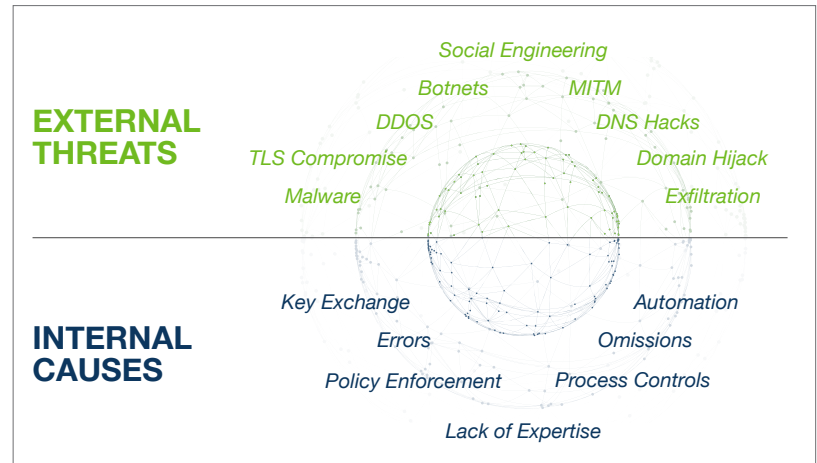# THE CHAIN OF TRUST IS BROKEN

DIGITAL BRANDS ARE EXPOSED TO INTERNAL AND EXTERNAL SECURITY RISKS

WHY DOES THIS PROBLEM PERSIST?

✘ *Organizational and system SILOs lack end-to-end control, visibility and automation*

✘ *Manual processes and legacy systems FAIL digital security compliance audits*

✘ *Certificate Authorities and SSL processes are vulnerable to COMPROMISE*

✘ *DNSSEC implementations FAIL due to mismanaged or missing DSKEYS*

✘ *TLS versions EXPOSE DATA to known exploits*

✘ *DNS security policies are UNENFORCEABLE*

EXTERNAL THREATS

Social Engineering
Botnets   MITM
DDOS   DNS Hacks
TLS Compromise   Domain Hijack
Malware   Exfiltration

INTERNAL CAUSES

Key Exchange   Automation
Errors   Omissions
Policy Enforcement   Process Controls
Lack of Expertise

DNS and TLS rely on a multi-part Chain of Trust vulnerable to people-dependent, error-prone processes. Data-in-motion is at risk with thousands of endpoints on multiple TLDs and hundreds to thousands of domains.
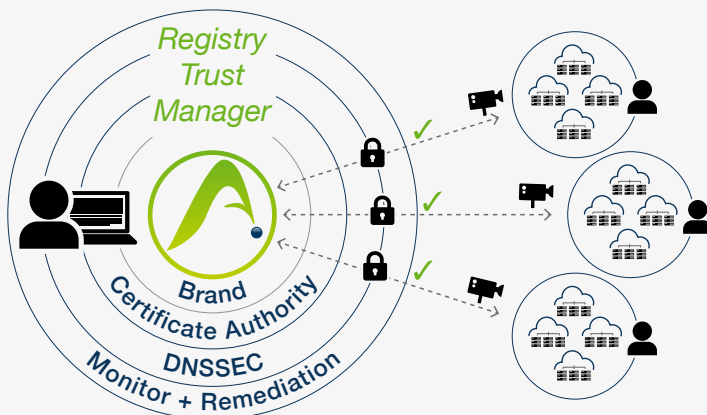
INTRODUCING THE REGISTRY TRUST MANAGER™ (RTM)

A SECURE AND TRUSTED NETWORK

Your Brand Registry is a trusted, authentic space with superior security capabilities over generic TLDs. RTM uses your Brand Registry to encrypt and authenticate connections to every enabled network endpoint. Brand TRUST is assured with data-in-motion protection.

Registry Trust Manager

Brand
Certificate Authority
DNSSEC
Monitor + Remediation

RTM FEATURE SUMMARY

✓ *Automated, trust certificates at each endpoint*

✓ *DNSSEC management automation*

✓ *Connection monitoring and remediation*

✓ *Policy based DNS security enforcement*

✓ *Protection from people errors/omissions*

✓ *Cost effective and massively scalable*

Control Systems to authenticate connections and ensure data-in-motion encryption