Securing Active Directory Operations in Untrusted Regions

Cross Domain Killchain: Step One

1. Domain Controller Breach: By raiding offices with domain controllers or otherwise compromising them State Threat Actors gain complete access to that child domain.

NTDS.DIT

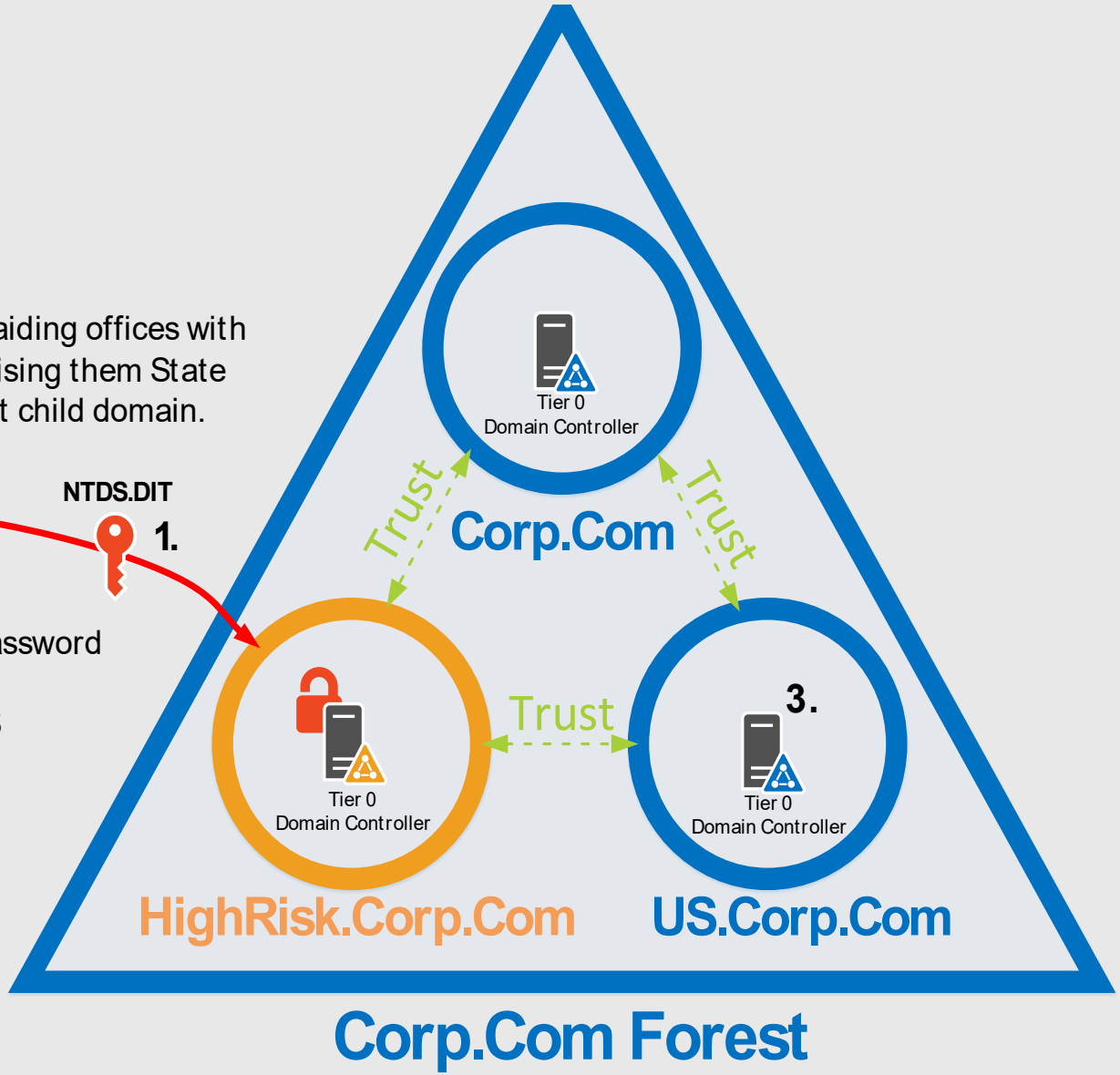
1.

Domain Admins

ServiceAccount1 = ReallyLongandPassword

Bob = Lovesecurity123!@#

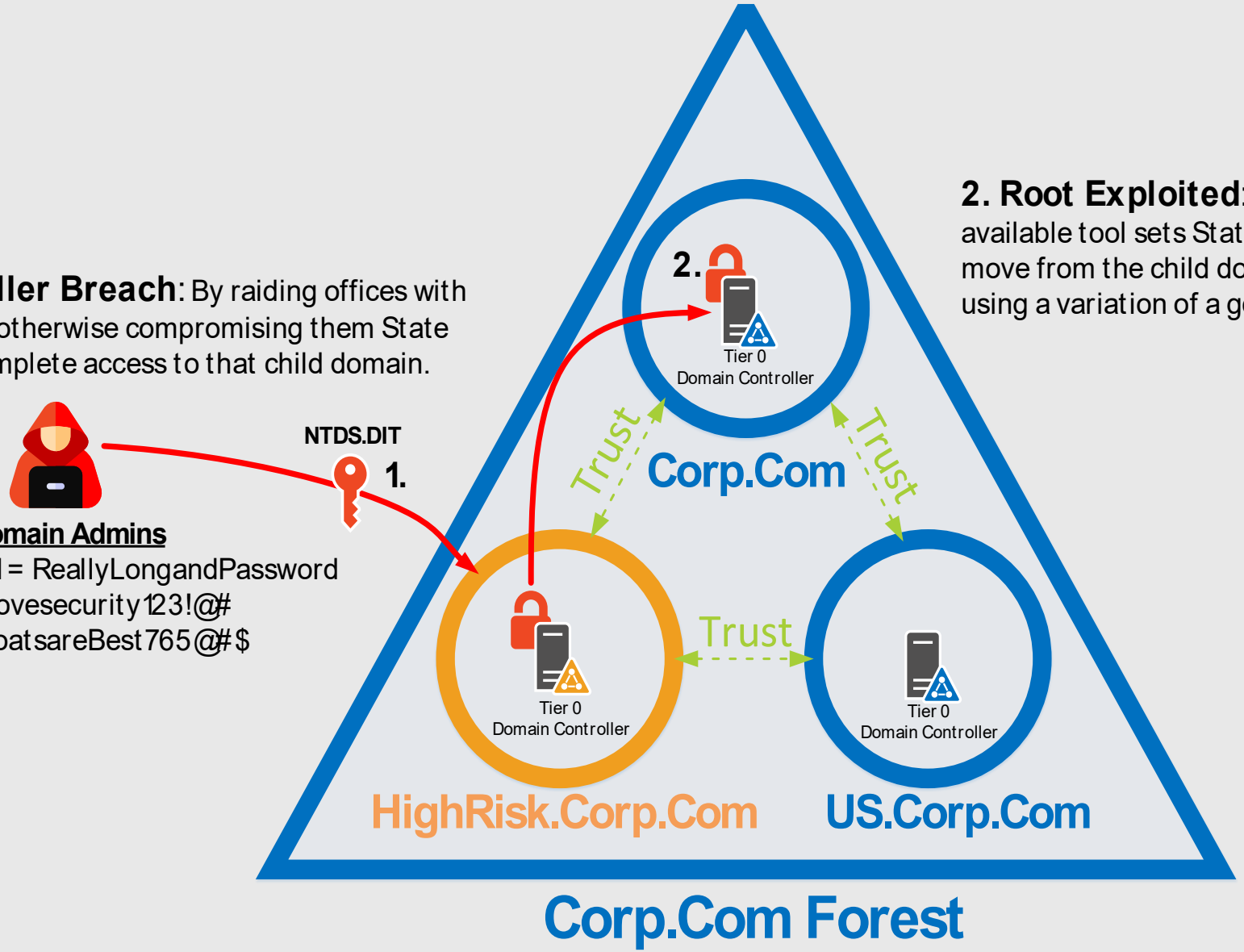
Sally = GoatsareBest765@#$



Cross Domain Killchain: Step Two

1. Domain Controller Breach: By raiding offices with domain controllers or otherwise compromising them State Threat Actors gain complete access to that child domain.

2. Root Exploited: Leveraging widely available tool sets State Threat Actors are able to move from the child domain to the root domain using a variation of a golden ticket attack.



Cross Domain Killchain: Step Three

1. Domain Controller Breach: By raiding offices with domain controllers or otherwise compromising them State Threat Actors gain complete access to that child domain.

NTDS.DIT

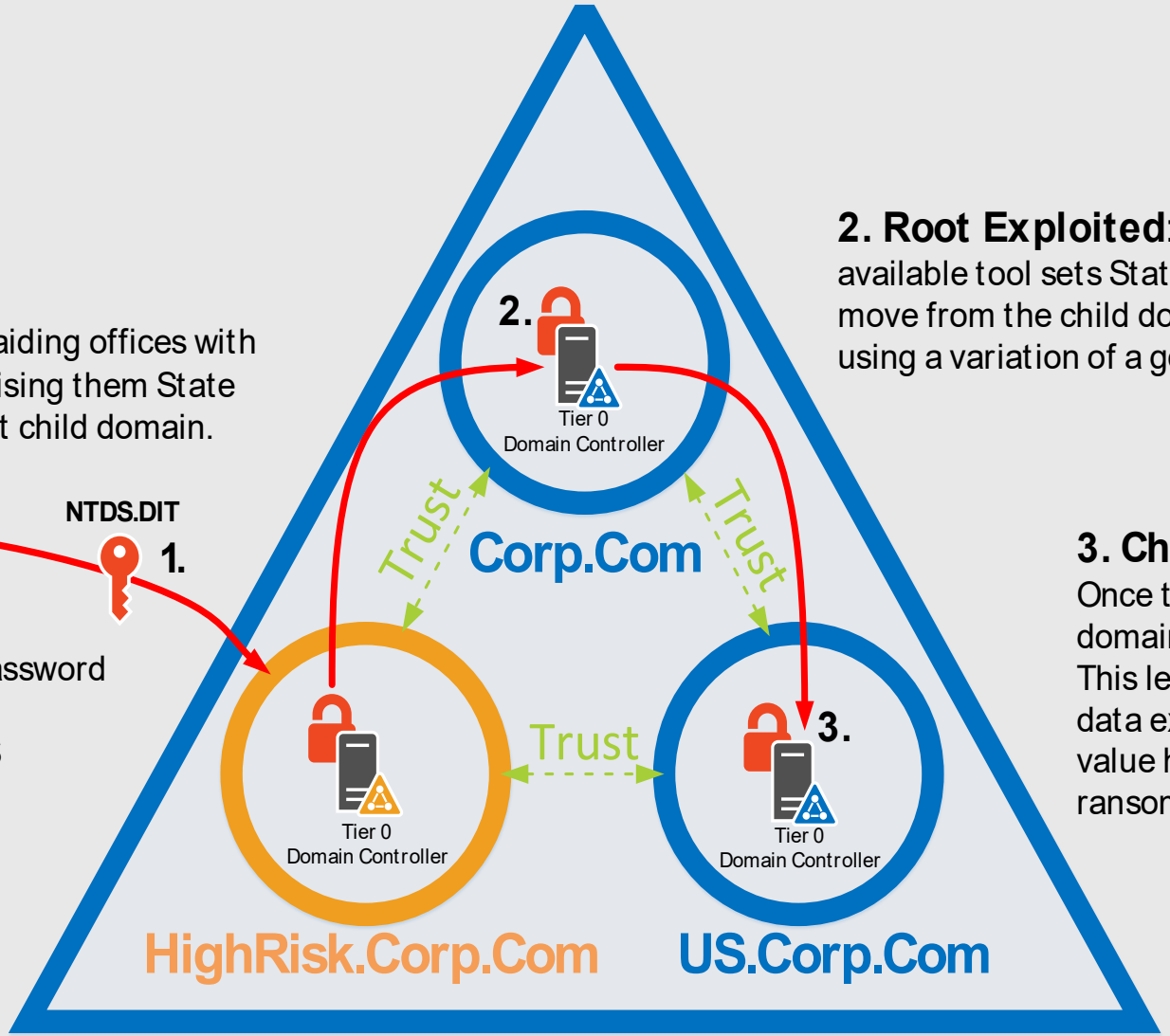
1.

Domain Admins

ServiceAccount1= ReallyLongandPassword

Bob = Lovesecurity123!@#

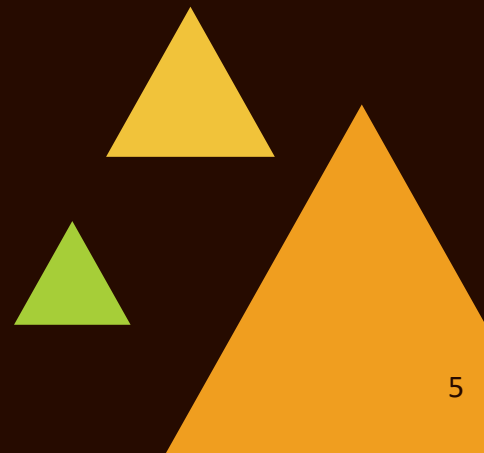
Sally = GoatsareBest765@#$



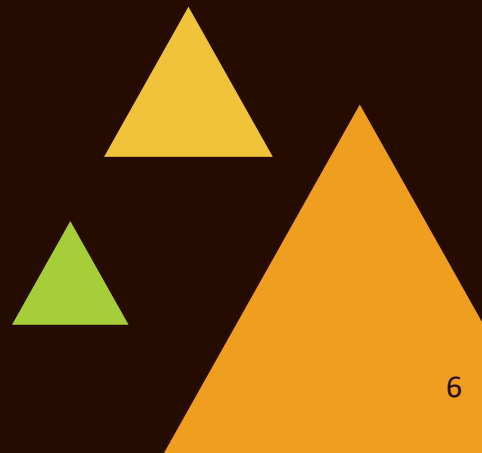
2. Root Exploited: Leveraging widely available tool sets State Threat Actors are able to move from the child domain to the root domain using a variation of a golden ticket attack.

3. Child Domains Compromised: Once the root has been exploited all child domains are exposed and easily breached. This leads to command and control nodes, data exfiltration, persistence and when all value has been extracted data destruction or ransomware attacks to cover their tracks.

Yeah, this is old news. (2015)



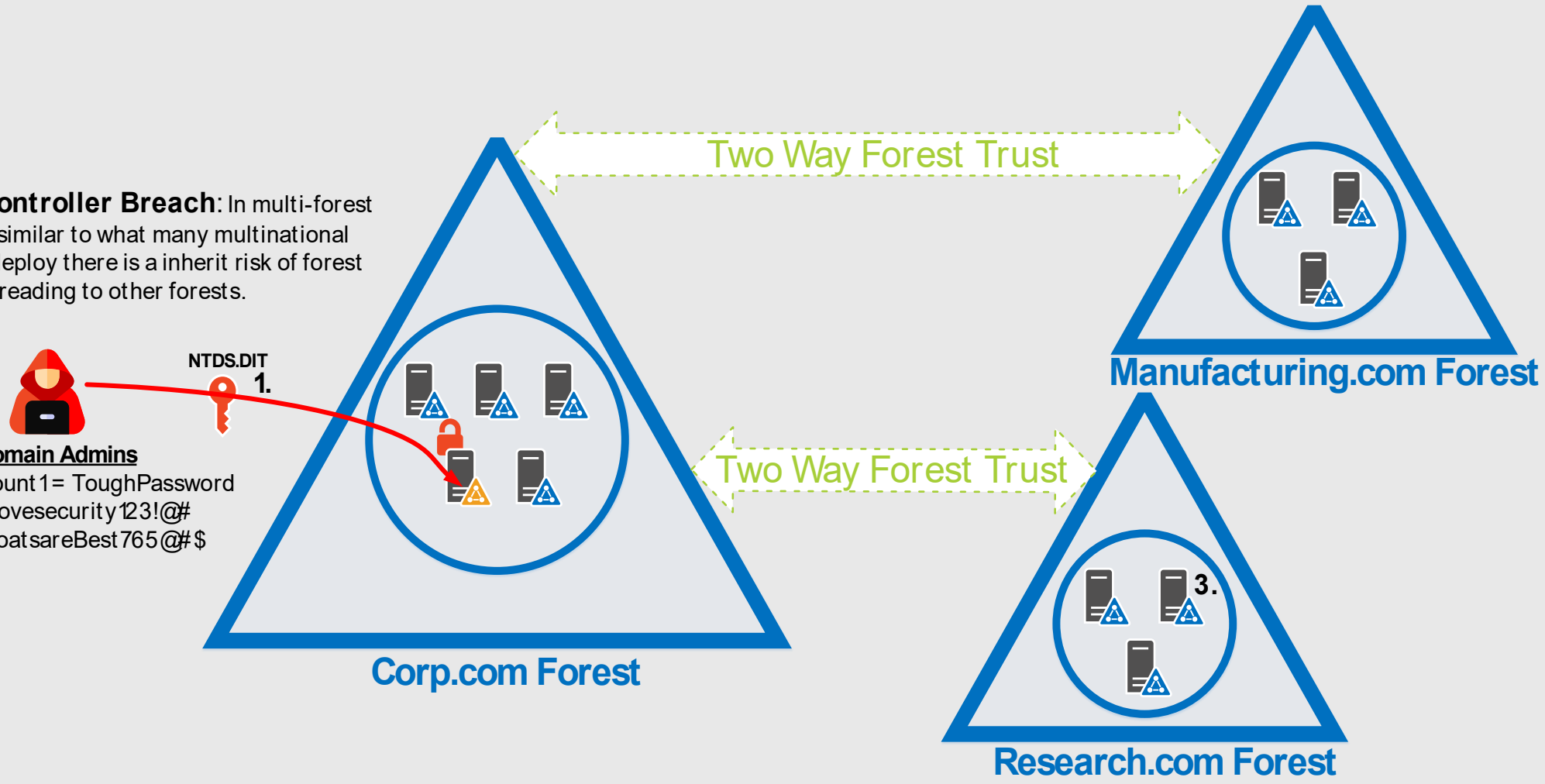
My domain controllers are in a separate forest and physically safe in region X anyway.



What’s the worst that can happen?

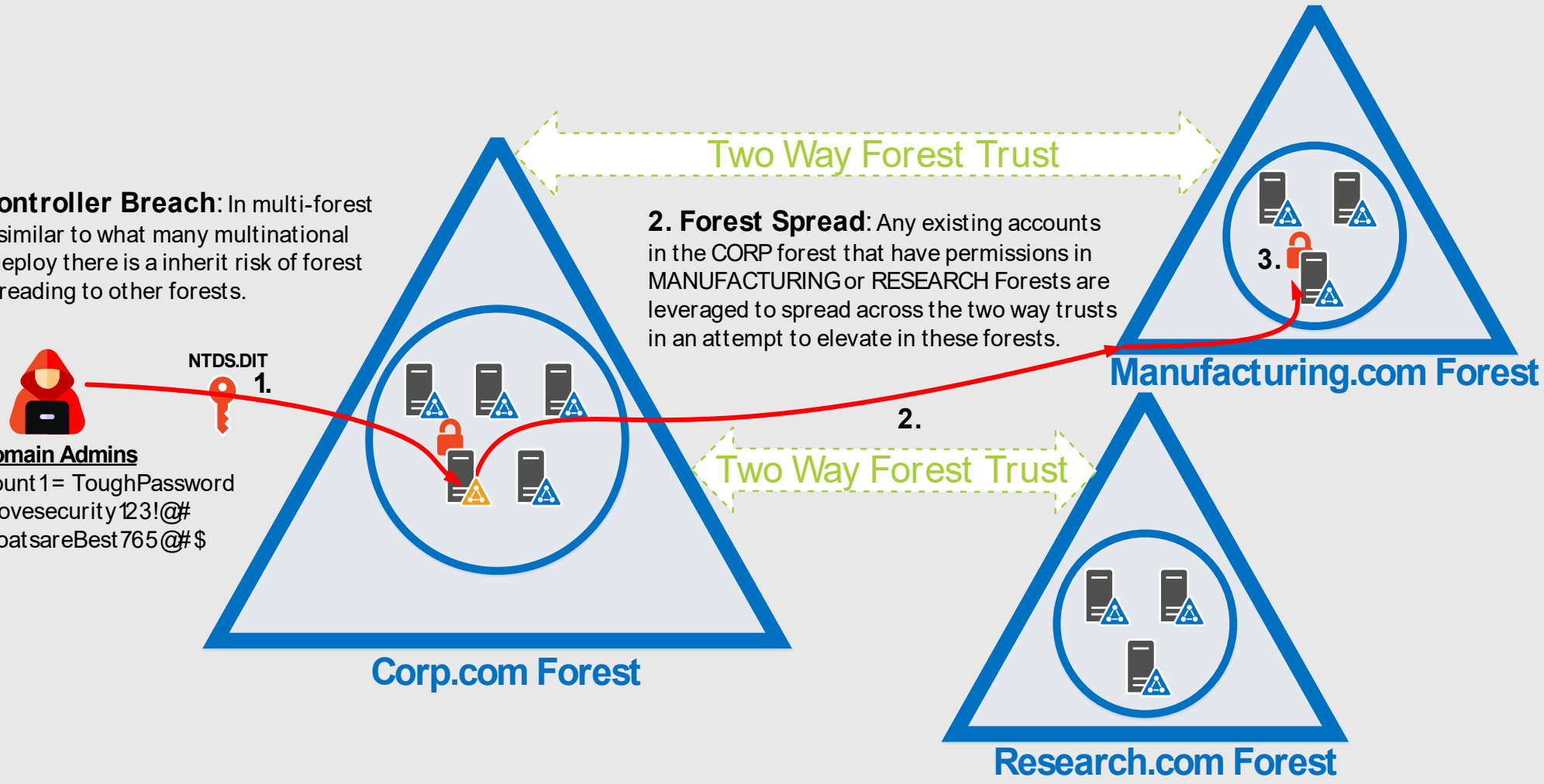
Cross Forest Threat Pathing

1. Domain Controller Breach: In multi-forest configurations similar to what many multinational fortune 500's deploy there is a inherit risk of forest compromise spreading to other forests.



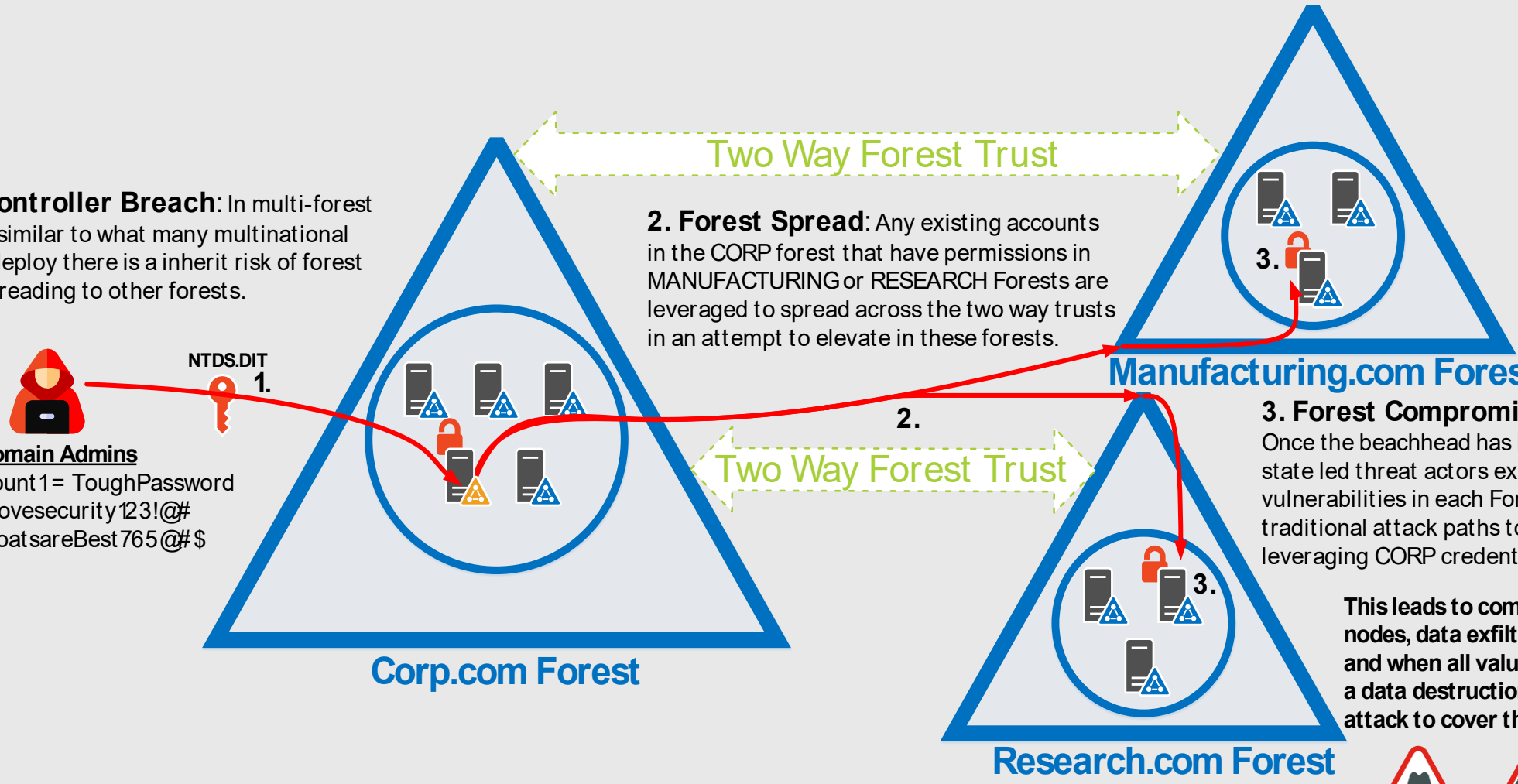
Cross Forest Threat Pathing

1. Domain Controller Breach: In multi-forest configurations similar to what many multinational fortune 500's deploy there is a inherit risk of forest compromise spreading to other forests.



So, yeah. This is the worst that can happen.

1. Domain Controller Breach: In multi-forest configurations similar to what many multinational fortune 500's deploy there is a inherit risk of forest compromise spreading to other forests.



2. Forest Spread: Any existing accounts in the CORP forest that have permissions in MANUFACTURING or RESEARCH Forests are leveraged to spread across the two way trusts in an attempt to elevate in these forests.

3. Forest Compromise:
Once the beachhead has been established state led threat actors exploit existing vulnerabilities in each Forest using traditional attack paths to elevate within leveraging CORP credentials

This leads to command and control nodes, data exfiltration, persistence and when all value has been extracted a data destruction or ransomware attack to cover their tracks.

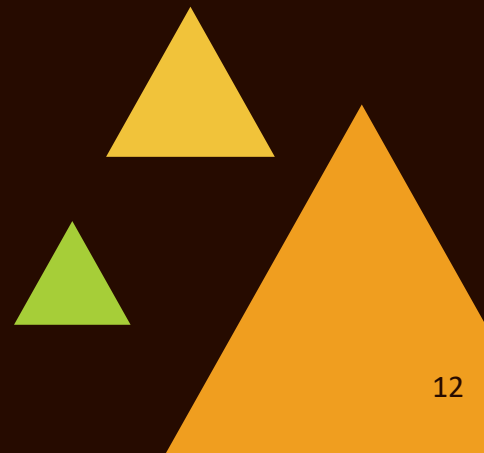
Ok, that’s pretty bad.

But I need those two-way forest trusts because of how our business operates.

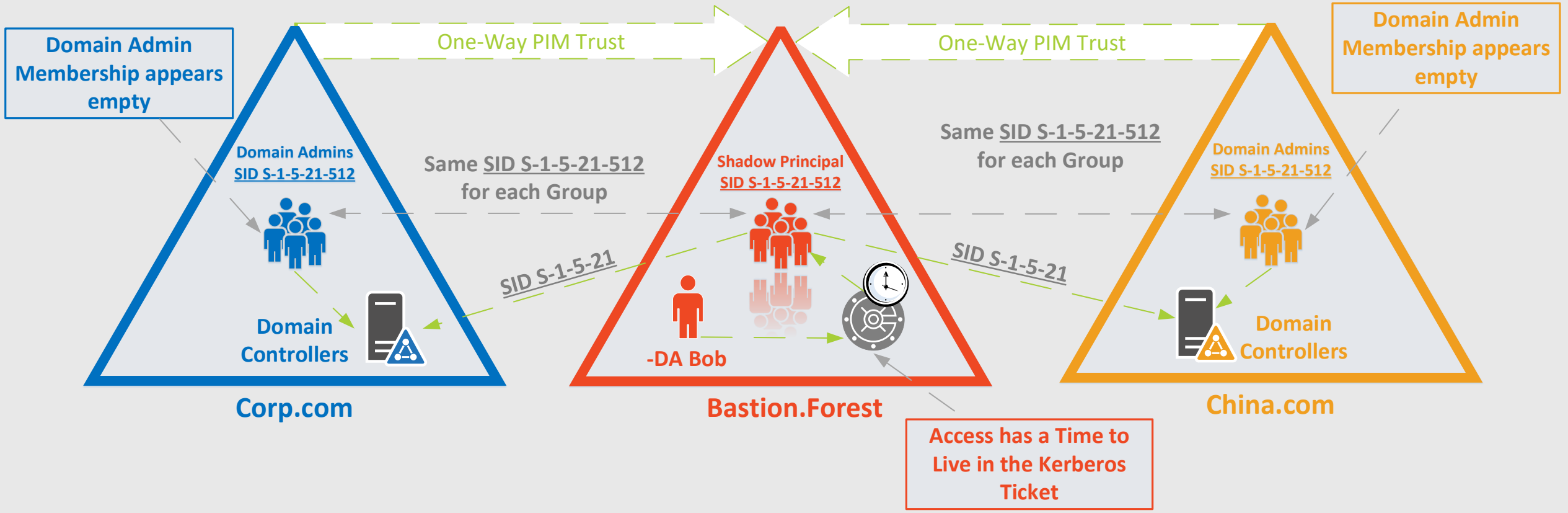
Can I mitigate this risk somehow?

YES.

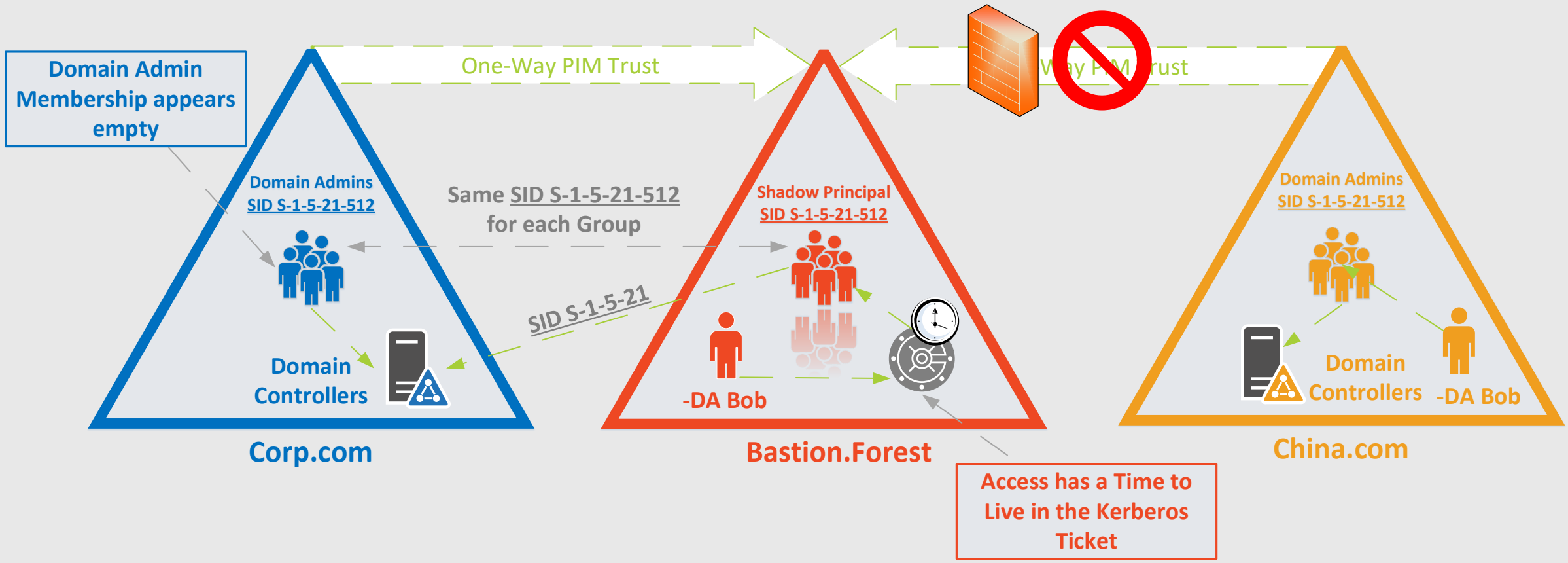
But it’s going to take some work.



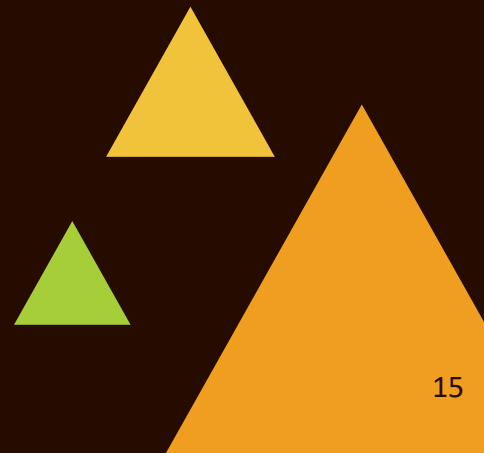
Secure Active Directory Operations in Untrusted Regions



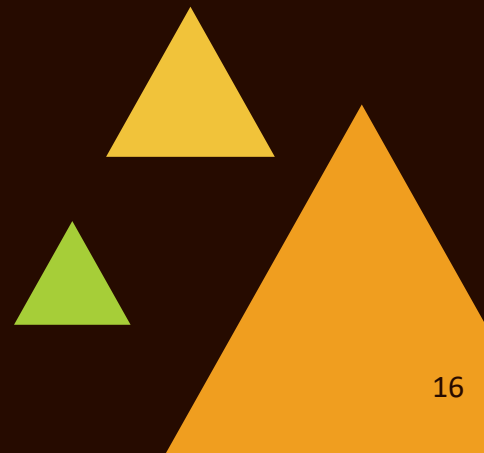
Secure Active Directory Operations in Untrusted Regions



Wait, isn’t this ESAE/Red Forest?

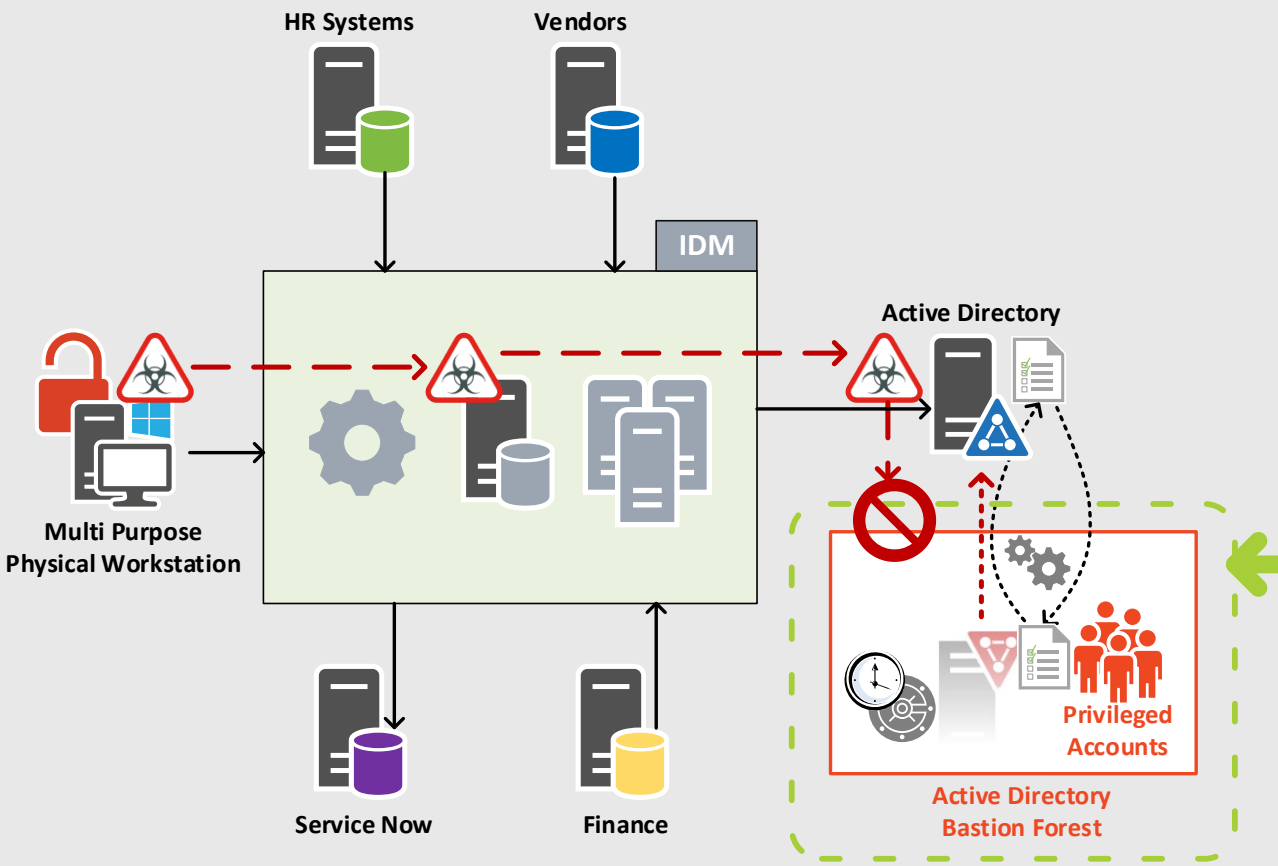


It’s too expensive/complicated, anyways Microsoft deprecated this model. Right?



But I don’t want MIM or any of the identity overhead of a bastion forest.

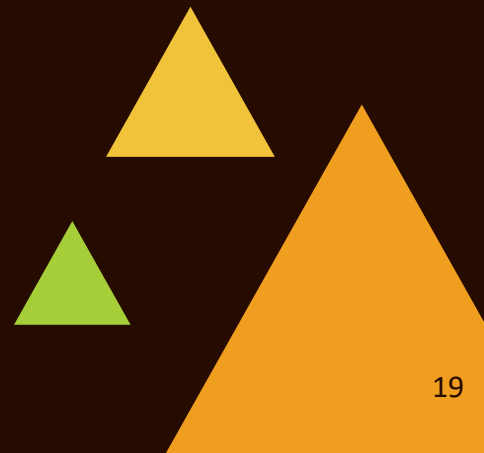
IDM Risks and Solutions



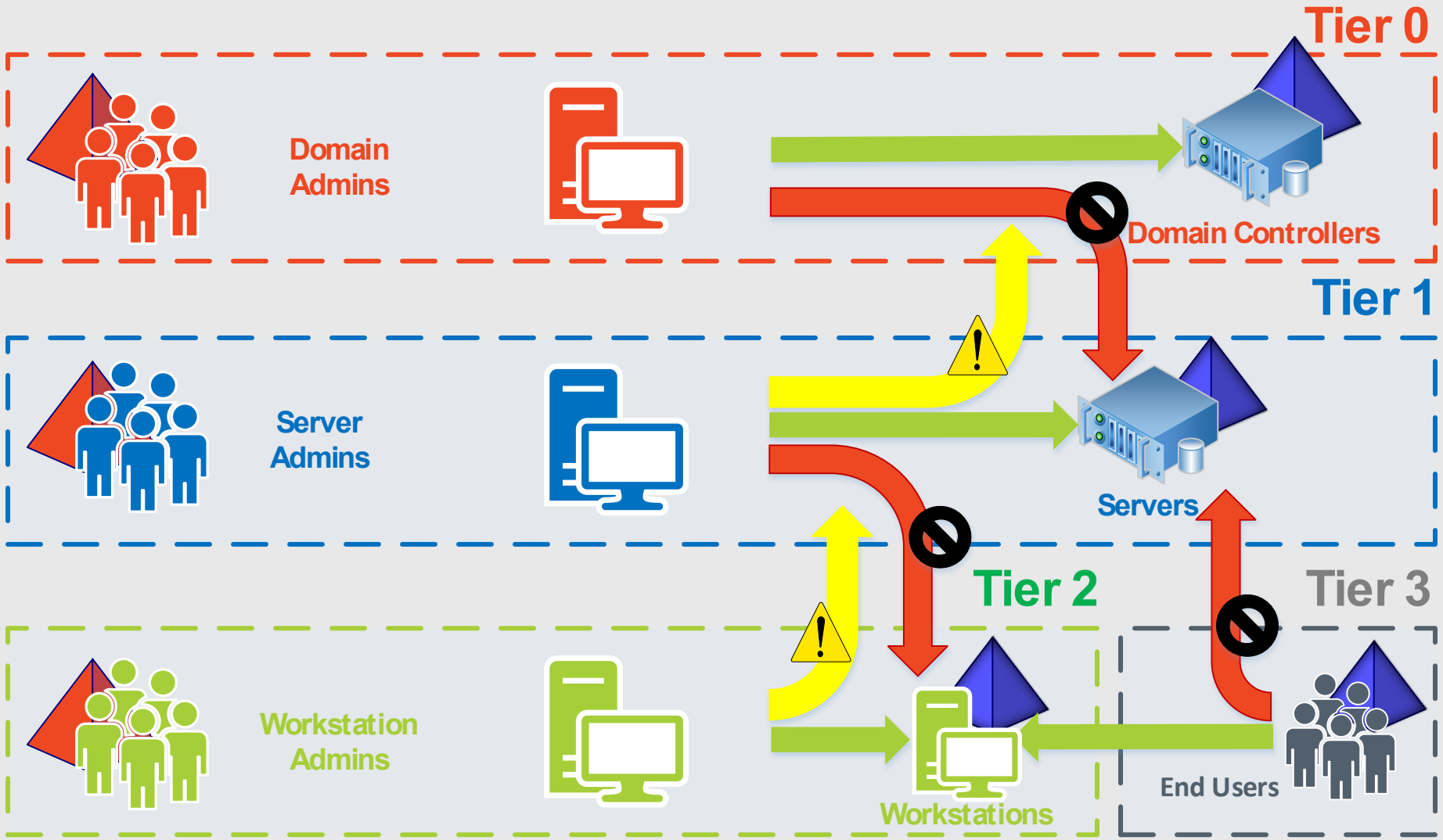
Logical Requirements - IDM Integrations

- Existing IDM solutions should not be able to directly manage Bastion Forest identities
- To solve for this existing workflows are kept in place with the addition of the ability to leverage honeypot accounts that integrate with SecOps
- The bastion forest automatically checks and pulls in new identities periodically and provisions all necessary groups and shadow principals

That can’t be it, what else do I have to do to implement this?



Account and Device Isolation Through Security Tiers

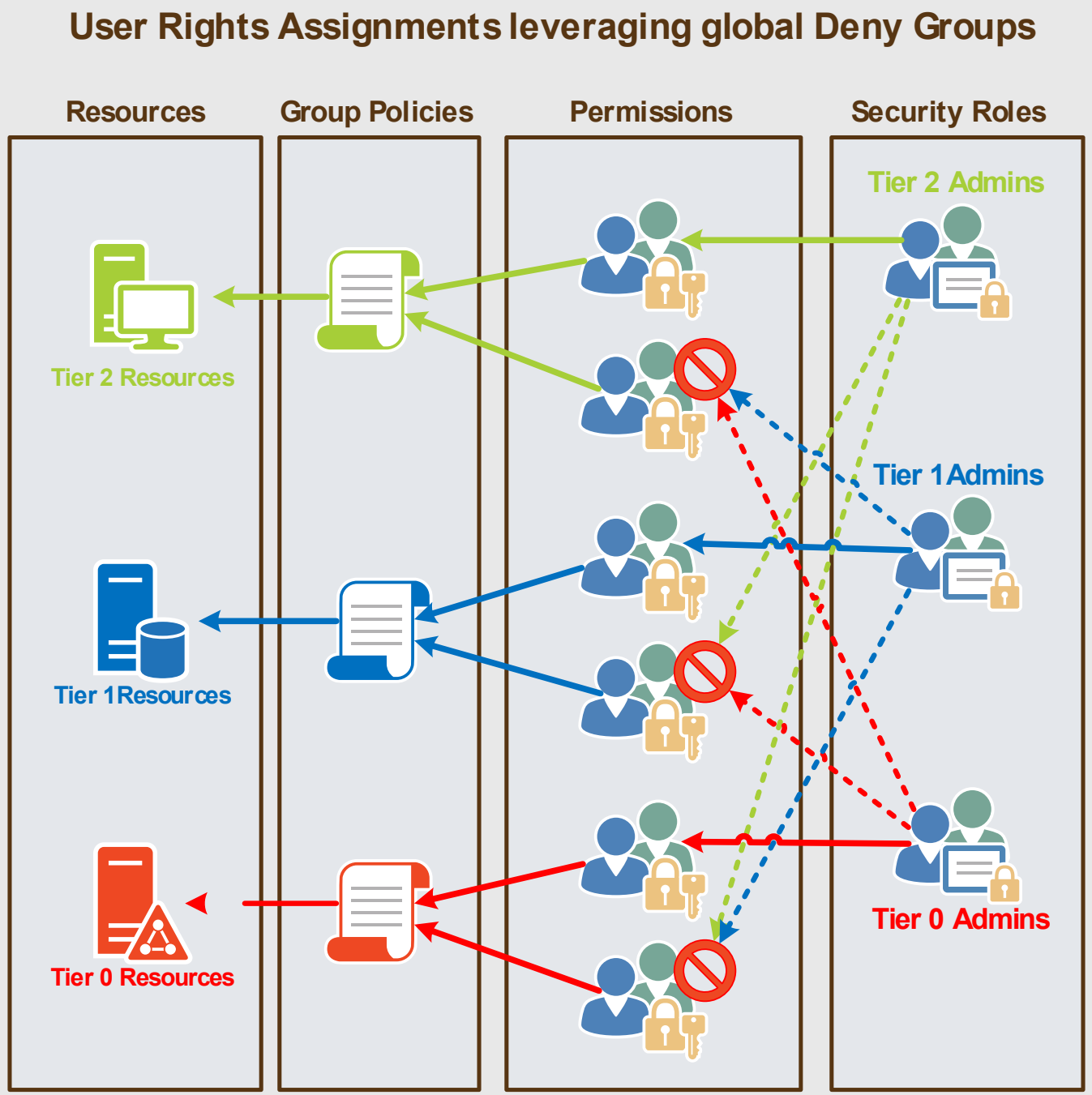


= All Access Blocked

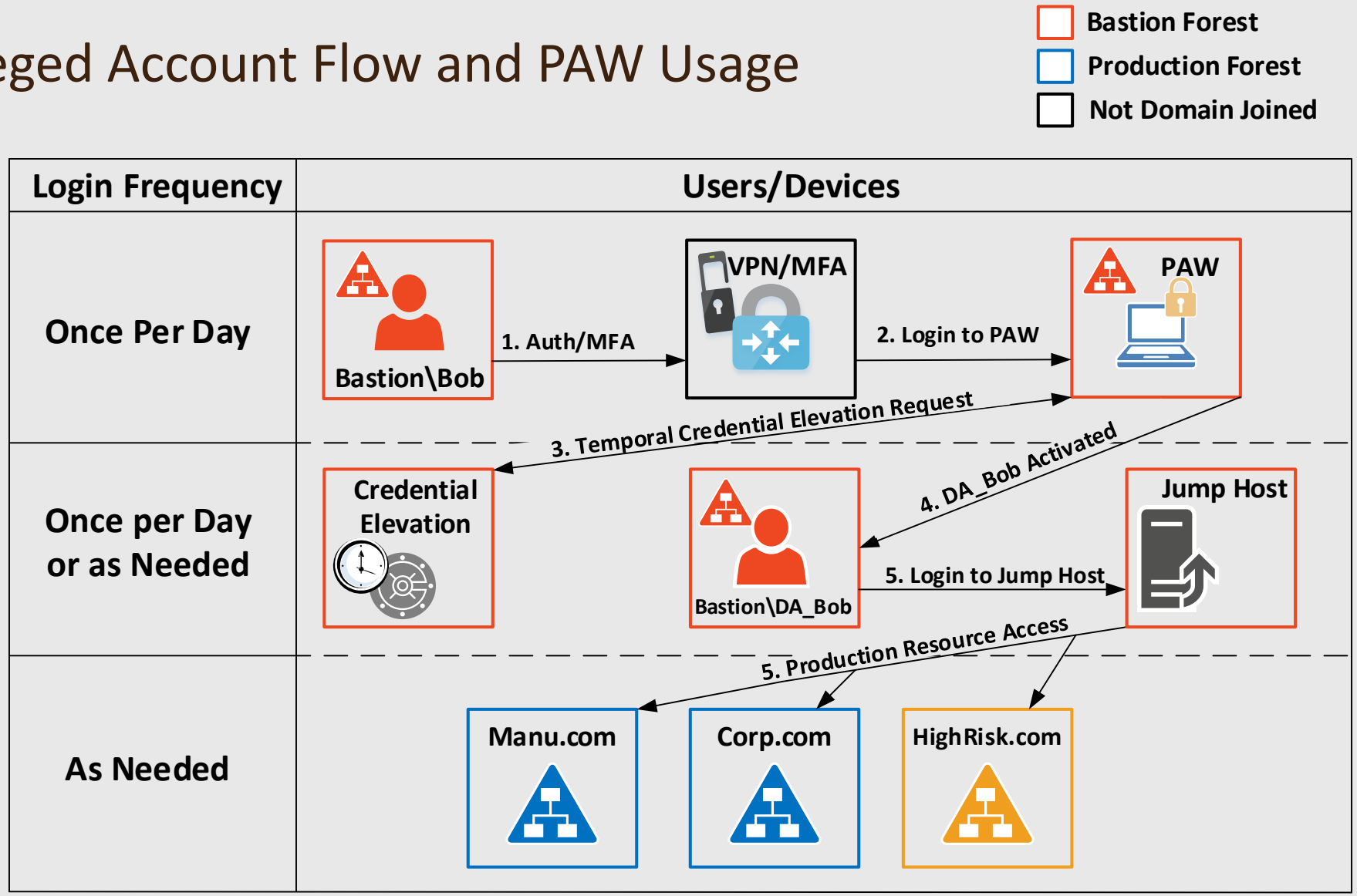
= If higher Tier access is needed the admin will require an additional privileged account.

Tiering Enforcement

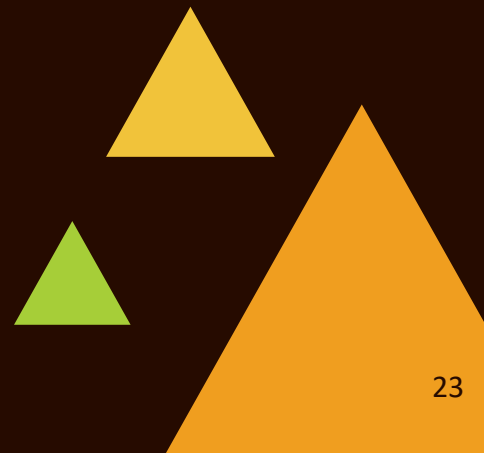
- Security policy and auditing of technical controls combined with tiering enforcement are required to maintain the model.
- In the **Security Roles** column, we see RBAC role groups linked to specific URA denies adding a layer of defense on top of existing controls.
- By nesting these role groups into URA denies we ensure that a compromised account doesn't have the ability to quietly elevate itself.



Privileged Account Flow and PAW Usage



Okay, that was a lot. Anything else that I should know?



Additional benefits of a Bastion Forest

- Achieves **Zero Trust** without additional products or subscriptions
- There are no known instances of exploit or breach of a Bastion Forest
- Centralized Domain Administration results in a dramatic reduction of Domain Admin accounts, typically around **90-95% reduction in the number of domain admins**
- Secure enclave from which production Active Directory environments can be restored from in case of a partial breach.
- You can securely run security tools leveraging GMSA accounts and if you want it temporal you can leverage shadow principals to monitor your entire environment globally from one secure and trusted location.

- **True physical isolation of the most powerful administrative accounts in an organization**

Challenges of Bastion Forest Implementation

- For true physical isolation users of the environment need to leverage Privileged Access Workstations (PAWs)
  - These devices are either dedicated physical devices or cloud hosted secure virtual machines
- Physical multifactor authentication devices are encouraged to be leveraged
  - YubiKeys are a **popular option**
- A tightly controlled and dedicated team is required to manage the Bastion Forest itself as the users of the environment while administrators in production are regular end users in the Bastion Forest itself.
  - This adds **checks and balances** to insider threats but also management complexity

Q&A