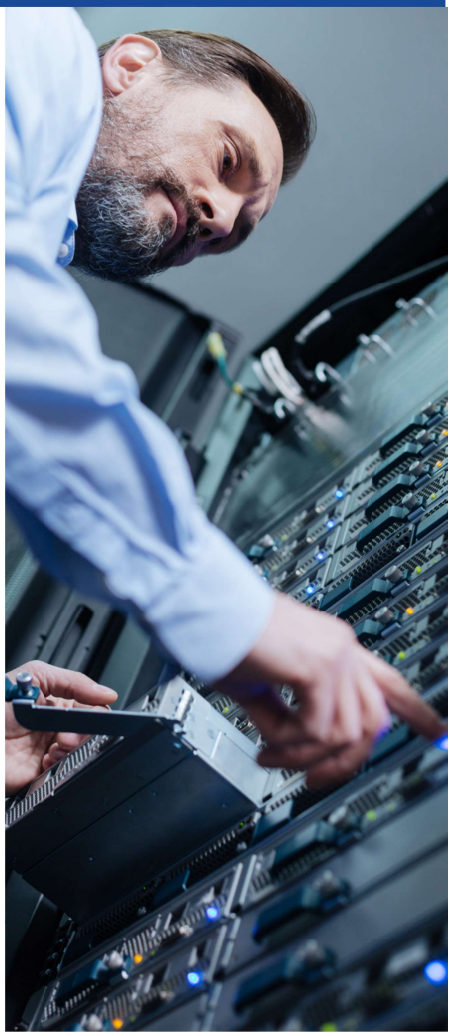
ARGENT


www.Argent.com

Argent White Paper

# Stopping Ransomware Permanently

# Introduction



**CIOs are faced with the perfect storm: not enough qualified people combined with a surplus of ever-more-effective ransomware criminals.**

The world is a global village. It's a platitude, but a relevant one because sophisticated hackers in mainland China or the former eastern Europe are electronically trying your doors to see which ones are unlocked, possibly while you are reading this. But it gets worse...

While Bring-Your-Own-Device might delight Sally May in Accounting, the new tablet she connected to your network just compromised your entire network.

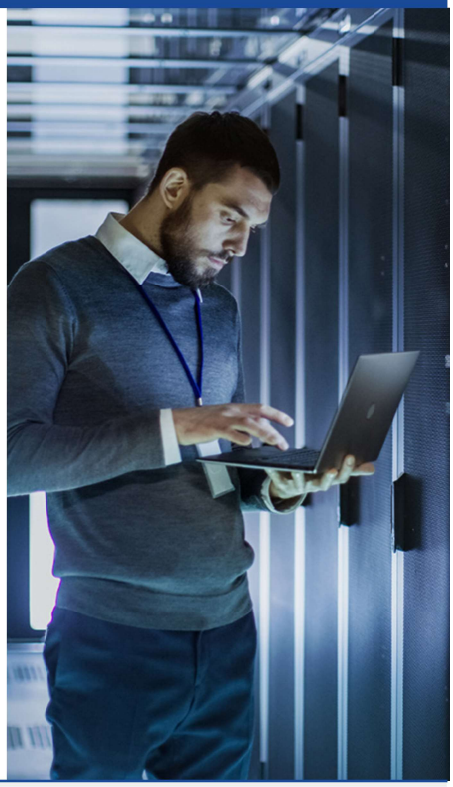
What to do?

Here are the essentials: automation, set-and-forget, and 7-by-24.

This brief White Paper explains the basics of how you can be secure, once and for all, in under 30 minutes.

# What Are You Actually Managing?

**Managing an IT infrastructure for all IP-based network end-points means all PCs, Servers, private tablets (attention Sally May), VOIP Phones, Printers, CCTV Cameras, Switches, Routers and Wireless Access Points.**



How many network end-points do you think you have?

How many of them connected to your network yesterday, today, and will connect tomorrow?

And how many were added in the past hour?

Do you recognize all end-points on your network?

## 200%

According to Juniper Research, the number of connected devices in 2025 is predicted to reach 80 billion worldwide. This is more than 200% the amount in 2020.

Enterprises typically manage a much larger network than they think.
**The larger the network, the more risk it faces.**

# Are Intruders Already in Your Network?


**Rogue devices are malicious. Some are connected to your network to steal sensitive information, such as financial details, passwords, and much more. Some are designed to disrupt your business.**

*Hackers gained entry into the networks of Colonial Pipeline Co. through a virtual private network account, which allowed employees to remotely access the company's computer network.*

***Source: https://www.bloomberg.com/***

*According to the New York Times, Colonial Pipeline paid approximately USD 5 million in ransom to hackers.*

***Even worse, the costs of ransomware are increasing.***

*As reported in the Insurance Journal, CNA Corporation Corp paid USD 40 million in ransom to a hacker in 2021.*

***Source: https://www.insurancejournal.com/***

*In 2024, a Fortune 50 company paid USD 75 million to a hacker.*

***Source: https://www.forbes.com/***

**The impact of cyber-attack can be very costly and, unfortunately, not all "bombs" are seen. The above are examples of potential damage from rogue devices connected to your network.**

---

Walk-in Device with an Employee or a Visitor

Third-party Vendor Appliance

Forgotten Device

Out-dated Network or Security Policy

# Argent Detects, Reports and Removes Rogue Devices

## Argent RansomSafe is a simple yet effective feature that achieves continuous improvement.

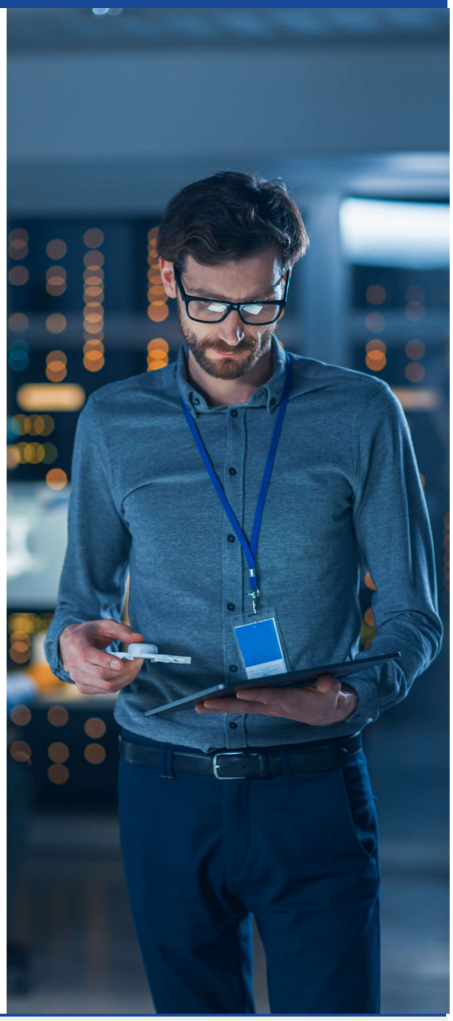
When first installed, RansomSafe is run to create a baseline of devices (the generated file can be manually edited).

Then, RansomSafe is set to automatic mode, whereby RansomSafe uses the existing baseline to check the network periodically (from 5 minutes to one day; the default is 60 minutes).


Each scan generates reports and alerts on new rogue devices.

Argent benchmarks show about 10**3 devices and takes under 10 seconds (and runs in the background.)

A fresh baseline can be optionally generated at any time.



Reports can be automatically emailed or saved to secure storage to keep the outside auditor happy – remember Sarbanes, CJIS, and GDPR?

**RansomSafe is included in Argent's latest flagship product suite – Argent Omega.**



Learn more by speaking to an Argent consultant today simply email

**Support@Argent.com**

**We'll do all the heavy lifting for you.**