IDC CIO SUMMIT · TORONTO · NOVEMBER 19, 2026

Before AI acts.

Readiness for the autonomous era.

Margie Sills · Director, Solution Engineering

External Use\General Business - Not Confidential

THE SHIFT

Everyone is heading toward autonomous IT.

Those who get there first will set the pace. Most leaders can’t yet say what ready means.

External Use\General Business - Not Confidential

INTENT VS. REALITY

The drift between intent and reality is where risk lives.

INTENT · WHAT SHOULD BE RUNNING

- Managed devices
- Baseline configurations
- Patched systems
- Active controls

REALITY · WHAT IS ACTUALLY RUNNING

- Unmanaged devices
- Drifted configurations
- Outdated, vulnerable systems
- Disabled or missing agents

DRIFT = RISK

Breach. Downtime. Regulatory exposure.

WHY: SILOS · STATIC PROCESSES · FRAGMENTED TOOLS · VELOCITY MISMATCH

External Use\General Business - Not Confidential

STORY 1 · OCTOBER 2026

No new vulnerability. Just the gap between policy and reality.

70,000+

firewalls compromised in the FortiBleed campaign

Attackers reused stolen credentials and guessed weak passwords.

Devices without MFA were the easy way in.

In some cases, attackers locked the real administrators out.

THE LESSON

The gap between intent and reality is the attack surface. See it live.

SOURCES: FBI AND U.S. SECRET SERVICE ADVISORY (OCT 6, 2026); SOCRADAR

External Use\General Business - Not Confidential

STORY 2 · OCTOBER 2026

Attackers tried PHP2Shell four days before the patch existed.

4 days

of attempted exploitation before the fix

Amazon saw the first attempts on October 17. Patches landed October 21.

Details leaked early, so the release had to be rushed.

CISA gave federal agencies three days to patch.

THE LESSON

The window between disclosure and attack is gone. Act in minutes.

SOURCES: AMAZON THREAT INTELLIGENCE; BLEEPINGCOMPUTER; CISA, OCT 2026

External Use\General Business - Not Confidential

STORY 3 · OCTOBER 2026

The attackers did not need a person. They used an application.

3 services

taken offline by ConnectWise on October 17

Stolen application credentials signed in to customers' Microsoft 365 tenants.

Applications sign in without MFA, so nothing challenged them.

In one tenant, an app gave itself Global Administrator.

THE LESSON

Guardrails decide what a stolen or runaway identity can do.

SOURCES: CONNECTWISE ADVISORY; HUNTRESS; TRADE PRESS, OCT 2026

External Use\General Business - Not Confidential

THE MAP

Four stages. One measure: how *fast* you manage drift.

01

Reactive

Drift happens. You react to the alert.

02

Proactive

Caught sooner. Still a response.

03

Preventative

Policy holds the line, at human speed.

04

Autonomous

Drift manages itself. Humans oversee.

MOST ORGANIZATIONS SIT BETWEEN REACTIVE AND PROACTIVE

External Use\General Business - Not Confidential

THE READINESS TEST

Five prerequisites for autonomy.

1

Real-time data

A live, trusted view of every asset and its state.

STORY 1

2

Immediate action

Detection closes the loop. Fixes reach everything at once.

STORY 2

3

Guardrails

Limits, staged rings, and automatic stop and rollback.

STORY 3

4

Auditability

Every action logged, explainable, and reversible.

5

Shared ownership

One picture Security and IT Ops both trust.

Score yourself 1 to 5 on each. Your lowest score is your first move.

External Use\General Business - Not Confidential

EARNING TRUST

Autonomy is earned task by task.

1 **AI recommends.**
It finds and ranks issues. Humans decide and act.

HUMANS DECIDE

2 **AI acts with approval.**
It prepares the fix and pauses before changing state.

HUMANS APPROVE

3 **AI acts within guardrails.**
Proven tasks run on their own, in rings, with rollback.

HUMANS OVERSEE

Patching may reach stage three in weeks. Privileged access may stay at stage two.

External Use\General Business - Not Confidential

YOUR NEXT MOVE

Find your lowest score.
That’s your first move.

Join the roundtable: Before AI acts, where do we draw the line?

External Use\General Business - Not Confidential