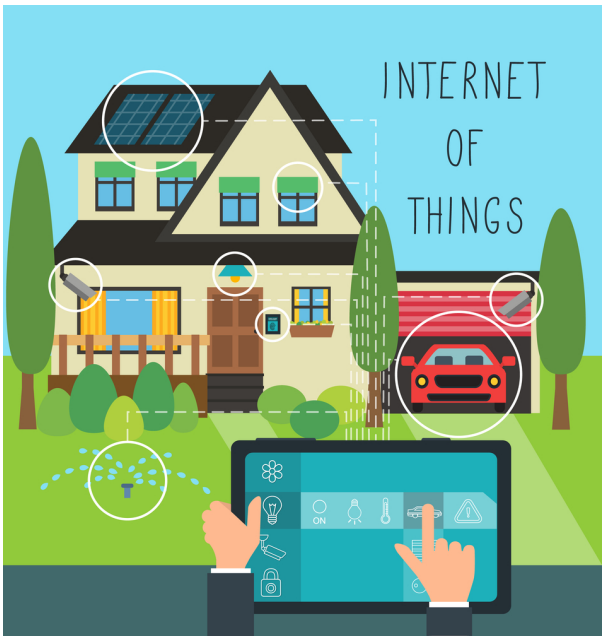
How To Stay Ahead Of The IoT Invasion

A corporate-owned, agent-enabled laptop with an OS that's out of date – that's an obvious risk. But what about an agentless video surveillance system? That's a potential disaster you never saw coming. And that kind of threat – the threat from something you can't see – is the most dangerous of all.

Today's enterprise networks contain a vast and increasing range of devices – traditional computers, mobile devices, industrial controls, medical equipment, virtualised servers and cloud-based applications to name a few. This diversity is accelerating as hybrid IT environments and the Internet of Things (IoT) become the norm.

The reality is that detecting IoT-related risks or malware is next to impossible without the ability to see all the devices, applications and servers connected to the network. And traditional security solutions can only mitigate risks they can see, meaning that unless an agent is installed on the endpoint, IT is blind to its presence.

IoT: Where the Wild Things Are



Cybercriminals are growing more sophisticated every day. Using connected devices that are undetected, hackers can gain access to networks and may not be discovered until after an attack. While investigating a customer's distributed denial of service (DDoS) attack, Imperva found that IP addresses belonging to CCTV cameras – all accessible via default login credentials – had been used to gain access to the network. Any kind of IoT device can be re-purposed as a DDoS "zombie" in an attack: printers, sensors, wearables, smart TVs or virtually anything that connects to a network using an IP address.

A Failure to Communicate

The newest security challenge today is not only the number of security, management and compliance solutions, but also the lack of coordination between them. Most major technology tools

today do not share information with other relevant solutions that could help detect, prevent or respond to a cyberthreat. Therefore, people – rather than technology – are required to connect the dots. However, as demonstrated by some well-publicised recent breaches, relying on overwhelmed security operations teams to sift through alerts from dozens of tools is problematic and falls short. The simple fact remains: fragmentation lets attackers in.

Staying Ahead of the IoT Invasion

Security through visibility is quickly becoming the new standard. This essential capability provides the means to activate the proper security solutions and orchestrate information sharing and operations.

To stay ahead of cybercriminals, best practices for securing endpoint visibility include:

• See. You have to see it to secure it. Once organisations gain enhanced visibility into their network, customers typically report they discover 20-30 percent of unknown devices on their network. That's largely because non-traditional devices such as security cameras, smart TVs and media equipment are generally left out of the network security equation because these devices lack security management agents. Organisations must have a single point of view of their connected environment, and they must be able to see IP-addressable devices on the network.

• Control. The ability to see devices is critically important. However, you need other advanced capabilities as well. You must also be able to control devices and automatically enforce your security and compliance policies based on rich contextual information. And what about devices that drop on and off the network? If you want nonstop security, your cybersecurity solution must continuously monitor and mitigate attacks. Best practices today call for solutions that provide identification, operational intelligence and policy-based mitigation of security issues—even in the most complex enterprise networks.

• Orchestrate. No single security tool will protect against the firestorm of threats facing networks today. Advanced threat detection systems may quickly detect indicators of compromise (IOCs) on your network and alert IT staff about this condition. But then what? Without multisystem orchestration, infected systems propagate the threat until manual IT intervention stops them. One thing is abundantly clear: manual processes simply can't scale to meet the explosive growth of mobility and IoT.

Through system-wide orchestration, systems share contextual data to improve security effectiveness. They also work together to automate response and security enforcement to quickly contain risks and remediate compromised endpoints. Not only does this save considerable administrative time, it dramatically reduces the attack window to protect your enterprise.

Transforming Security through Visibility

Organisations should identify agentless security solutions that can see their network-connected devices, intelligently control those devices according to pre-defined policies, and, most importantly, orchestrate information sharing with the vast number of IT tools already in place. It's the only way

to stay a step ahead of today's increasingly hostile cybercriminals.

Take our Internet of Things quiz!