Putting CICS on the SIEM Radar with HTAC

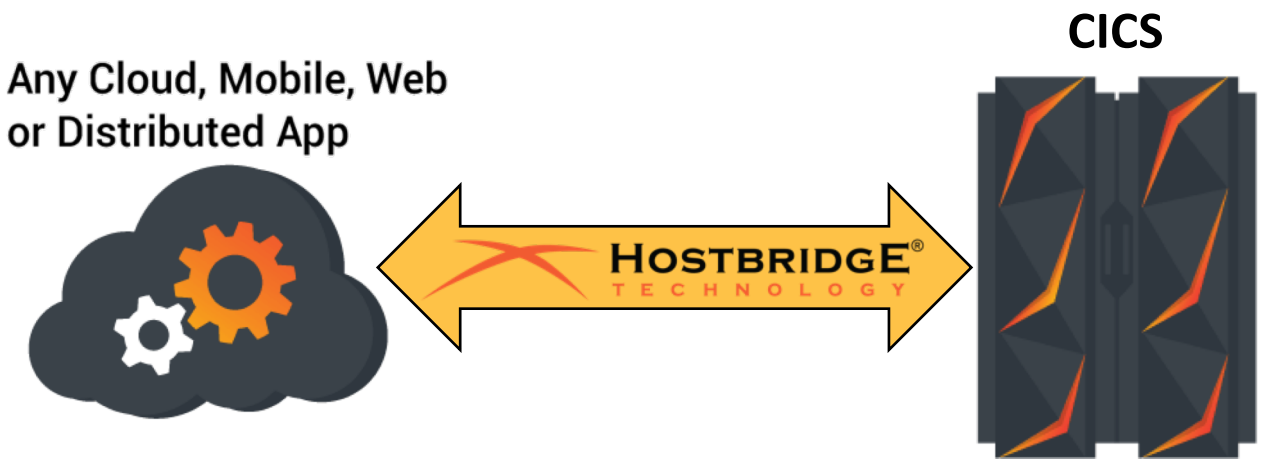
Russ Teubner, Co-founder & CEO

HOSTBRIDGE®
TECHNOLOGY

HostBridge in Brief

High-fidelity, precision integration for CICS & z/OS

- ✓Founded in 2000
- ✓Obsessed with performance
- ✓Exploit what's already "in the box" (no application changes)
- ✓Leverage industry standards
- ✓***Innovate and do the hard stuff***



IBM Business Partner

Representative Customers

HOSTBRIDGE® TECHNOLOGY

What is HTAC?

HOSTBRIDGE® TECHNOLOGY

HostBridge Transaction Analytics Connector (HTAC)

✓For enterprises with mobile, web or cloud applications that are supported by CICS on the back-end

✓HTAC allows SIEM platforms to capture end-to-end analytic data:

- From point-of-origin
- Up to and including CICS transactions

✓Addresses the SIEM “visibility gap” when CICS is involved

✓***Puts CICS on the SIEM radar screen!***

Definitions

HOSTBRIDGE® TECHNOLOGY

✓ splunk>

- Splunk is a leading SIEM software platform for searching, monitoring, and analyzing machine-generated big data, via a web-style interface.
- Splunk captures, indexes, and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards, and visualizations.
- Splunk is used for application management, security and compliance, as well as business and web analytics.

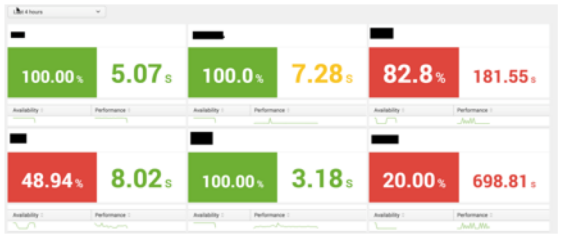
- Splunk is being used by a significant number of our customers.
- **<u>However, for most of them, Splunk and CICS have never “met”!</u>**

The Need for HTAC

HOSTBRIDGE® TECHNOLOGY

Cloud, mobile & other distributed apps

SIEM Dashboard



Complete, end-to-end visibility!

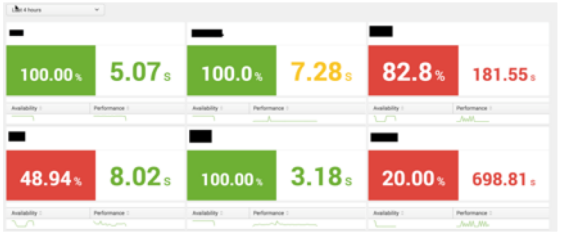
The Need for HTAC

HOSTBRIDGE® TECHNOLOGY

Cloud, mobile & other distributed apps

CICS

SIEM Dashboard



Partial visibility

DEAD END

?

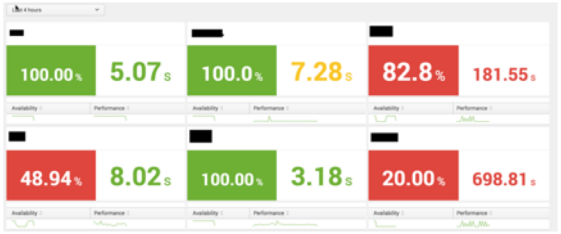
The Need for HTAC

HOSTBRIDGE® TECHNOLOGY

Cloud, mobile & other distributed apps

CICS w/ HTAC

SIEM Dashboard



Full visibility

HTAC exploits CICS Transaction Tracking

CICS TT provides a "framework" for correlating work that occurs inside CICS.

But, there is no way to associate information:

- ✓From an HTTP request with a Transaction Group
- ✓Sent via a CTG/EXCI request with a Transaction Group
- ✓Received with a socket request with a Transaction Group

CICS TT is therefore a <u>partial solution</u> that doesn't let CICS workload get on the SIEM radar.

✓***HTAC exploits CICS TT infrastructure to solve this problem!***

HTAC initial version focus

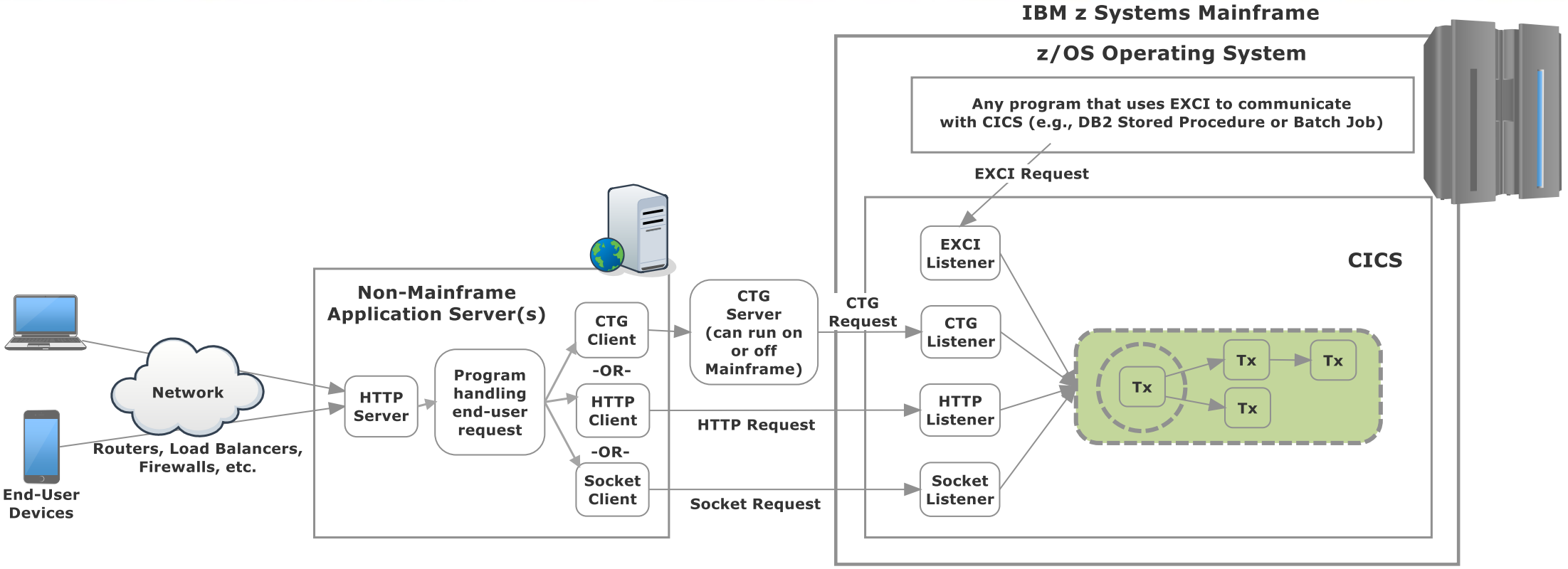
HOSTBRIDGE® TECHNOLOGY

- ✓Workload sent to CICS via:
  - HTTP
  - CTG / EXCI
  - Sockets
- ✓Splunk as the SIEM
- ✓CICS-based emitter(s) for rapid POC projects and testing
- ✓Syncsort Ironstream® support for highly-scaled CICS environments

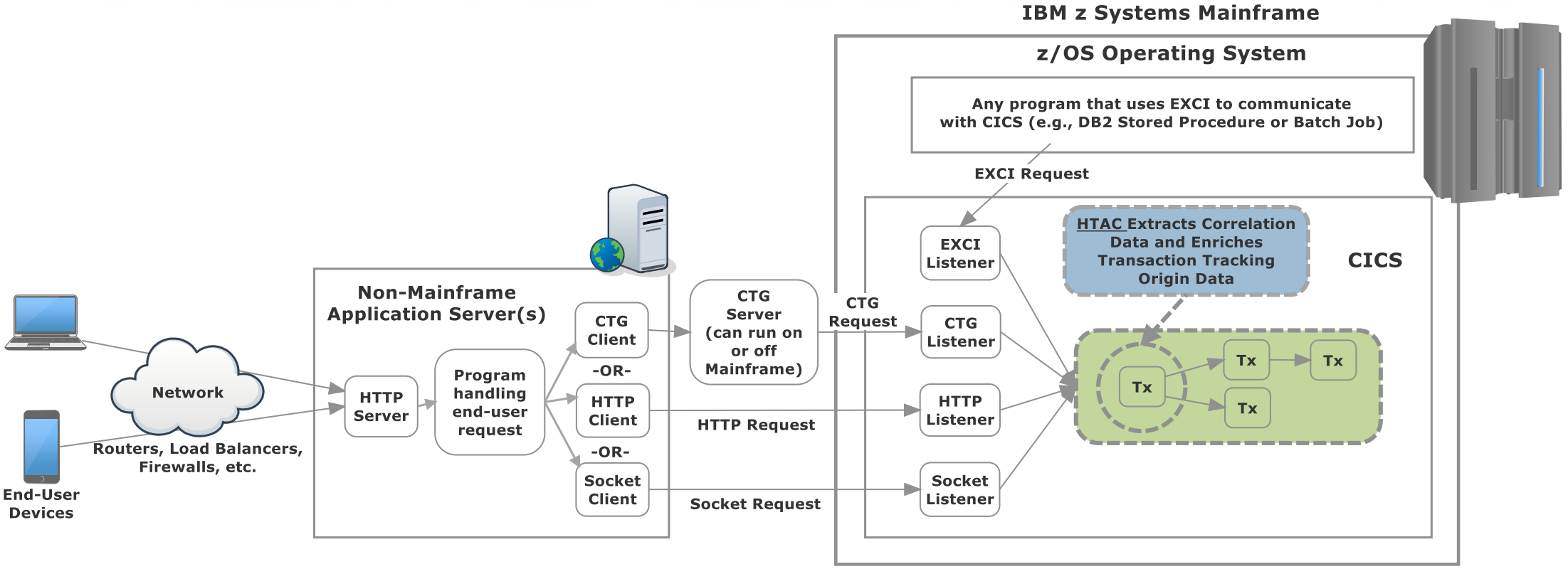
splunk>

syncsort

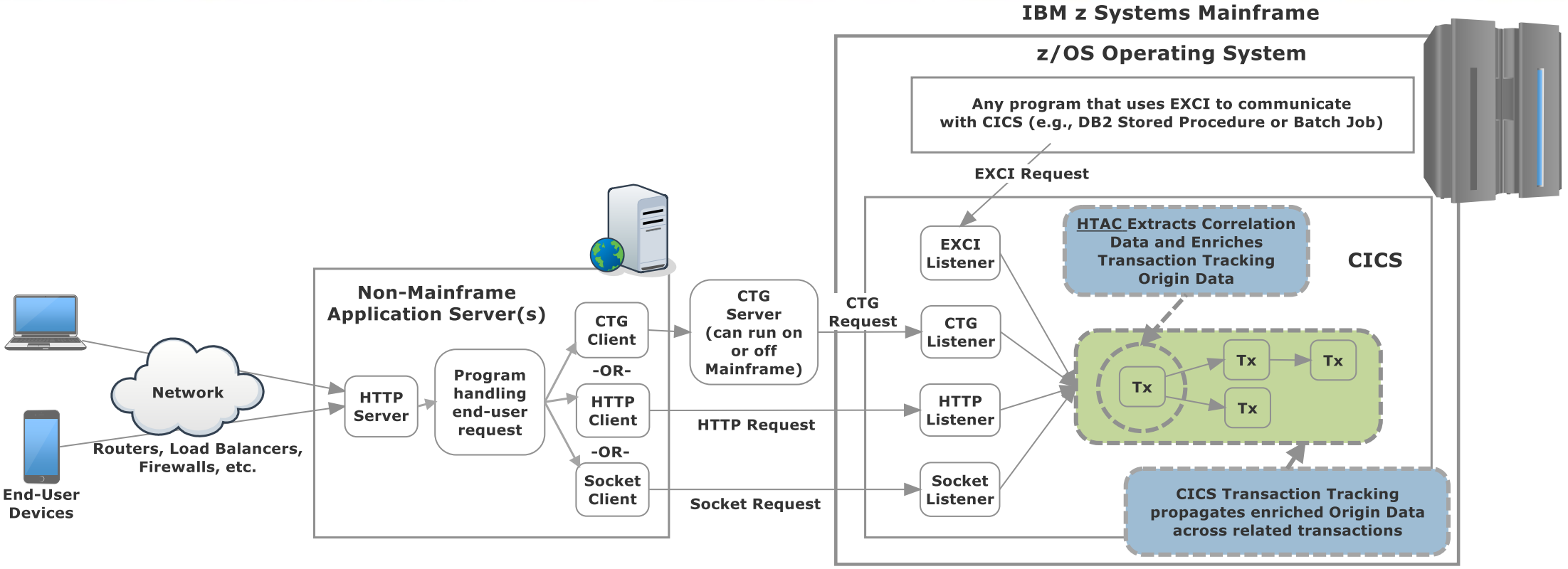
HTAC Operating Environ.



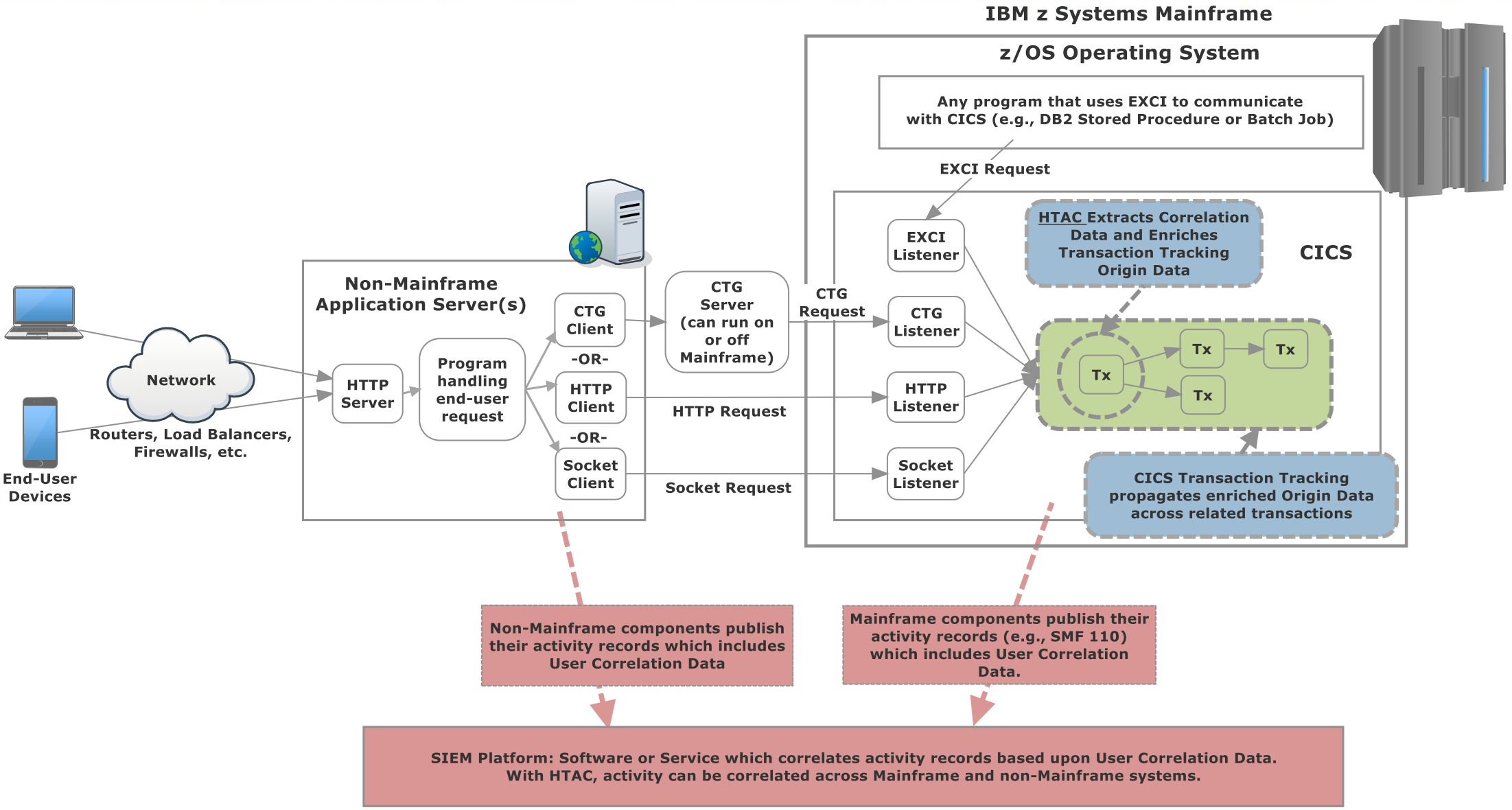
HTAC Operating Environ.



HTAC Operating Environ.

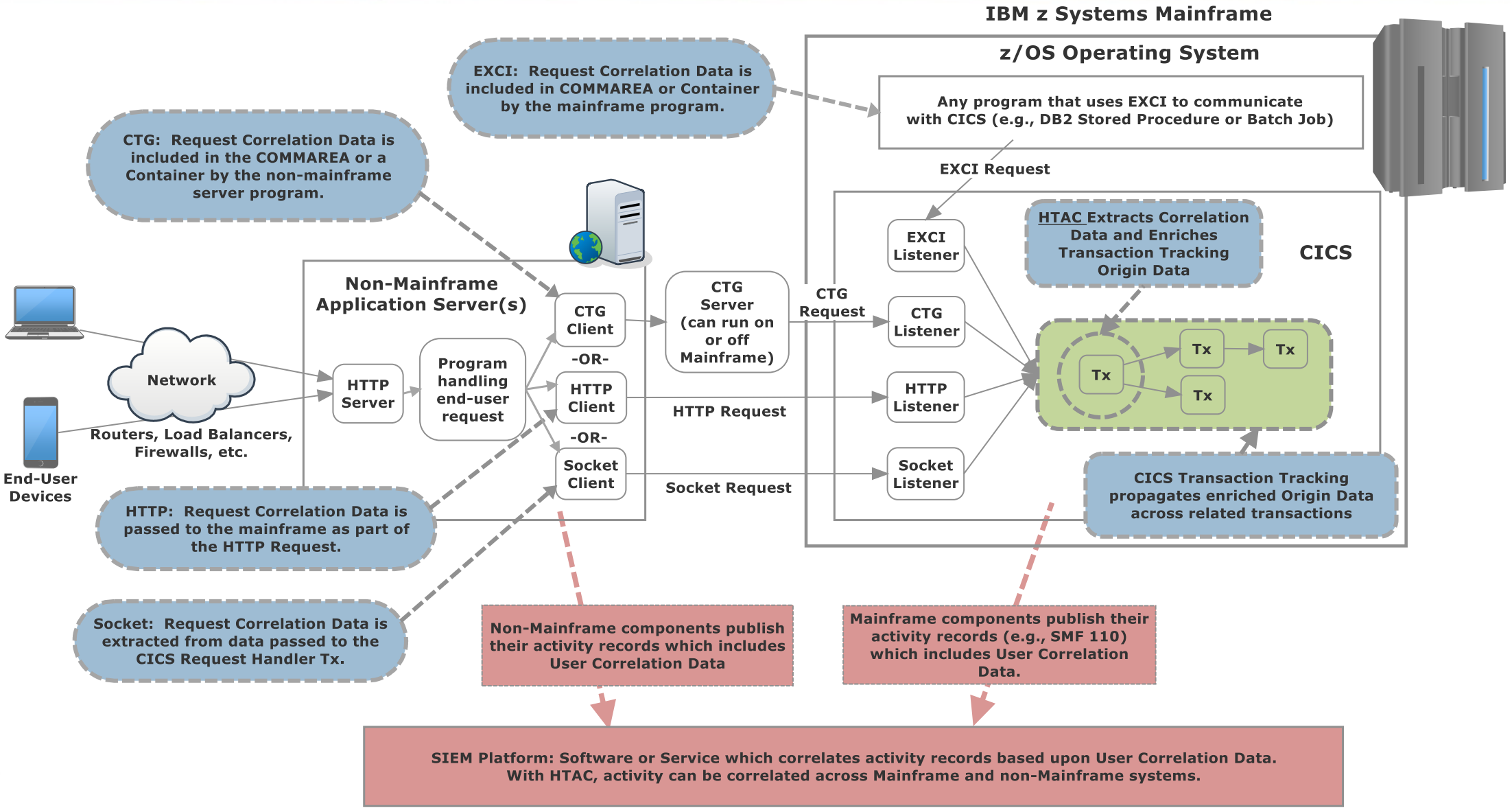


HTAC Operating Environ.



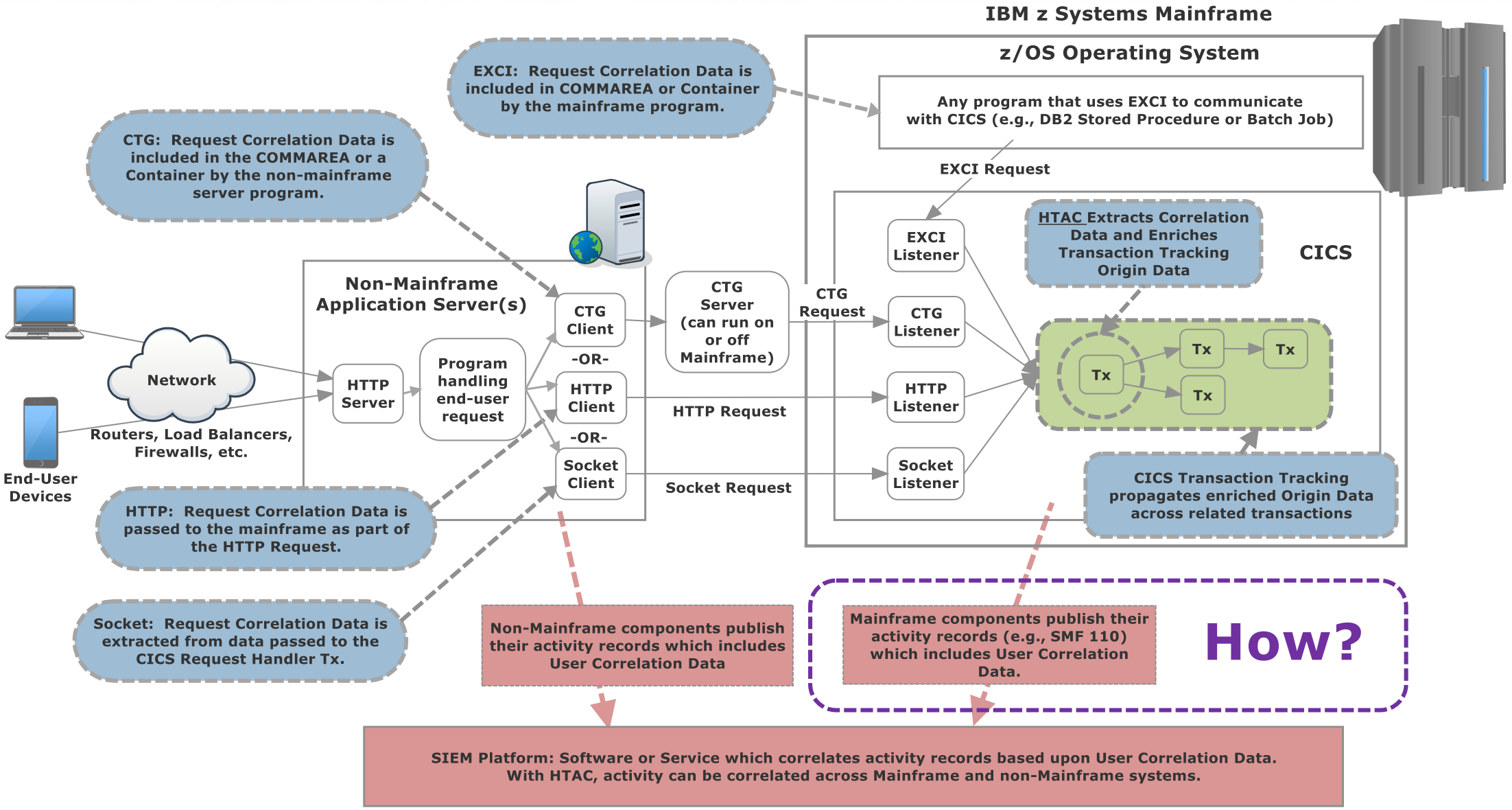
HTAC Operating Environ.

HOSTBRIDGE® TECHNOLOGY



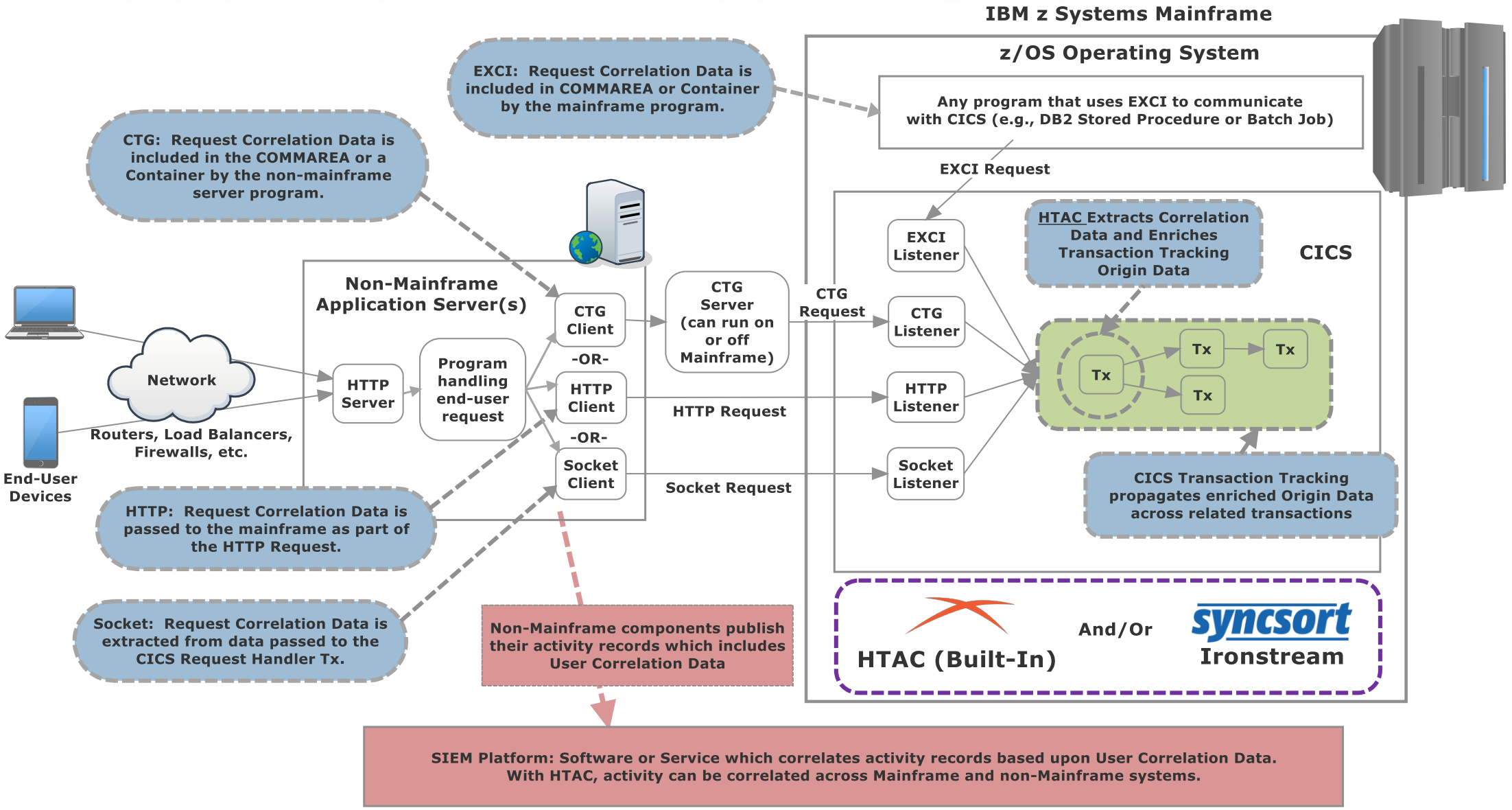
HTAC Operating Environ.

HOSTBRIDGE® TECHNOLOGY



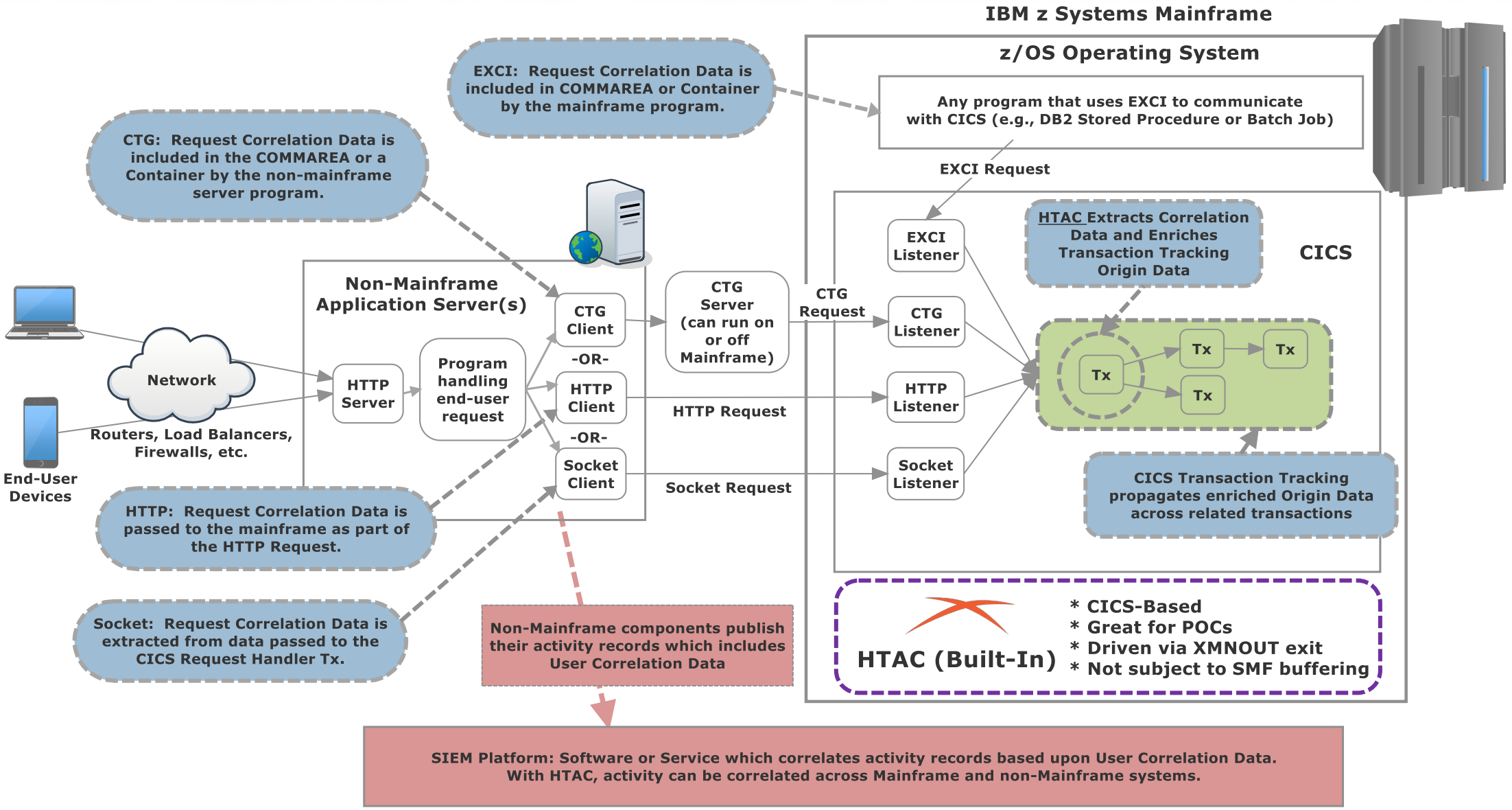
HTAC Operating Environ.

HOSTBRIDGE® TECHNOLOGY



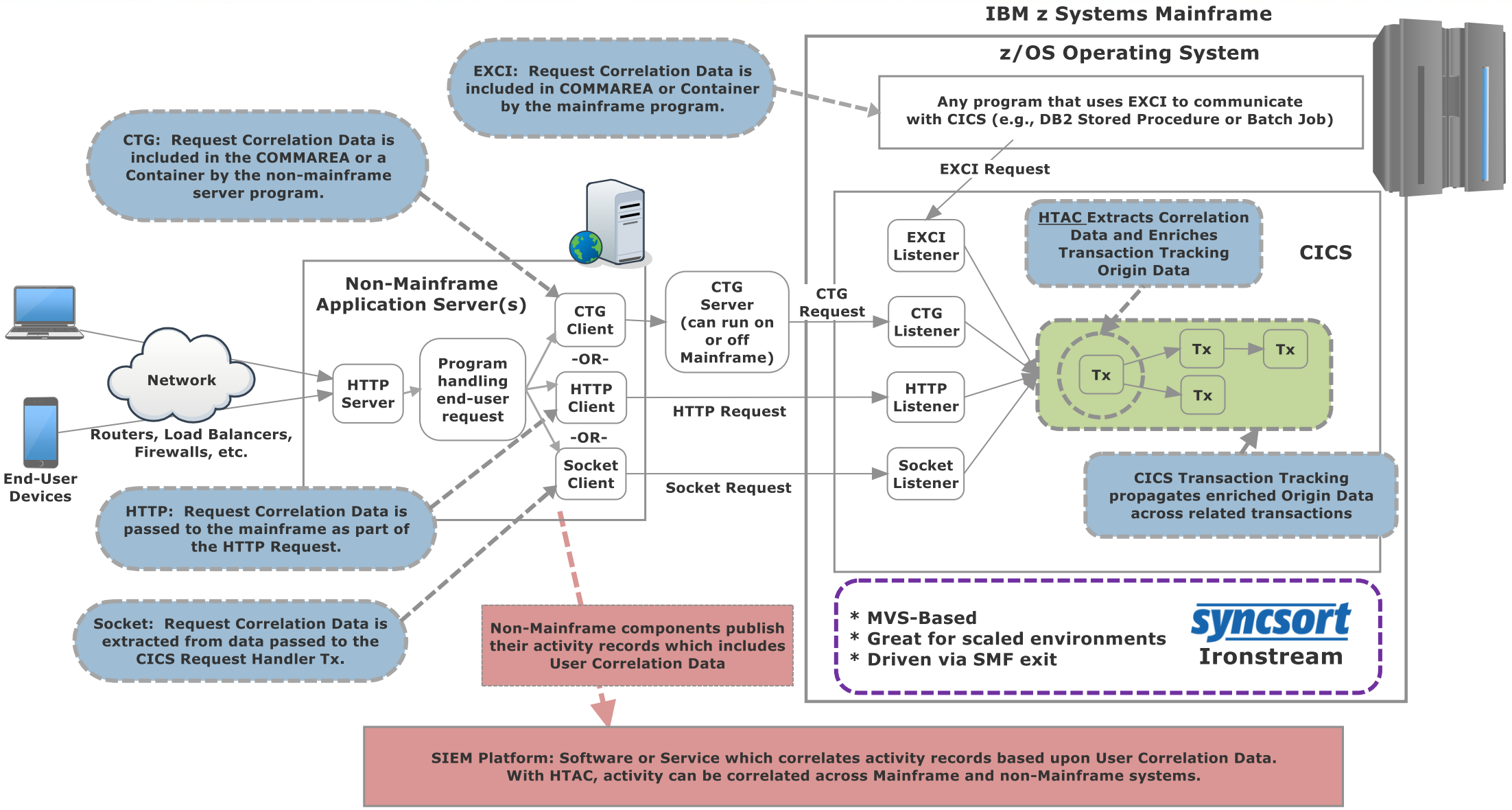
HTAC Operating Environ.

HOSTBRIDGE® TECHNOLOGY



HTAC Operating Environ.

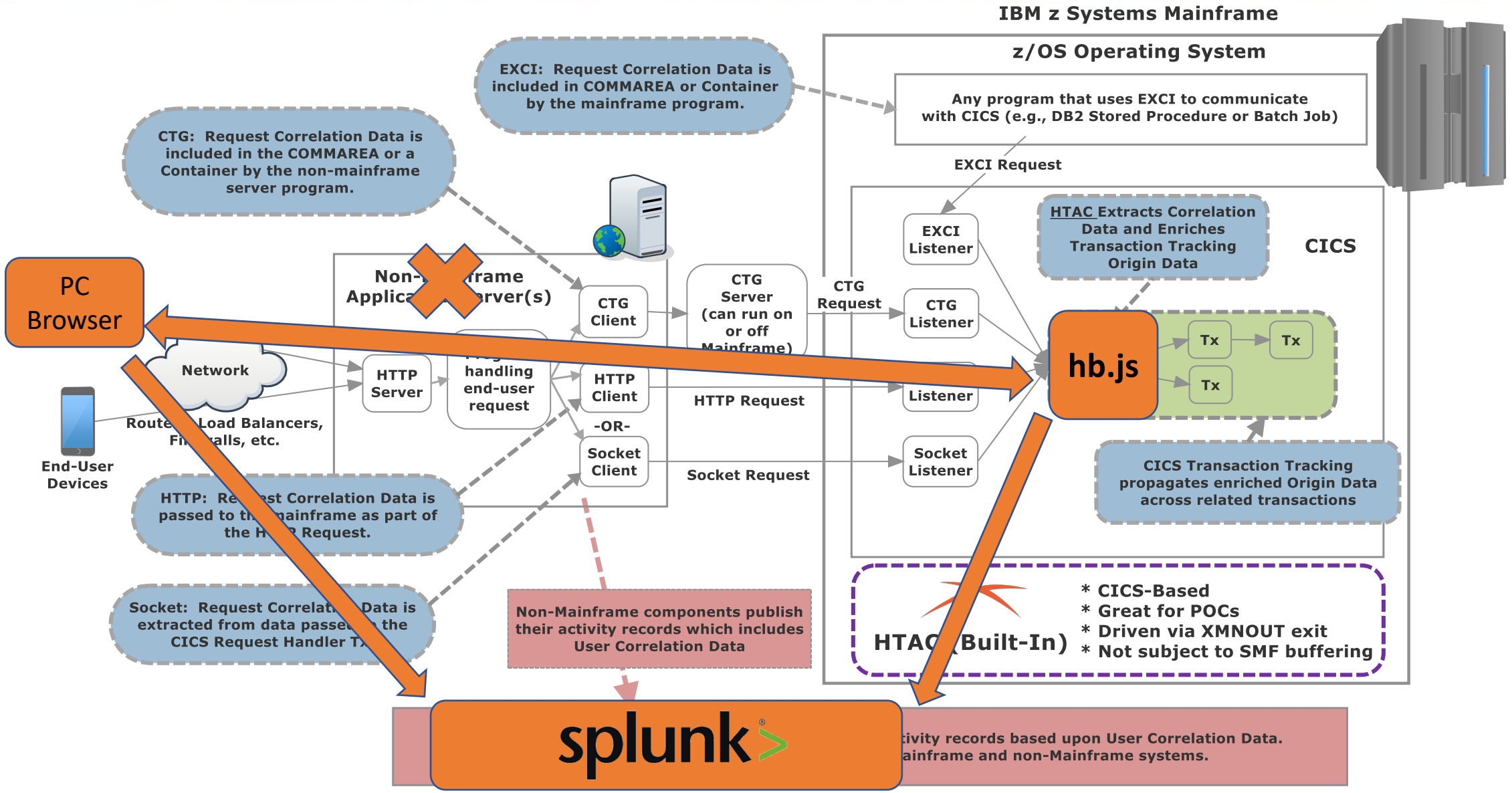
HOSTBRIDGE® TECHNOLOGY



HTAC Demonstration

HTAC Demo Environ.

HOSTBRIDGE® TECHNOLOGY



HTAC pricing & availability

HOSTBRIDGE® TECHNOLOGY

✓Available Feb. 20, 2018

✓Pricing model based on the number of daily correlations HTAC does:

Daily volume of correlated transactions	Total Annual License Cost
Less than 1,000	Free
1,000 to 99,999	$4,000
100,000 to 999,999	$9,000
1 million to 9,999,999	$12,000
10 million or more	$21,000

Questions?

Free Eval License of HTAC

HOSTBRIDGE® TECHNOLOGY

Try HTAC!

✓To get a free evaluation license, contact:

- 866.965.2427 (International: +1.405.533.2900)
- info@hostbridge.com

Thank you!

HOSTBRIDGE®
TECHNOLOGY

www.hostbridge.com