Building and Verifying Security Trust in Today's Complex Tech Stacks and Hybrid Solution Environments.

Kurt Barndt

How can your organization be harmed as a result of a Cyber Security breach?

Data Theft

Intellectual Property Leak

Financial Theft

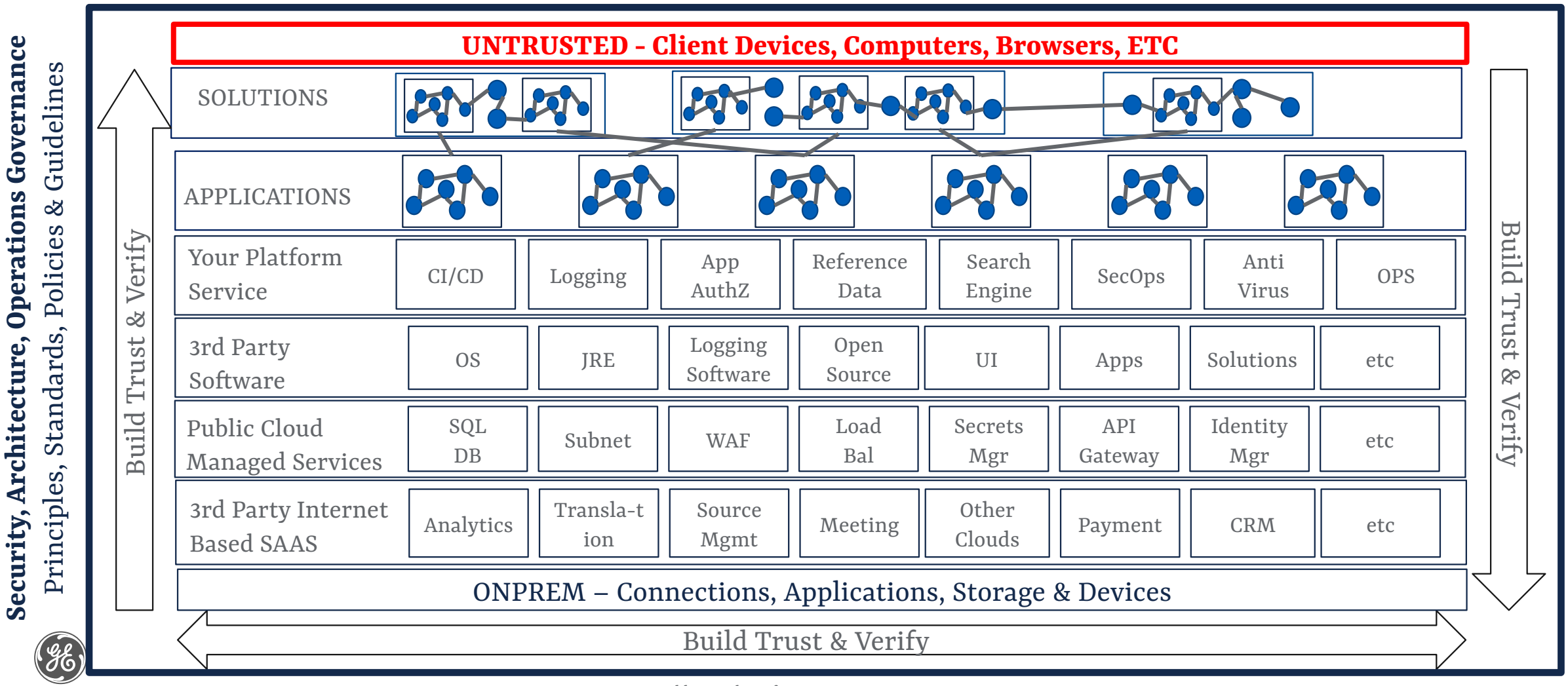
Loss of Trust

Reputation Damage

Data Tampering

Data Loss

Trust Stack to Consider (Cloud, Platform Services, Apps, Solutions)



Some of the Capabilities Needed to Build Trust Chain for SDLC

Defined Security Requirements	Governance Architcture, Apps & Security	Standards(Security, Dev, Coding, Runtime, etc)	Architecture
Secure Build Process	Operations / SecOps	Credential Requirements & Management	Security Testing
3rd Party Software & SaaS Management	Integration	Digital Asset Lifecycle Management	Patching / Upgrade / Replacement

Zero Trust to Verified Trusted

- Understand your risk appetite.
- Don’t assume the other party has controls in place and can be blindly trusted.
- Build your software with security controls to defend itself
- Evaluate any software you use/buy by your own standards
- FYI, Your Public Cloud provider doesn’t trust you.

- App Trust starts with architecture
- Software “Supply Chain” trust needs to be built. This will involve multiple internal/external orgs
- You either build a certain degree of trust based on requirements and verification or you remain untrusted.
- Some services must be trusted by default like Identity Mgmt.
- Building Trust requires additional resources and activities. Plan for it.

Governance is the Foundation in Defining what Trust Means and How to Verify

- Identify Governance Competency Enterprise Architecture, CMMI
- Security Standards - ISO, NIST, etc
- Formally Defined, Managed and Automated processes
- Impact analysis for any change
- Principle, Standards, Policies Guidelines
- Define required security capabilities
- Identify, enforce NFRs for all assets
- Planned obsolescence
- Set and Control API standards
- Set engineering behaviour
- Org needs to trust governance is in their interest. Appropriate Approval process and board members is critical
- Don’t rethink commodities Reuse vs rent vs buy vs build.
- If it doesn’t conform it doesn’t release
- Defined Software Selection Process
- Define Mandatory and recommended security requirements

In General Treat Users as Untrusted – Human, Device, Services

- Start by assuming device (PC, laptop, smart phone, etc) is compromised
- Don’t trust any uploads
- Don’t trust browser version and also enforce allowable browsers and versions
- Defend against sloppy credentials: set id/password minimums also mandate MFA.
- Timeouts – tokens and certificates
- Be careful not to reduce security for easy user experience unless the business case requires it

Selecting, Building & Managing Trusted Components / Capabilities / Custom Services / Platform services.

- Catalogue all 3rd party software
- Decide what Open Source model is fit for you.
- Get Emergent Vulnerability/Threat alerts
- Use Cloud services first. Unless you can create a managed service as good, cheap and secure as Azure or AWS.
- Continuous asset management including “out of support” apps still deployed.
- Need to plan Upgrades and when software goes Out of Support
- Software Scanning Tools to verify vulnerability state of code/binaries
- Application Lifecycle management – requirements to build to sunset.
- Have a Patch plan for all assets.
- Application Store: 3rd Party contributors. Define security standards they must comply with. Verify compliance. Also don’t trust them

Trust in our Partners – Internal & External

- Define and implement Processes for 3rd party engagement.
- Verify Source code, packages, exec binaries/apps , SaaS – All need to be considered differently
- “Internal” does not mean trusted
- What are their processes regarding security for Proprietary or Open Source software?
- Are they managing their 3rd party software? (do they have a list?)
- Did they do Penetration testing?
- Do they have Data protection policy and assessment?
- Should have Defined NFRs and Availability
- Insurance policy? NDAs?
- Do they have a Patch plan?
- What Security controls are in place?
- Is there Asset lifecycle Management and SDLC
- Are they Multitenant? Is that ok?

Lift and Shift to the Cloud requires Trust Rebuild – Security Reassessment & Improvements

- The concept of running in a ”trusted” customer network is gone.
- Reassess Security controls can defend against an internet attack
- Will need a Cloud aligned patch and upgrade capability
- Ops and SecOps are now your responsibility if they weren’t already
- Log messages must be monitorable and centrally correlated
- Stress test and retest the application and security systems to Cloud
- Fix old security bad habits: hard coded credentials, weak TLS, old 3rd party.
- Make sure still PCI or HIPAA compliant Cloud provider will require it
- Harden Admin access
- Prove Security Defects are fixed
- Profile/Monitor executables

Cloud Based Multitenancy / MultiApp / MultiCountry Trust Implications

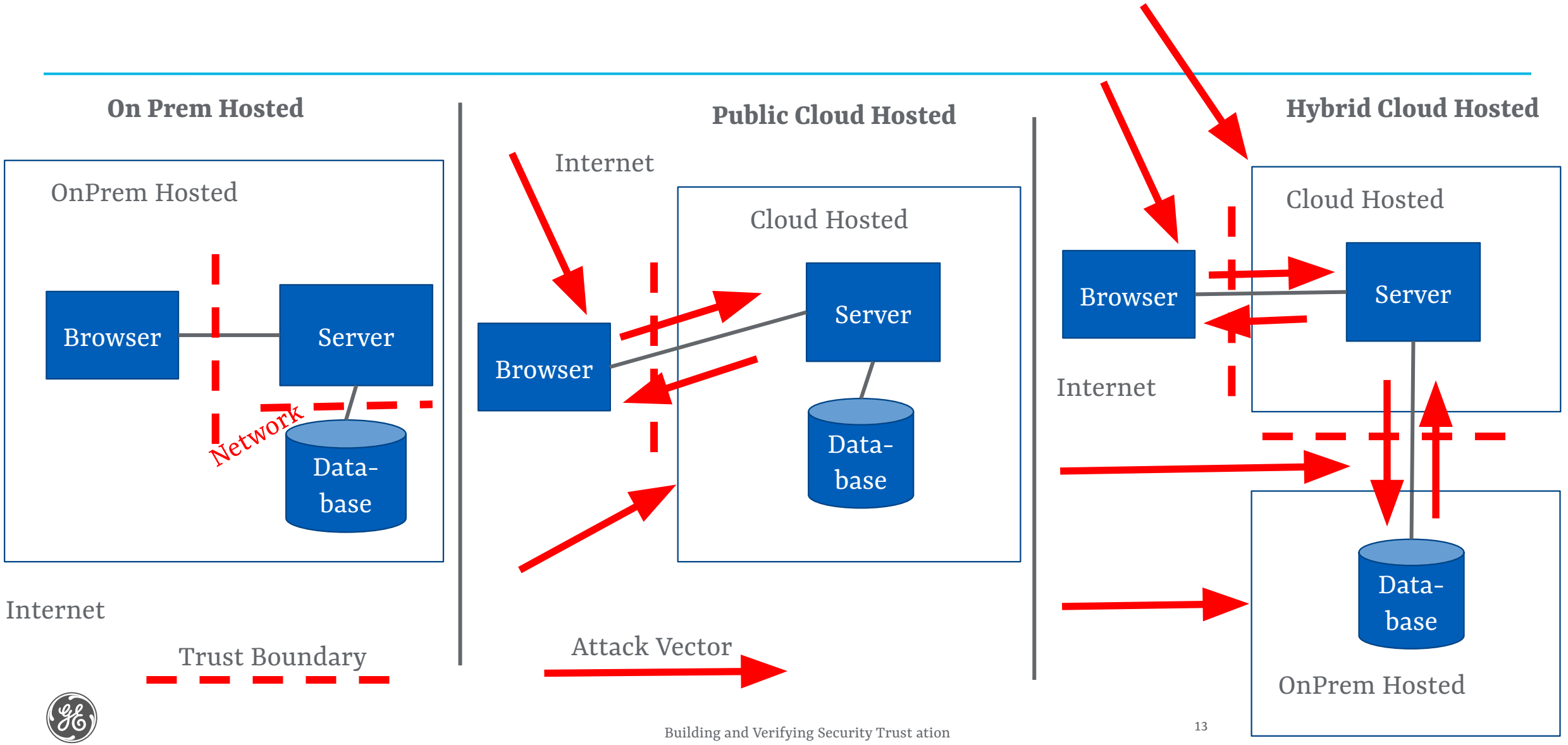
- It increases Software complexity. How complex do you want it? Should you do it?
- Operations complexity increases
- Think Maturity - Steps 0,1,2,3,4… Not Big Bang
- Driven by pressure on infrastructure cost reduction
- An opportunity for new customers and markets
- Don’t loosen security for all apps because of one app
- Can’t just say every app for themselves regarding security and trust.
- Design and Verify tenant isolation don’t allow an attacker to move between tenants
- Are Encryption paths required?
- Verify data, execution isolation
- Adding, deleting, migrating tenants securely. Manual increases mistake opportunity
- Data Protection polices need verification
- Now require ability to fix in flight
- Pressure and cost shift from infrastructure to engineering

Building Cloud-to-OnPrem Trust

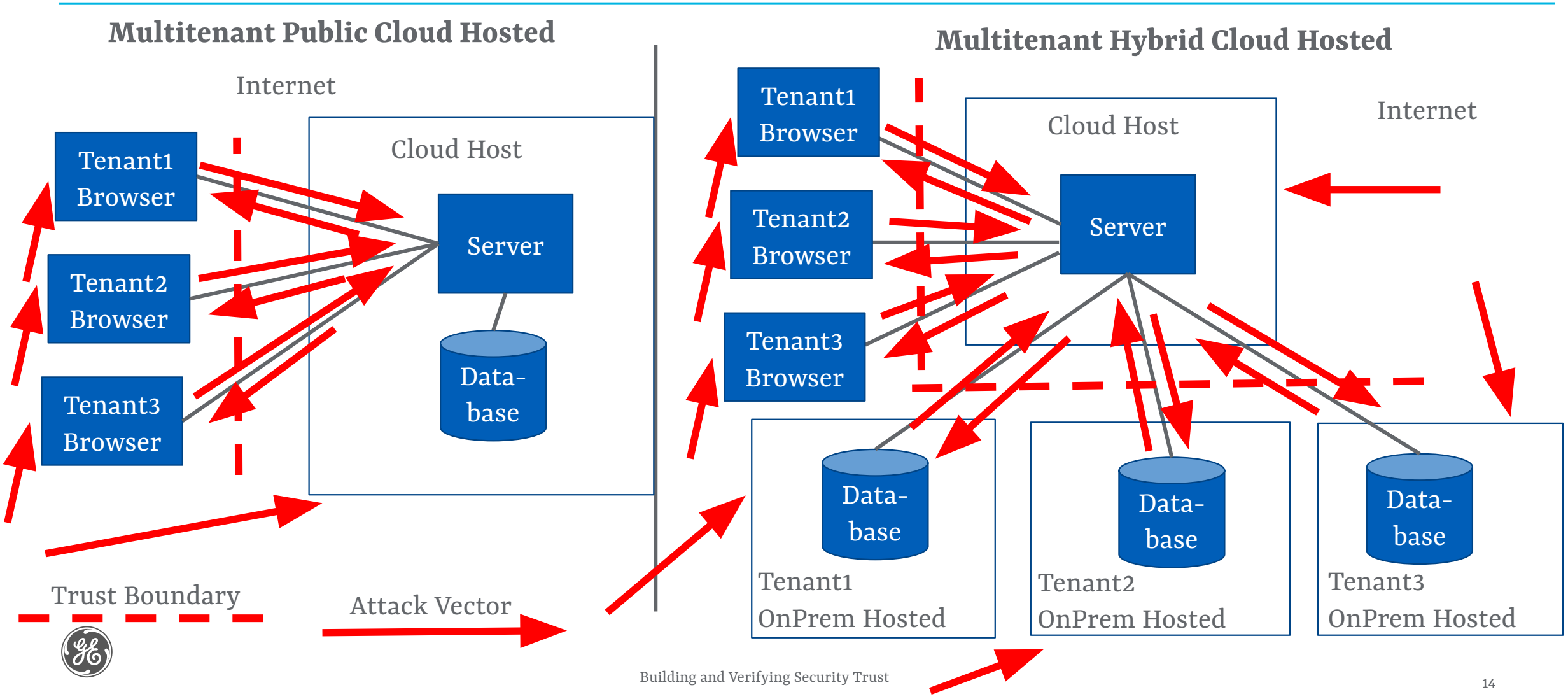
Deploying hybrid OnPrem/Cloud solutions has addition security risk due to added attack vectors coming from either direction that must be mitigated.

- Install OnPrem Edge Device for securely brokering the Cloud connection.
  - Bootstrap for secure Edge Device installation
- Implement Mutual Authentication / TLS
- Zero trust for Uploads / Downloads. Scan both directions
- Security logging is critical on both platforms. Ensure all communication can be correlated to/from Cloud and OnPrem for analysis.
- Consider VPN

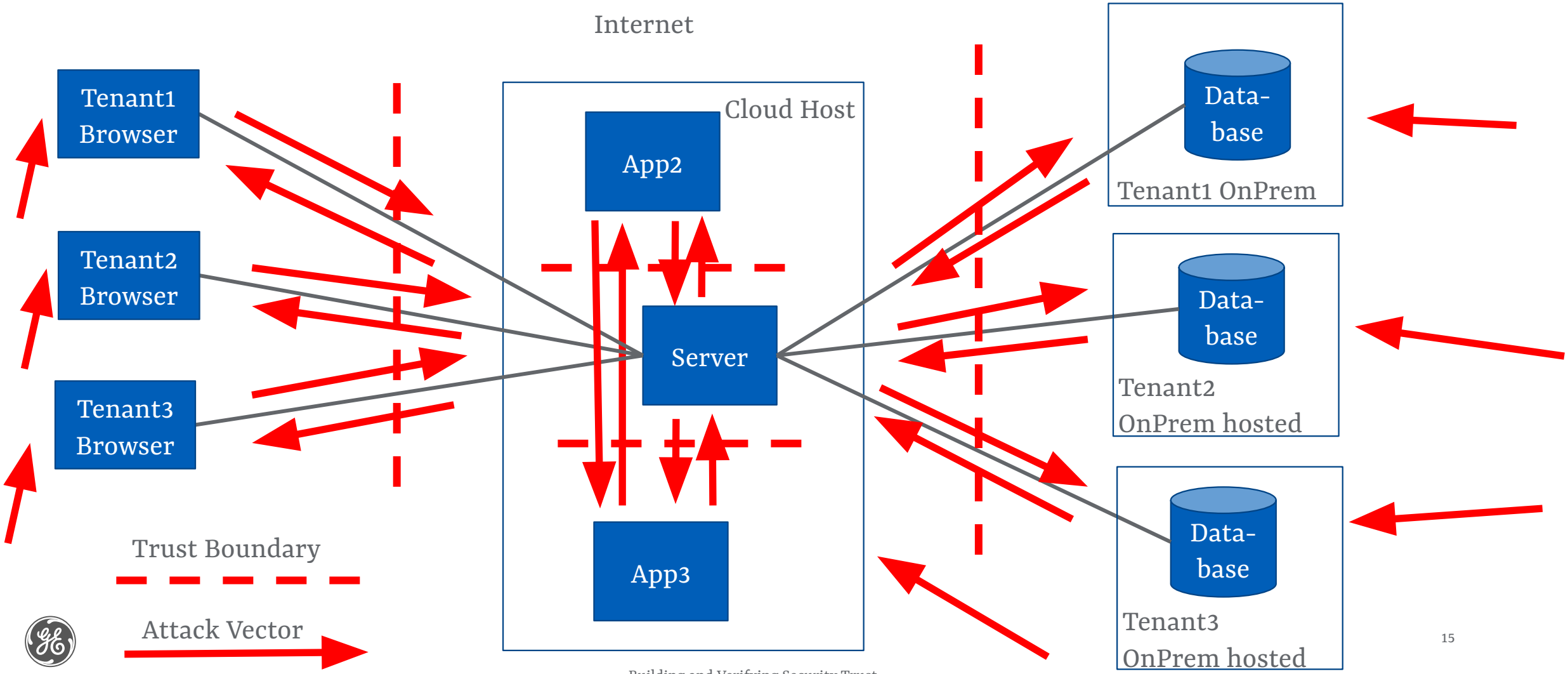
Complexities of Cloud Trust:
On Prem Hosted vs Public Cloud Hosted vs Hybrid Cloud Hosted



Complexities of Cloud Trust – On To Multitenancy



Complexities of Cloud Trust - MultiApp Multitenant Hybrid Cloud Hosted



Trusted DevSecOps

- Know What was Deployed
- Know What will be Deployed
- Know What is Deployed?
- Know What shouldn't be there
- Restrict Who is authorized to deploy
- Plan/coordinate when to deploy
- Be able to verify everything is Secure

- Attackers actively look to exploit Deployment pipeline as it basically controls everything
- Don't do Development in Prod
- Restrict and Monitor any Access
- Automate and remove Human element when possible
- Have defined Processes, Policies and Standards

Trusted Operations

- Governance is again key.
- Fixing broken software in a secure trusted manner is hard
- Plan/Control/Automate Upgrades
- Migrations need planning and tools
- Make no direct production changes
- Treat Ops like any other solution
- Automate as much as possible
- Use best of breed operations software
- Ops requires highly privileged access. Give specific access when needed don't just blindly grant admin
- Determine availability needs
- Have Backup / Restore Capability
- Rollback planning each release
- Plan and test Disaster Recovery
- Store & access logs securely
- Operations needs security testing
- Monitoring – "who's watching the watcher?"

Why should your customers trust you?

- Know your risk. Have answers. Provide/plan fixes.
- Have a good secops & ops story
- “Stuff” happens to everyone. The lasting impression is the reaction.
- Assume they will ask the same questions you ask of 3rd parties
- They hire security researchers, specialists, cyber testers
- If you provide Cloud based APIs they will test them.
- If you provide on prem binaries, containers etc they will scan them
- Missing simple security controls influence. “if they can’t enforce TLS1.2+ for a public internet facing browser…”
- Disclose only enough to build trust without disclosing IP/design/risk
- Existing customers will talk about the issues to fix. New ones may walk away.