

You've been... CrowdStruck

Lesson's Learned from July 19th, 2024





TOMASZ HABERNY

Squad Lead CrowdStrike Engineering

**DEUTSCHE TELEKOM CYBER SECURITY
AUSTRIA GMBH**

Rennweg 97-99
1030 Vienna, Austria
tomasz.haberny@telekom.com



SANDRA VRDOLJAK

Incident Response & CrowdStrike Engineering

**DEUTSCHE TELEKOM CYBER SECURITY
AUSTRIA GMBH**

Rennweg 97-99
1030 Vienna, Austria
vrdoljaks@telekom.com

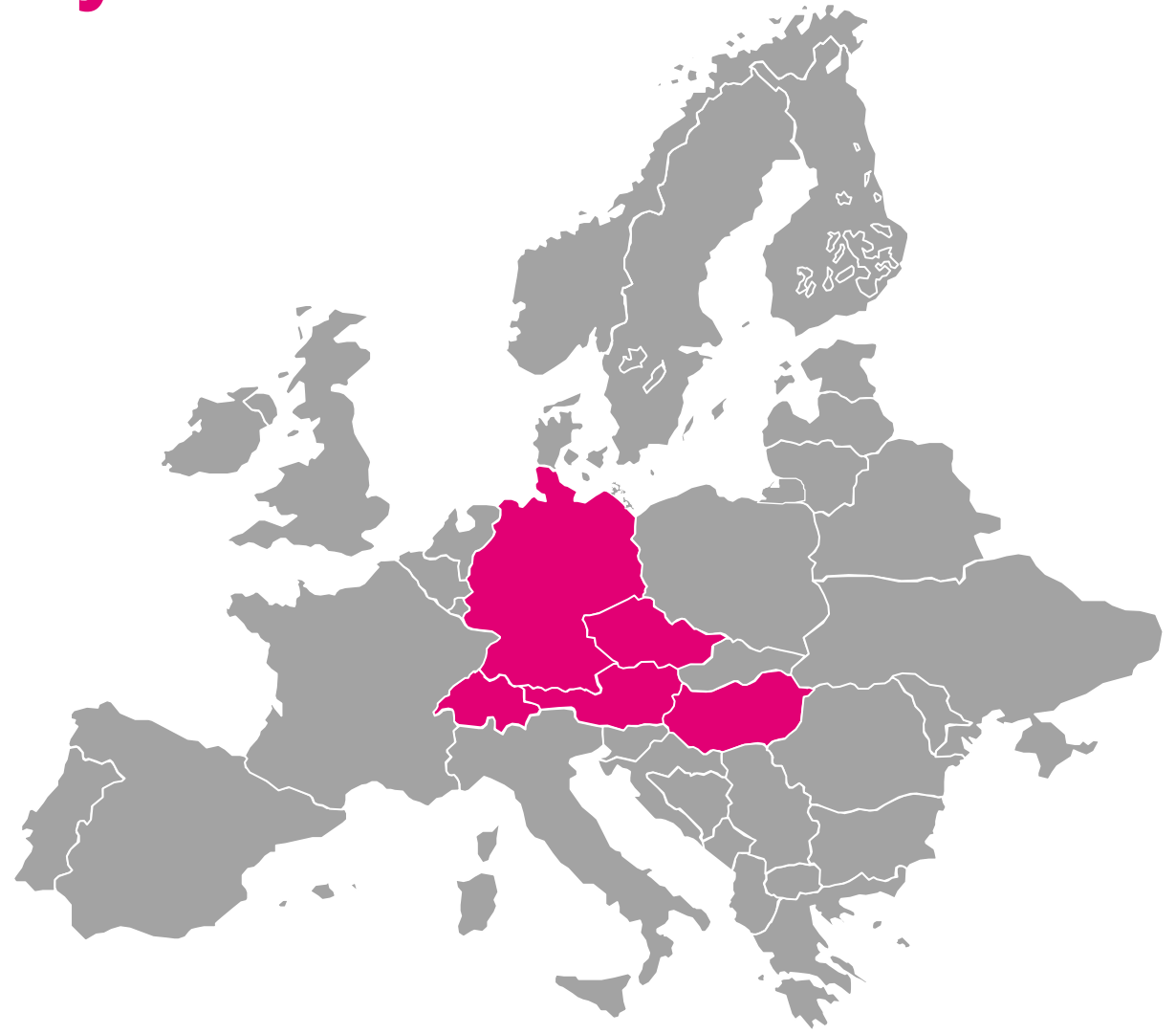
Deutsche Telekom Security

Securing **Deutsche Telekom**
and its subsidiaries

Directly providing (managed)
security services **to customers**

Five Security Operations Centers
in Europe (DE, AT, CH, HU, and CZ)

Over **1.600** information security
specialists – and hiring ;-)

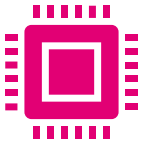


A Brief History on Endpoint Protection



1980s – 2010s: AntiVirus Era

- Signature- & heuristics-based detection
- Malware stored on disk
- Began the cat & mouse game of detection vs. obfuscation



2010s onwards: Shift in Attacker Tactics

- Attackers move away from disks
- Rise of fileless malware – runs only in memory
- Surge in living off the land binaries (LOLBin) abuse



Image created by DALL-E

Endpoint Detection & Response



Image created by DALL-E

Enter: Endpoint Detection & Response (EDR)

- The term EDR was coined in 2013 by Gartner
- It describes software suites that allow the analysis of massive amounts of data on **endpoints**, to **detect** threats, and to **respond** if necessary
- EDR solutions observe all activities on a system and focus on **detecting suspicious behavior at run-time**, rather than suspicious files
 - Shift from scanning files to monitoring behavior in volatile memory – can also detect *fileless* malware and LOLBins!
 - “Malware can hide, but it must run”

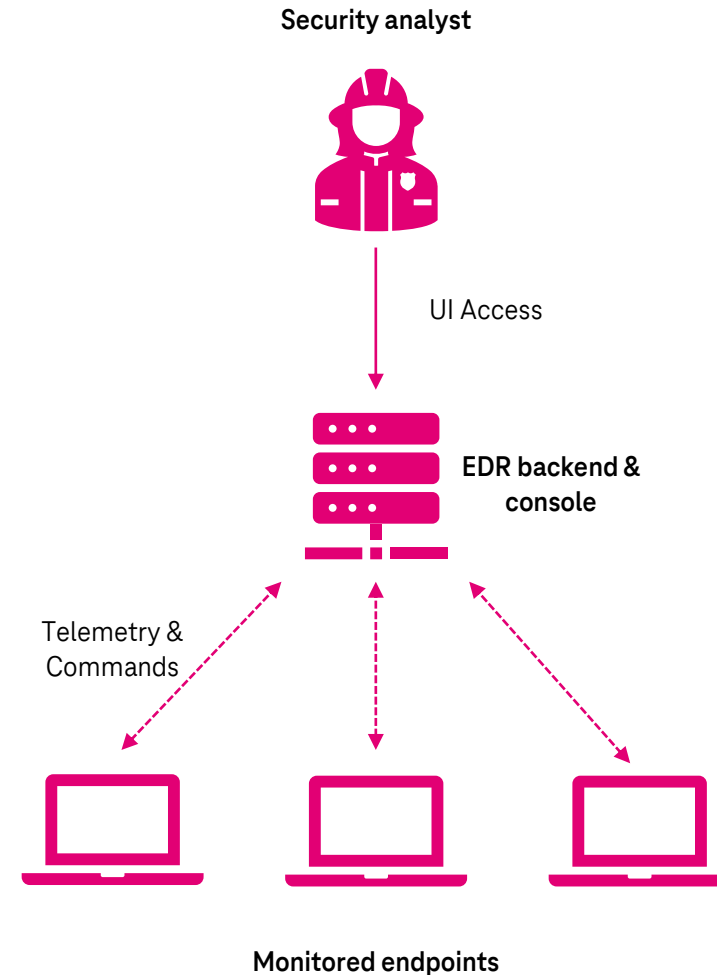
What do EDR solutions monitor?

Security-relevant events – for example:

- Process-level **network activity** (*established network connections, DNS requests, ...*)
- **Process executions**
- **File creations** (*especially archives & executables*)
- **Admin tool usage** (*PowerShell, CMD, bash, ...*)
- Usage of **removable media**

Crucially, there is an **R** in **EDR**:

- EDRs can **block suspicious processes & activities**
- Additionally, they allow **host isolation**, as well as **direct access to endpoints**



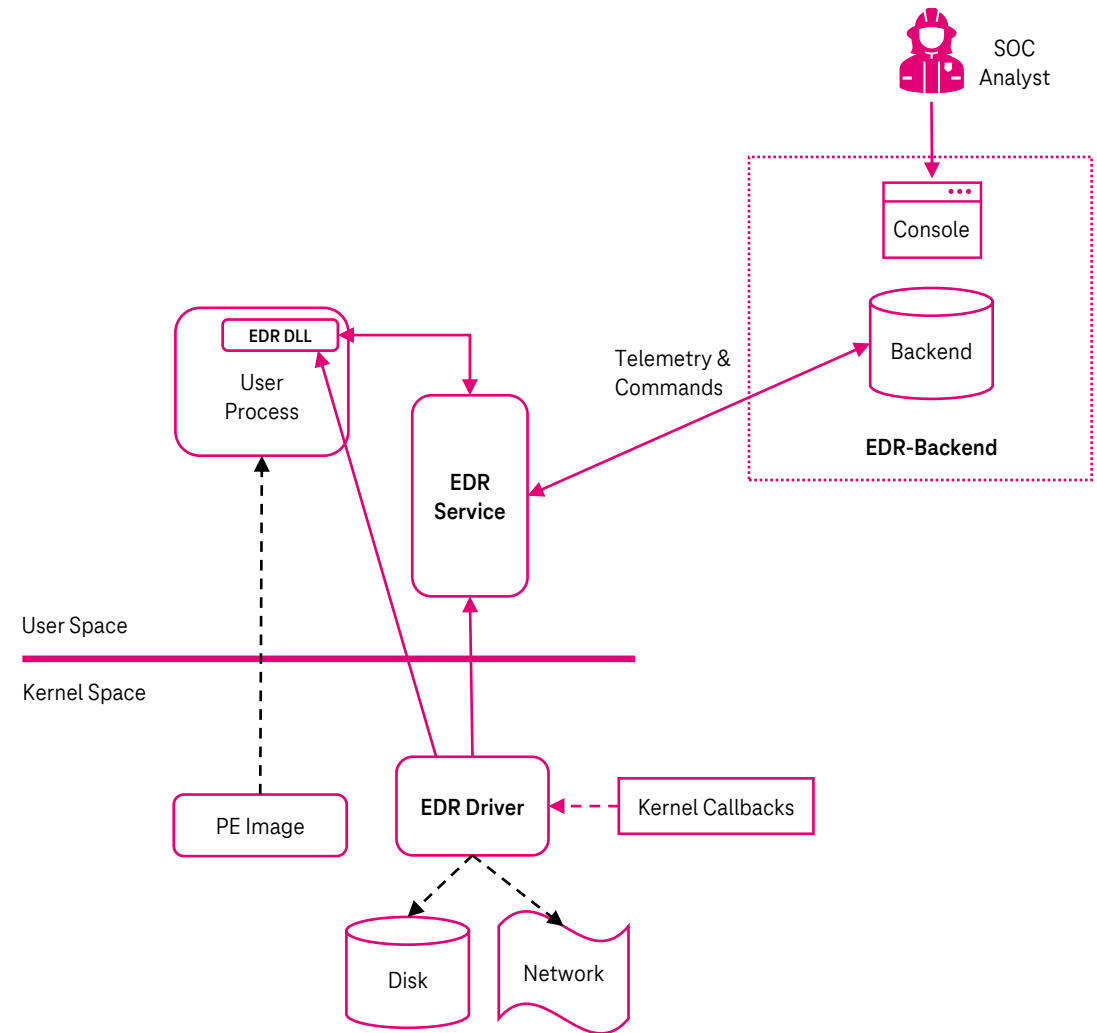
How does an EDR work?

Components

- User space component (*service*)
 - User process component (*executable*)
 - Kernel space component (*driver*)
- On endpoint

- Backend to receive and analyze telemetry
- Console for analysts/responders

Usually in the cloud



A simplified EDR architecture for Microsoft Windows

The Kernel Space Component

Why operate in Kernel space?



Visibility/Telemetry: Some data can only be collected at kernel level



Enforcement: Inline blocking of activities



Tamper Protection: Protecting against tampering with the security product itself



Performance: Processing security decisions in the kernel is more efficient than in user space



EDR products **must operate on this level...** not doing so would **render the product much less effective**



July 19th, 2024

The day we gave up on sleeping

Counting the Costs of a Global IT Outage

A “historic” tech failure alarmed investors, after a security update caused problems for Microsoft devices and services, and took down businesses worldwide.

CrowdStrike file update bricks Windows machines around the world

Falcon Sensor putting hosts into deathloop - but there's a workaround

Simon Sharwood

Outage for Microsoft Users Knocks Out Systems for Airlines and Hospitals in Chaotic Day

Companies across the world reported disruptions, citing technical issues from a cybersecurity software update.

Published July 19, 2024 Updated May 5, 2025

Sydney, Today

CrowdStrike outage sparks global chaos with airline, bank and other disruptions

than 8,000 were delayed in the U.S.



Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Mass IT outage affects airlines, hospitals, media and banks

19 July 2024

Hafsa Khalil
BBC News

Tiffanie Turnbull
BBC Sydney

re outage



Sign in

Home News Sport Busir

NEWS

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | UK | Business

a tech outage that t

Share Save



MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVE

TECH

How a software update from firm CrowdStrike caused one of the world's biggest IT blackouts

PUBLISHED FRI, JUL 19 2024 8:21 AM EDT | UPDATED FRI, JUL 19 2024 11:42 AM EDT



Ryan Browne
@RYAN_BROWNE

SHARE f X in

Timeline of Events



04:09 UTC/06:09 CEST: Faulty CrowdStrike content update released

04:09 UTC: Immediate outages reported in **Microsoft Azure**

05:27 UTC: CrowdStrike **update reverted**

06:00 UTC: **Unofficial remediations** being shared on Reddit, X, ...

06:30 UTC: **Official remediation** published by CrowdStrike

06:48 UTC: Outages reported in **Google Compute Engine (GCE)**

08:00 UTC: **Airlines, hospitals, banks, and critical infrastructure** affected

09:45 UTC: CrowdStrike CEO George Kurtz confirms that the issue was fixed and that **outages were not the result of an attack**

Windows endpoints that were online between 04:09 and 05:27 UTC were affected – systems entered a boot loop or booted into recovery mode.

Linux and Mac endpoints were not affected.

Official Remediation Support by CrowdStrike



Asset Identification

- CrowdStrike released **updated Falcon dashboards** to help identify affected Windows endpoints
- **Goal:** help **prioritize** recovery workflows



Remediation Instructions

- Administrators advised to **boot into Safe Mode or WinRE**
- Manually **delete the faulty channel file**

```
%WINDIR%\System32\drivers\CrowdStrike\  
C-00000291*.sys
```



Cloud Remediation

- Some devices could **auto-recover** after several reboots
- This **Cloud Remediation** was improved and pushed to all environments by July 23rd

Challenges and Pitfalls



Unofficial Workarounds

- Ad-hoc fixes resulted in **non-functional CrowdStrike sensors**



Always-On VPNs

- **Impeded** cloud remediation



BitLocker

- **DCs** containing BitLocker keys non-functional
- BitLocker **prevented access** without the 48-digit key



Cloud-Based VMs without Safe Boot

- VMs in Azure, AWS, and GCP **often lack Safe Mode / WinRE**

Pitfalls present during the Cleanup Phase

- **Rotating** BitLocker keys
- **Repairing** CrowdStrike installations
- **Removal** of temporary workarounds/automations



Global Consequences

- ~**8.5 million** Windows devices affected around the globe
- Over **7000 flights cancelled**, resulting in **\$550+ million losses** for airlines
- Significant **impact in the health industry** (emergency operations, hospital operations, ...)
- Interruptions and failures in **banking and payment systems**
- Estimated global losses are estimated to **exceed \$10 billion**
- News dissemination was disrupted, resulting in **media outages**
- Recovery proved challenging as **manual intervention was required** for many systems





CrowdStrike Internals

How could this happen?

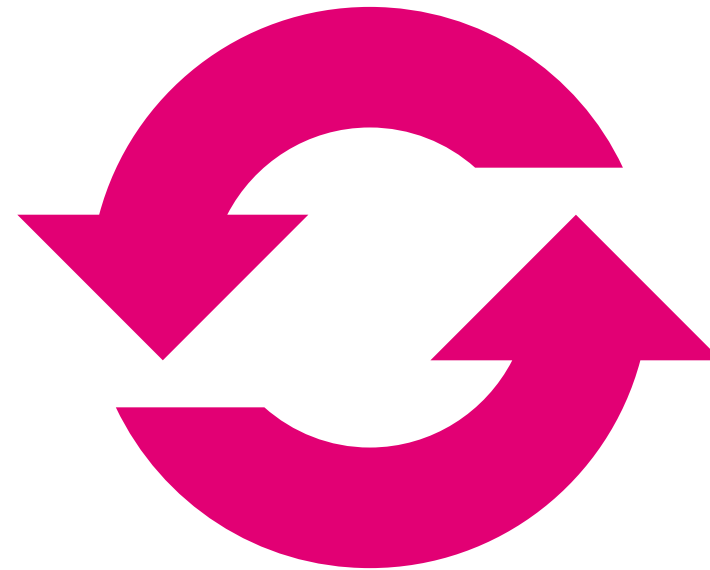
CrowdStrike Updates

Two Types of Updates

- **Software Upgrades (Sensor Versions)**
 - Upgrades the **Falcon Sensor** binary
 - Upgrades are **controllable**
 - Typically follow **version control and QA before deployment**
- **Content Updates (Channel Files)**
 - Include updates to **detection logic, configuration templates, ...**
 - Delivered silently, and **not controllable**
 - We'll talk about **QA** for those

Implication

- Content updates are lightweight, **but can affect runtime behavior**



The Error in Detail

Channel File n

- Fields 0 – 19: <value> or %
- Field 20: %

Channel File 291

- Fields 0 – 19: <value> or %
- Field 20: <value>

The Error (simplified)

```
// Erroneous memory allocation: length == 20
char dest[20];
memcpy(dest, src, 20);

// Out-of-bounds access: template.length() == 21
for (int i=0; i < template.length(); i++) {
    if (template[i] == '%') {
        continue;
    }
    validate(dest[i]);
}
```

Template files have **21 fields**... with Channel File 291, **field 20** was assigned an **actual value** for the first time.

Fun fact: The corresponding Channel Template was rolled out in **Feb 2024**

Field index 20 is dereferenced for validation but **has never been allocated**. Until **Channel File 291**, the value for this field was a **wildcard (%)**, which did not require validation, **therefore the field was never dereferenced before**.

...remember how this is **embedded in the Kernel module?**

A Simple Error – With Global Impact



A relatively simple error led to global outages

- No staged deployment, no pre-release validation at scale
- The update was simultaneously applied **silently across millions of systems**
- The error was in the **Kernel module**

This responsibility lies with CrowdStrike



But there's a deeper problem

- Modern Kernels, including Windows, offer **no safe mechanism for correcting this once deployed**
- Kernel-mode memory faults **can't be easily hotfixed or remotely recovered**
- Crashes often require **physical intervention**

**Silver Lining: This has
attention now**



The Aftermath

What lessons can we learn from this?

CrowdStrike's Quality Assurance Changes



QA Enhancements

- ✓ **Dogfooding:** Sensors now run internally across diverse environments **before public release**
- ✓ **Expanded Quality Control:** More **extensive tests** for content updates
- ✓ **Endpoint Health Monitoring:** Real-time telemetry on **sensor health**
- ✓ **Feedback Loops:** High-priority support cases now **feed into staging and validation before release**



Content Update Deployment

- ✓ **Staged Rollouts:** Content updates are **not pushed globally at once** – rollout occurs in waves
- ✓ **Staggered Deployment:** Not all Falcon-clouds and customers **receive updates at the same time**
- ✓ **Customer Control:** Organizations now have **more granular options** for deferring or approving content updates before deployment

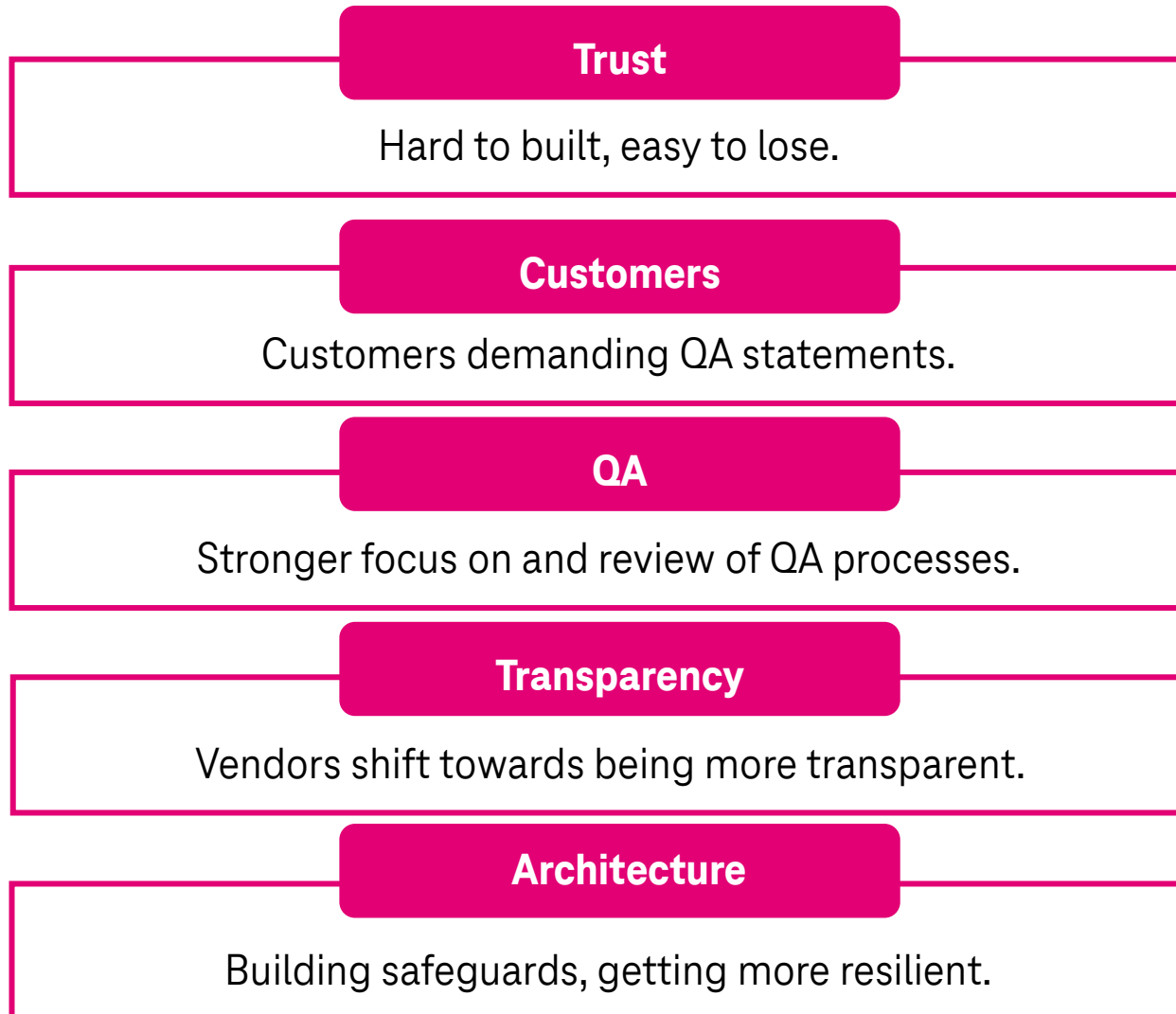


Architecture Enhancements

- ✓ **CrowdStrike Sensor Safe Mode:** Sensor can now detect sensor-related system crash loops and switch to safe mode

Most importantly: CrowdStrike is now way more transparent

Impact for EDR/SaaS vendors in general?

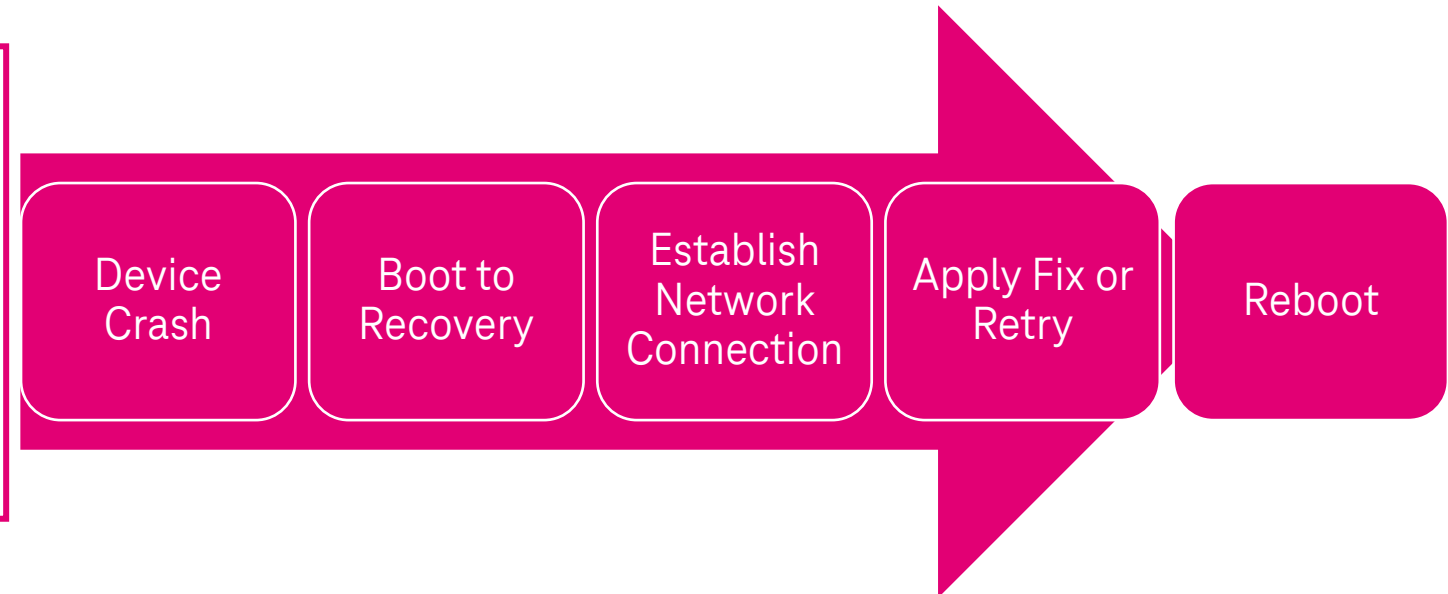


2010: McAfee „5958 DAT Update“

Microsoft - Quick Machine Recovery [1]

Overview

- Part of **Windows Resiliency Initiative**
- Windows 11 24H2 with August 2025 KB
- Feature is **customizable**
 - Pre-populated network credentials
 - Remediation scanning interval
- Microsoft pushes fix remotely



[1] <https://learn.microsoft.com/en-us/windows/configuration/quick-machine-recovery/>

What Measures can you take Yourself?



Hold Vendors Accountable

Transparent **QA processes**, **visibility** into update pipelines, and **rollback** mechanisms



Stay Calm Under Pressure

In crises, the instinct to “*just do something*” can cause **more harm than good** – **Act deliberately**, avoid *headless chicken* mode



Strengthen Your Own Readiness

Revise and test your **Business Continuity Management (BCM)** and **Disaster Recovery (DR)** plans regularly, and track your dependencies – **don't discover gaps during the real thing**

**This applies to all
crises – no matter the
cause**

Final Notes

EDRs aren't perfect – but still critical

- Like any software, **EDRs can fail** – this time it was CrowdStrike, but **it could have been any vendor**
- Despite this, EDRs remain the **most cost effective and impactful defense** in modern environments
- Yes, they can be bypassed – but that **doesn't negate their value** in detection and response

The real takeaway: **we shouldn't abandon EDRs**, we should make sure **the ecosystem learns from this**



Image created by DALL-E

Questions & Discussion