FORESCOUT

AI-Accelerated Threats Demand AI-Driven Defense: From Visibility to Au

AI-Accelerated Threats Demand AI-Driven Defense: From Visibility to Automated Risk Enforcement

Rhonda Holloway, Director of Network Security & Federal Solutions Marketing

Most security operations can’t keep up with machine-speed attacks

AI Has Changed the Game

Attack velocity has outpaced traditional security operations.

- AI-assisted reconnaissance at scale
- Automated vulnerability chaining
- AI-generated phishing + social engineering
- Faster weaponization of zero-days


Cybersecurity Attackers Exploiting Vulnerabilities
Automated Vulnerability Discovery & Zero-Day Exploits
AI-Driven Initial Access via Automated Scanning
Mass Reconnaissance → Exploitation Pipeline
Fake AI Tools Used to Deliver Exploits
AI-Enhanced Ransomware Operations

The first weak points AI-driven attackers exploit

- Unknown devices
- Unmanaged endpoints
- Legacy OT systems
- Shadow IT / cloud sprawl
- Misconfigurations

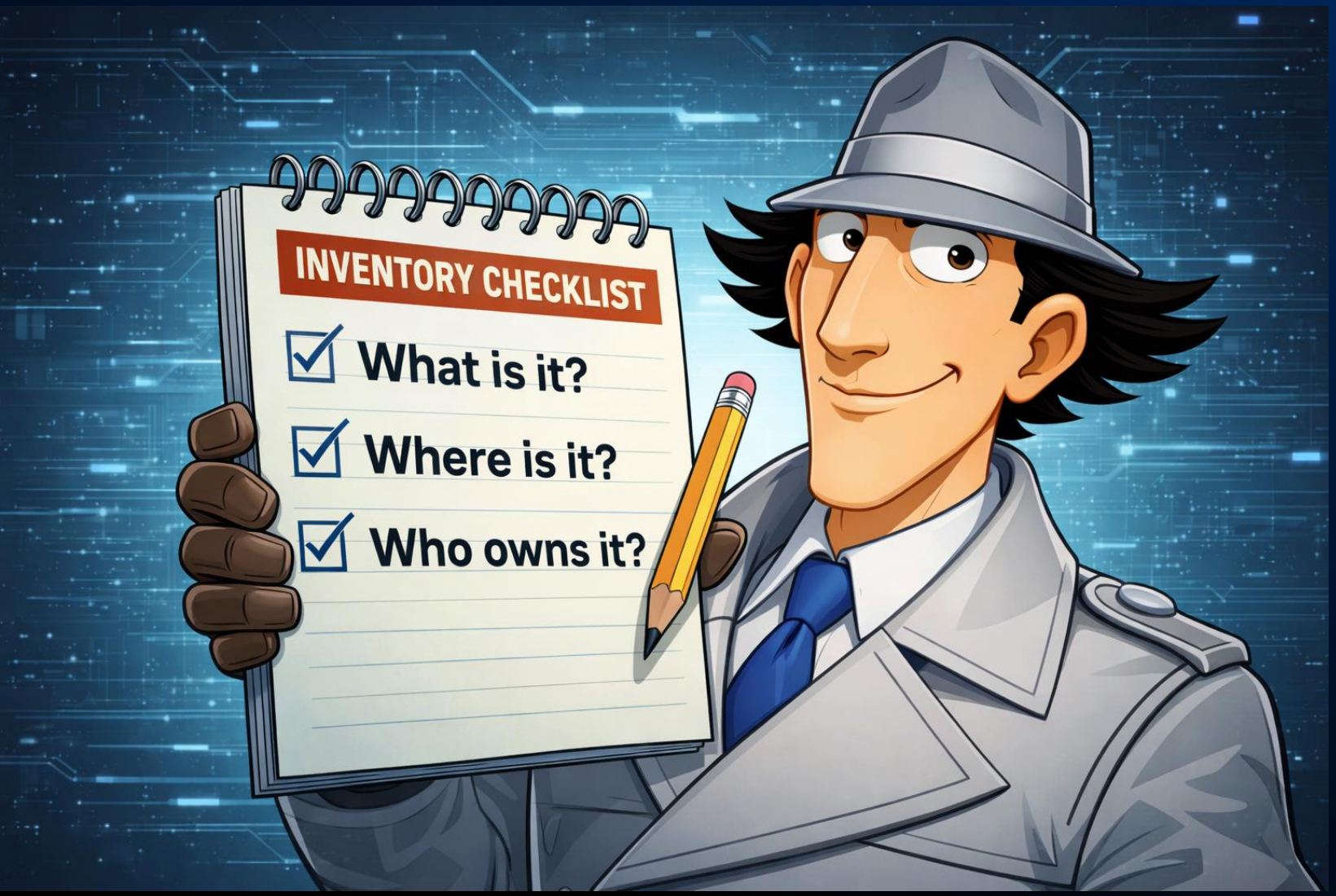
The foundational problem: incomplete visibility

- Multiple tools = fragmented asset inventory
- CMDB drift
- NAC-only visibility gaps
- OT/IoMT often out of scope
- Cloud/device identity mismatch

You can’t secure what you can’t see

At AI speeds, visibility is critical.

But you need more.



Risk assessment:

- Is it vulnerable?
- Is it exploitable?
- Is it exposed?
- Is it critical?

Traditional vulnerability prioritization misses real risk

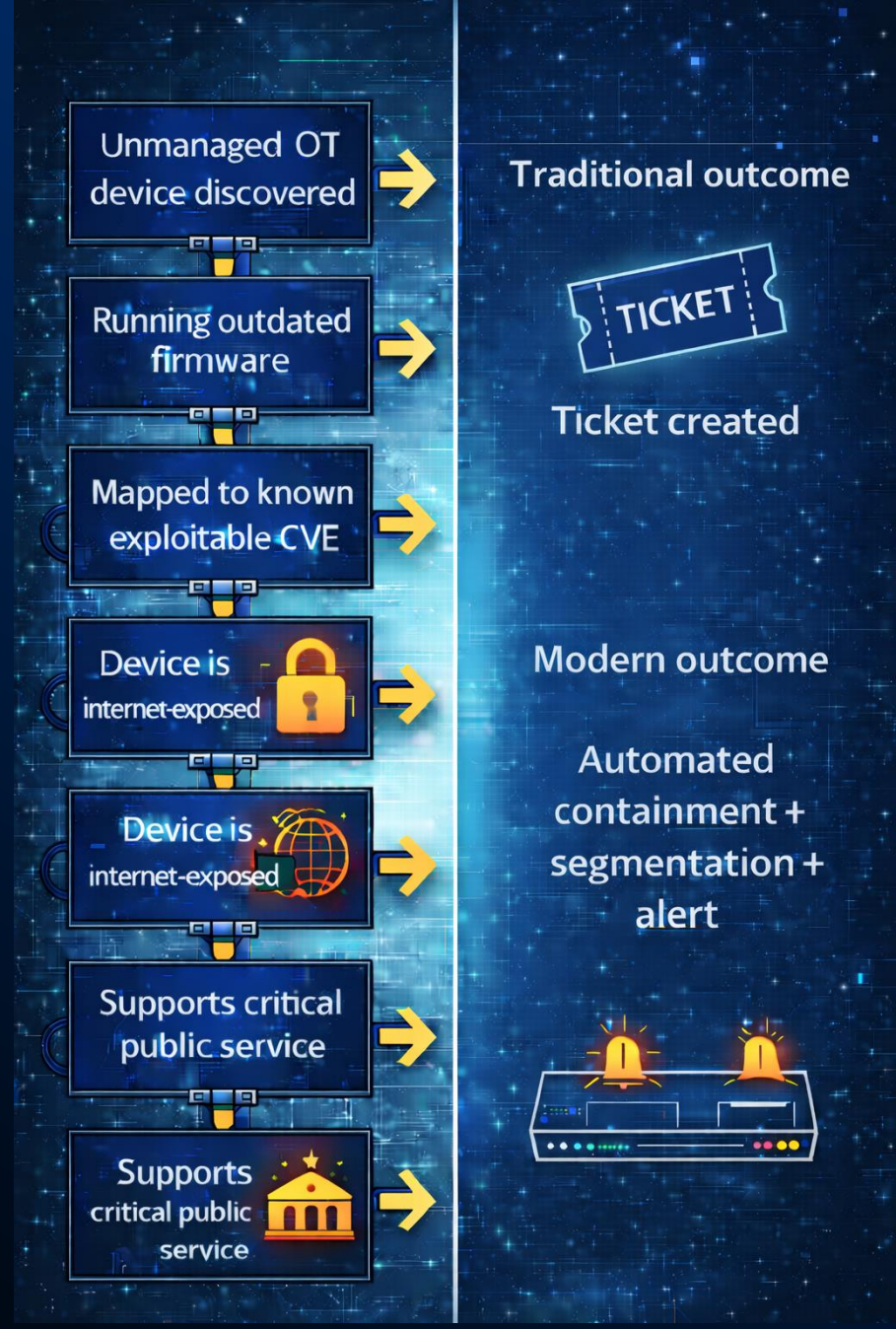
- CVSS inflation
- Patch fatigue
- Thousands of “critical” alerts
- No business context
- No exploit likelihood weighting

Risk scoring engine

- Weighted, policy-aware
- Time decay on stale data
- Continuous updates

Automate routines and focus on the threats that matter

- Reduce noise by correlating signals instead of adding new surfaces to monitor
- Automate low-risk actions to free analysts for high-impact investigations
- Prioritize real threats using context, not volume
- Integrate into existing workflows instead of requiring new consoles



Time + manual dependency creates an enforcement gap

- Discover risk
- Generate report
- Create ticket
- Wait

Visibility without enforcement is not security

Cybersecurity Enforcement Must:

- Turning risk insights into automated protective actions
- Applying policies consistently across every device, user, and network segment
- Shrinking the attack window by reducing manual steps
- Ensuring continuous alignment with Zero Trust principles
- Enabling adaptive response based on real-time risk scoring

Turn policy into protection

- **Translate risk signals into action**
  Automatically trigger segmentation, quarantine, access revocation, or policy updates based on risk context.
- **Apply controls everywhere risk appears**
  Enforce policies consistently across IT, OT, IoT, cloud workloads, and unmanaged devices.
- **Reduce attacker dwell time**
  Automated containment eliminates delays introduced by manual workflows and ticket queues.
- **Operationalize Zero Trust**
  Continuous verification only works when policies can be enforced dynamically across the network.
- **Adapt defenses in real time**
  Risk scoring, behavioral analytics, and threat intelligence must drive immediate changes to access and network posture.
- **The Outcome**
- Security moves from **detect and respond** to **detect, decide, and enforce automatically**.

Continuous risk reduction powered by AI

Canada’s public sector is a growing target

- Expanding attack surface
- Legacy infrastructure
- Critical services (healthcare, utilities, municipalities)
- Increased regulatory scrutiny
- Budget constraints

New KPIs that Measure Success

Final thoughts…

- AI has accelerated attackers; defense must match speed
- Visibility is foundational
- Risk assessment is more than severity; it's context
- Enforcement must be automated and adaptive

The goal is *measurable risk reduction*

They are always out there. They are always learning from each other, building on their successes and learning from their failures.

Visibility is survival. Context is strategy. *Automation is resilience.*

Let's connect on LinkedIn!
Rhonda Holloway,
Forescout Technologies


FORESCOUT®