INFOSERV360°

TrendAI™
AI Fearlessly

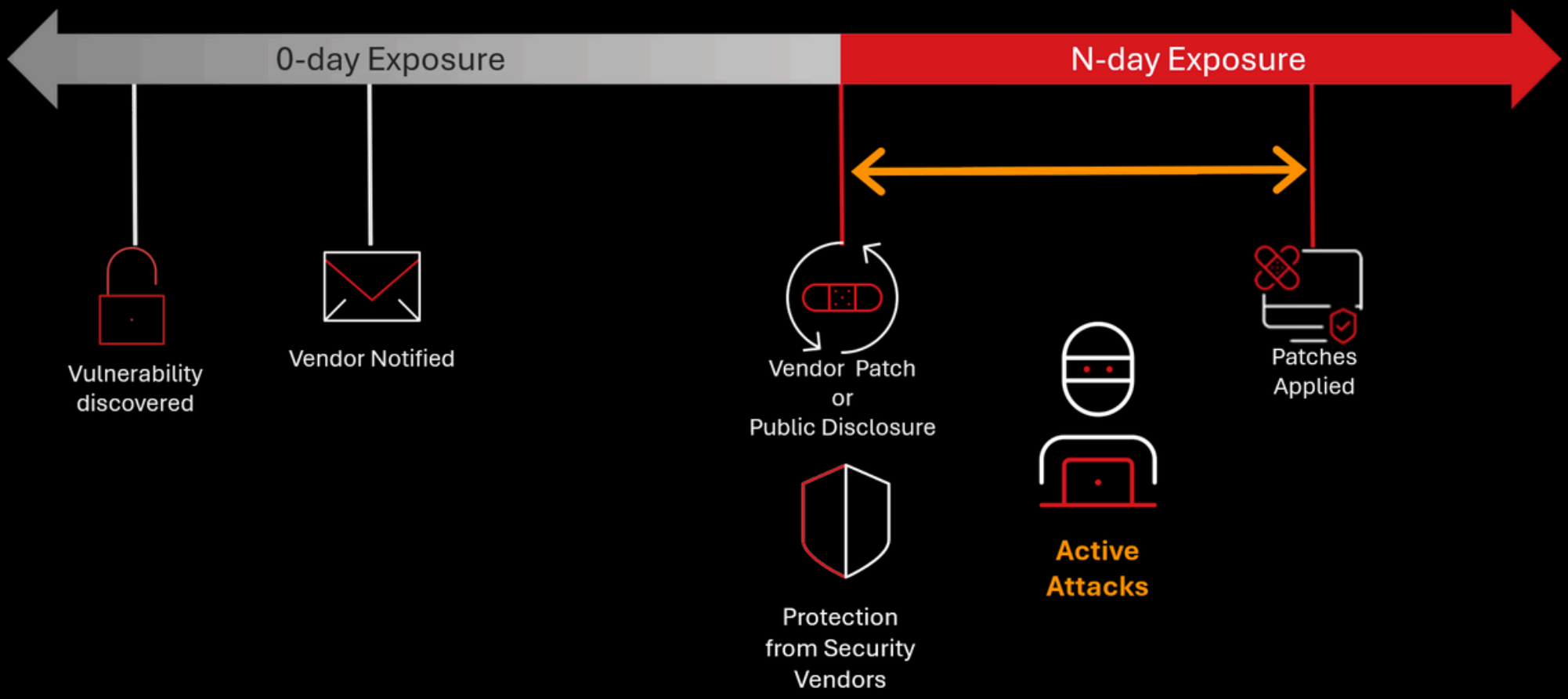
Ahead of the Patch

how we helped a bank stop waiting on patch cycles to close its exposure window

Case Study - Banking Industry

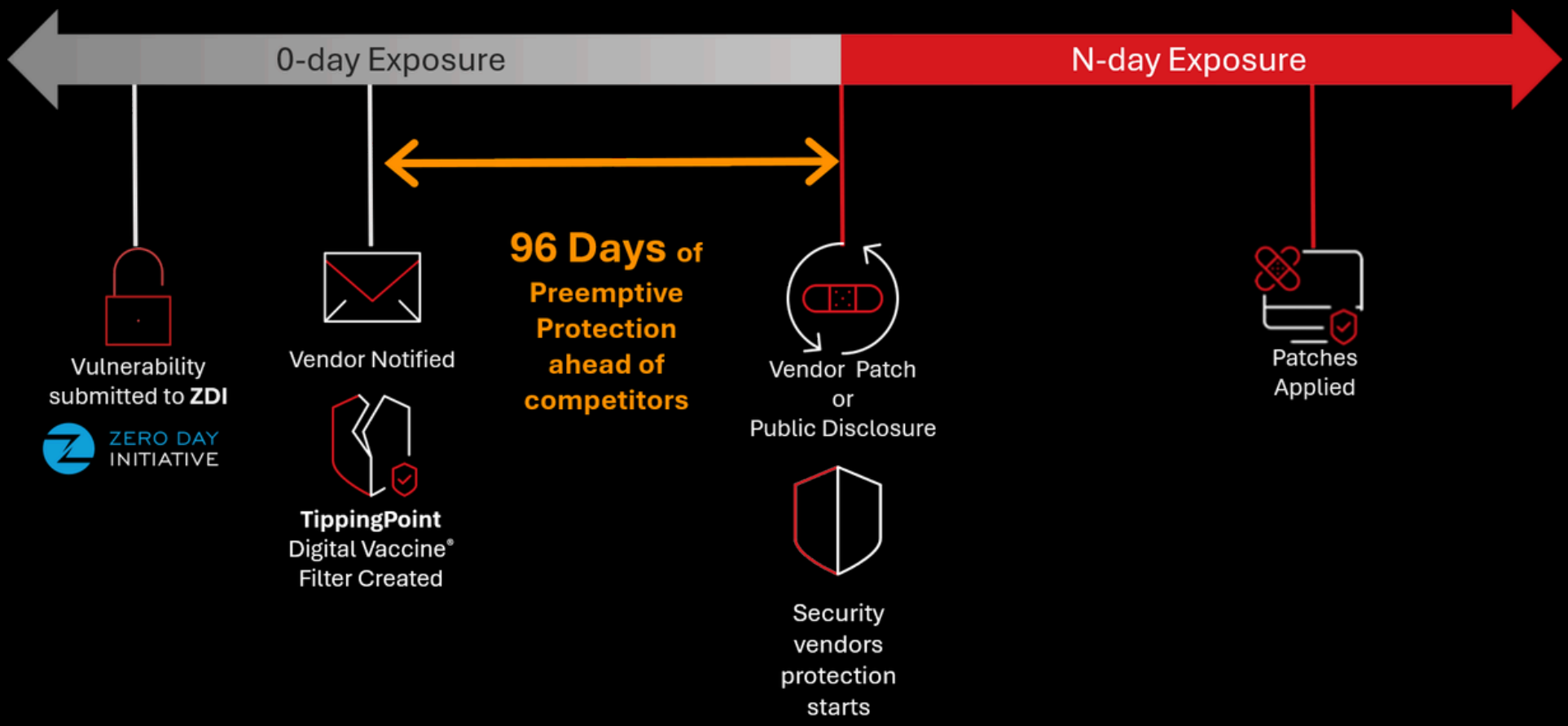
Most security starts too late.

the industry waits for public disclosure. By the time a CVE is announced, the flaw has been alive for months, and you still have testing and change approval ahead of it.



Patch the risk, not the server.

deep security inspected traffic at the host and blocked the exploit before it reached the vulnerable code.



What it is already blocking.

every recommendation the platform raised against the estate has been reviewed and assigned. Following are some of the threat families patched in the live rule set.

Log4Shell
Apache Log4J
Remote Code Execution

Spring4Shell
Spring Framework
Remote Code Execution

Zerologon
NetLogon
Privilege Escalation

PetitPotam
DCERPC EFSRPC
Over SMB

Ransomware
File-Rename Activity
Over Network Share

Shellcode
Suspicious Execution
On Client & Server

Apache Struts
Multiple OGNL
Injection Paths

SharePoint
Deserialization of
untrusted data

coverage across

RHEL 7 · RHEL 8 · RHEL 9 · Windows Server 2016 · Windows Server 2019 · Windows Server 2022 · Windows Server 2025

The Partnership

support & professional services are our cornerstone, by embracing teamwork and strong partnerships we aim to solve problems effectively.

DIGITAL BANK | MANAGER IT INFRASTRUCTURE

“I truly appreciate INFOSERV360° team’s continued support and strong work ethics (throughout the project). We look forward to receiving the same level of support and commitment in the future.”

Case Study - Banking Industry

INFOSERV360°

TrendAI™
AI Fearlessly