THE RED DOT PROBLEM

—— A case for Consolidation ——

Dealing with the RED DOT problem in cyber security

Why is the RED DOT problem a case for Cyber Security Consolidation?

Cyber threats are everywhere. They are really like those red dots we see on threat maps, constantly appearing and disappearing, changing in size and intensity, and targeting different locations and assets. They are hard to track, hard to predict, and hard to prevent.


Trying to analyse the risk of each red dot is insanity.
Many organizations have tried, and we see them buying something as an antidote to a particular red dot. Each time they have failed, why?
Well, a static solution to a dynamic problem simply won't work.

- It is impossible to know the exact nature, source, and impact of every red dot. Some may be harmless or devastating. Some may be random, some may be coordinated. Some may be visible, some may be hidden while others morph all the time.

- It is impractical to allocate resources and attention to each red dot. There are too many of them, and they change too fast. Trying to keep up with them would consume too much time, money, and energy, and distract from the core business objectives too many times.

- It is ineffective and unsustainable to rely on traditional security measures for each red dot. They are good but not good enough to stop sophisticated cyber-attacks. They can be bypassed, hacked, or compromised by malicious actors.

An intelligent way to deal with the red dot problem is to adopt a consolidated approach. A platform that can provide comprehensive visibility, protection, and a proactive response across the entire organization. A consolidated platform should:
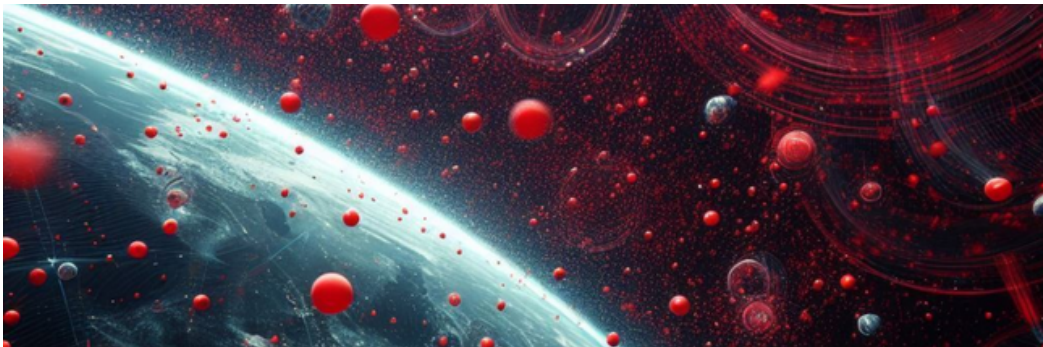
- Detect and identify in near real time these red dots, regardless of their type, origin, or location. It can collect and analyse data from multiple sources and systems while using advanced algorithms and artificial intelligence to spot anomalies and patterns.

- Prevent and mitigate the impact of the red dots on the organization. It can deploy proactive and reactive measures to block, isolate, or neutralize the threats, and minimize the damage they can cause.

- Respond and recover from incidents. It can provide timely alerts, reports, and recommendations to the relevant stakeholders, and help them restore normal operations as soon as possible.

As the famous man with scattered white hair once said "doing the same thing over and over and expecting a different result is the definition of insanity"

Well we are not insane so the time has come for us to adopt a different approach.
A consolidated platform is the best solution to the red dot problem because it can provide a holistic view of the cyber landscape, a unified approach and resilient posture to cyber defence.

Don't let the red dots overwhelm you. Choose the right consolidated platform for your organization today.

Don't know where to start?
Please contact Micro Nova Security @
 www.micronovasecurity.com

Stay Safe!
Micro Nova Security