Detect and Protect Your Networked Internet of Things (IoT) Systems

Many companies are adopting new, networked systems like buildings management systems, card access control systems, and industrial control monitoring sensors to improve efficiency and cut costs. Though useful, these Internet of Things (IoT) systems often use very lightweight software that often can't accommodate traditional security controls designed to deter malware and intrusions.

The inherent security shortfall presented by IoT systems can provide cybercriminals with an entry point into your network – with hackers potentially using your IoT as a starting point to reach your more traditional IT hardware. This can understandably lead to malware infections, hacking attempts, exposed vulnerabilities, and more.

Therefore, companies that use IoT systems may struggle to defend their networks against cybersecurity threats. And as the IoT trend grows, it will become harder and harder for organisations to keep track of their growing IoT inventory and manage the potential risks it brings.

So, how do you keep your whole network protected when some of your systems can't necessarily use more traditional cybersecurity protections?

What is the Internet of Things (IoT)?

The term "internet of things" or IoT refers to devices and systems that connect to a network, but aren't necessarily PCs or other "traditional" IT devices. Some day-to-day examples of IoT include smart watches, smart appliances (e.g., refrigerators), smart speakers, and app-controlled heating and lighting systems.

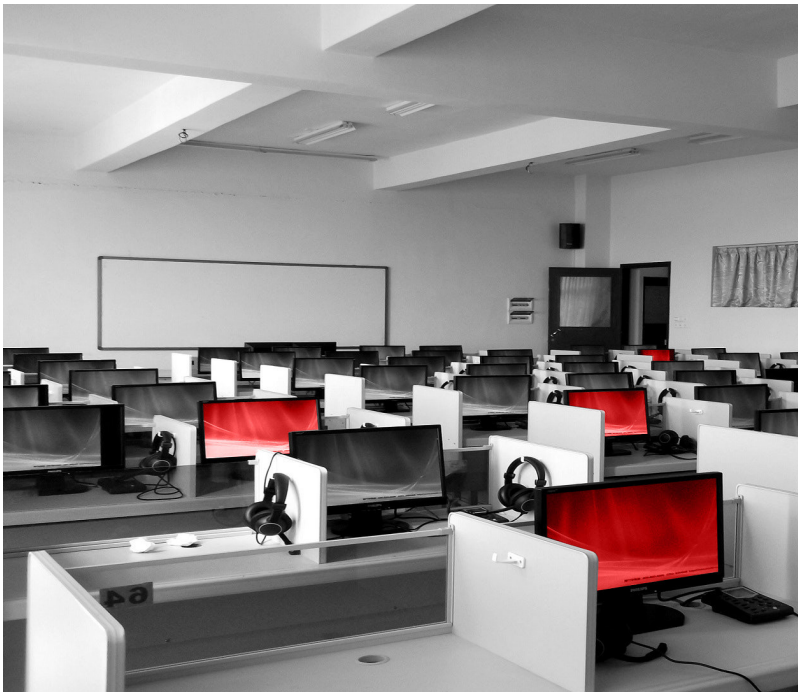
However, many modern workplaces run business-critical functions through IoT systems which vary wildly in their complexity. At the more straightforward end of the scale there's access control systems or buildings management systems that might feed data to the cloud.

At the more complex end of the scale, an engineering firm may depend on information fed back to them by networked sensors and actuators; or infrastructure organisations may be contingent on real-time information coming in through internet enabled SCADA systems.

IoT usage is rapidly growing year-on-year, with 75.44 billion installed IoT devices predicted worldwide by 2025 (Source: Statista).

Why IoT Security Controls are Needed

Any device that connects to your network can potentially serve as a point of ingress for hacking attempts or malware. PCs are relatively easy to protect through readily available antivirus software. Servers may also be able to use traditional antimalware controls but if not, then they can generally rely on state-of-the-art firewall systems.



IoT systems often use lightweight operating systems to help keep costs and complexity to a minimum. Therefore, most IoT devices can't run antivirus software and many such devices lack fundamental security controls. This makes them understandably very vulnerable, and a network is only ever as protected as its weakest device.

With the right tools, a hacker could hypothetically gain access to your network through an unsecured IoT system. This could cause widespread disruption, including potential production line outages, malware outbreaks, data theft, and even denial of service attacks.

Additionally, many IoT providers package their devices with off-the-shelf software and operating system solutions. Because these solutions are generic, that can make the IoT very sensitive to attack. It only takes one hacker - familiar with a particular operating system's security flaws - to exploit the device and potentially cause untold havoc on your network.

How Rebasoft Secures Your IoT Devices

Rebasoft provides a 360-degree, real-time, bird's-eye view of all devices and traffic on your network, making light work of monitoring IoT devices and any suspicious traffic that may flow through them. As soon as Rebasoft is deployed on a network, it identifies and catalogues all connected devices. Put simply, if something connects to your network then Rebasoft can provide surprisingly detailed insight into what it is and what it's doing – whether it's a PC, a server, a switch, or an IoT system.

Rebasoft eliminates the need for manual asset recording by providing an accurate, real-time picture of all devices connected to your network. Rebasoft even discovers potentially vulnerable devices that are connected to your network but may have been long forgotten.

IoT systems on your network (and other devices where anti-malware controls can't be applied) can easily be flagged, profiled, and monitored using Rebasoft's comprehensive malware and hack detection features. Our solution operates in real time and at network level, so it doesn't rely on individual software agents or periodic scans that may cause areas of the network to be overlooked.

But looking at a network's hardware will only ever provide part of the story. Rebasoft's robust behaviour monitoring functionality establishes an ongoing picture of what normal, everyday network activity looks like so it can raise an alert when something suspicious may be happening.

Hacking attempts and malware propagation commonly cause spikes in uncommon types of network traffic. Thankfully, these behaviour patterns are easily detected by Rebasoft's real-time behaviour monitoring capabilities.

If any suspicious activity is detected around any given endpoint (not just an IoT system), Rebasoft can use automated port blocking to effectively quarantine the device from the network and alert an engineer to investigate further.

So even though IoT devices typically can't be protected by anti-malware controls, Rebasoft provides a way of holistically securing your whole network with robust asset, perimeter, and behaviour monitoring functions.

Rebasoft Can:

- Help you identify and log devices where traditional antivirus controls can't be implemented.
- Automatically defend your network from hacking attempts, malware, or other cyber-threats.
- Locate all network endpoints and monitor the traffic that flows in, out, and around them.
- Provide much-needed peace of mind surrounding business-critical IoT systems.
- Bring long-forgotten networked devices to light that may require updated security attention.

Rebasoft's Core IoT Security Benefits

- Monitors your network's hardware and behaviour in real time, discovering all connected devices and systems, regardless of their functions.
- Gathers data directly from the network using established protocols, meaning it doesn't rely on individual software agents.

- Provides a holistic, up-to-the-minute picture of your network, enabling timely reactions to malware propagation, hacking attempts, shadow IT, and other potential cyber risks.
- Offers a non-invasive, lightweight alternative to solutions that rely on periodic or partial scans – Rebasoft gives you a complete 360-degree picture at all times.
- Enables immediate response to suspicious network changes through automated alerts and port blocking.
- Applicable to numerous practical use cases, including network access control, edge/perimeter security, asset management, malware resilience, hack detection, and more.
- Offers flexible integration and extensive API support, working in tandem with your existing security systems and enhancing their effectiveness.
- Effortlessly scalable, handling infrastructure changes and growth with ease.
- Capable of protecting 100 to 100,000+ end points.
- Helps busy CEOs, CIOs, CISOs, and IT technicians make educated decisions about networked IT systems and security.
- Retains historical data on detailed network and hardware metrics, enabling informed reflection and review.

Why not experience Rebasoft's comprehensive network visibility and cyber resilience capabilities for yourself?

Book your free, no-obligation demonstration today by **calling the team** on 0800 799 7322 or **emailing** sales@rebasoft.net.