Why (Only) Chasing Threats Is a Flawed Security Strategy

Chasing threats alone is an impossible, reactive task. 230,000 new malware samples are produced every day1. 84% of organizations claim traditional security solutions don’t work2. 197 DAYS is the mean time to identify data breaches2. 84% of organizations say their ransomware protection is ineffective3. 230,000 new malware samples are produced every day1. Traditional defense mechanisms do not work because they do not focus on reducing the attack surface. 72% focus on identifying and reacting to threats, while 28% focus on reducing the attack surface4. Chasing threats AND reducing the attack surface provide more effective security. Cybersecurity is getting worse. What you need to enforce known good behavior.

Deep application understanding. Getting known good information is hard. Getting a deep understanding of your applications is even harder. You need to know your apps inside and out, including app topology, app processes, acceptable state, who’s using them, from what devices, and how this changes over time.

Intelligent automation. Applications and application policies frequently change. You need intelligent automation to properly define, deploy, change, and remediate policies based on your dynamic apps.

Intrinsic security. Getting known good information is hard. Getting it without adding more complex security products and agents is even harder. You should use security that’s built into the infrastructure you already have.

Enforcing known good behavior reduces your attack surface. This means knowing your applications and allowing ONLY what they’re supposed to be doing.