Solution Brief

Direct Access Management

Ironsphere
A Krontech Company

Introduction/Background

Ironsphere provides privileged access security capabilities to prevent credential theft of super-user accounts, eliminating unsupervised user access to the technology infrastructure, including servers, VMs, databases, and network elements. Ironsphere helps organizations to centrally enforce access policies, such as who can access which servers/ systems, and what they can do once connected, based on their role in the organization. With flexible access request and approval flows, Ironsphere ensures privileges are used only for legitimate business purposes, and provides audit trails, regulatory compliance reports, VCR-like replay of all sessions, and live session watching, based on a man-in-the-middle architecture.

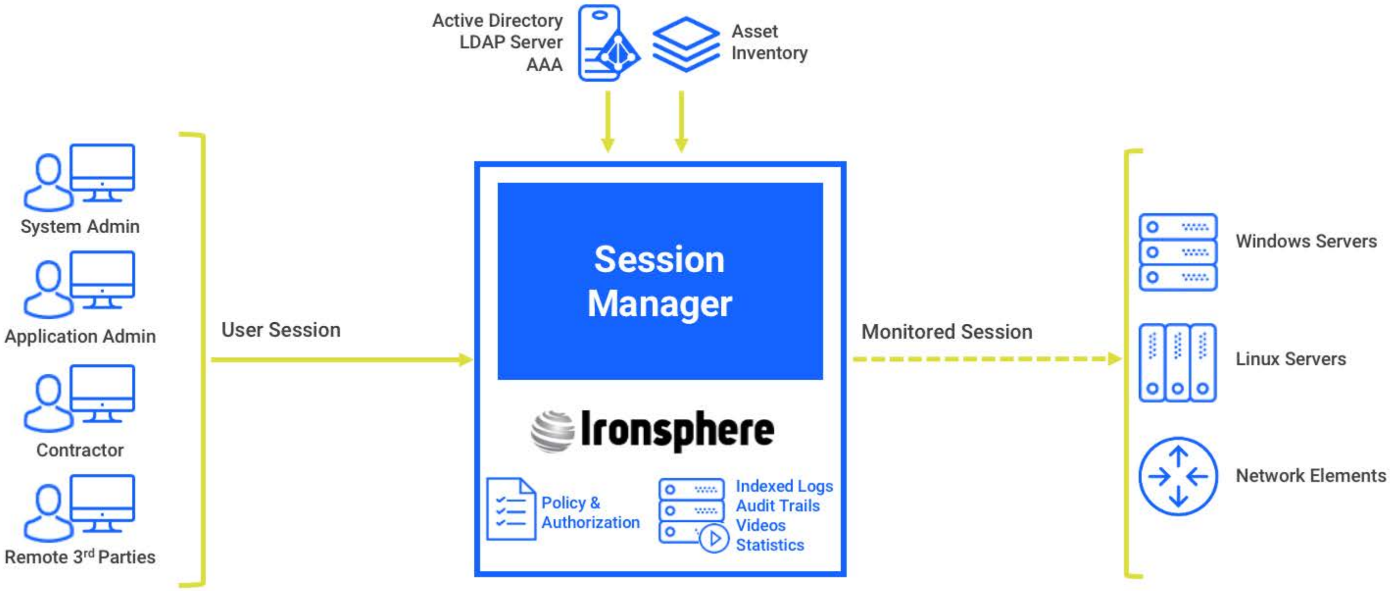

Figure 1— Ironsphere Session Manager, High Level Topology

Challenge/Problem

As long as users access target hosts through Ironsphere, all sessions are supervised, and user activities are tracked/monitored using a man-in-the-middle architecture. The challenge is how to manage user access if they attempt to access target hosts directly, bypassing Ironsphere.

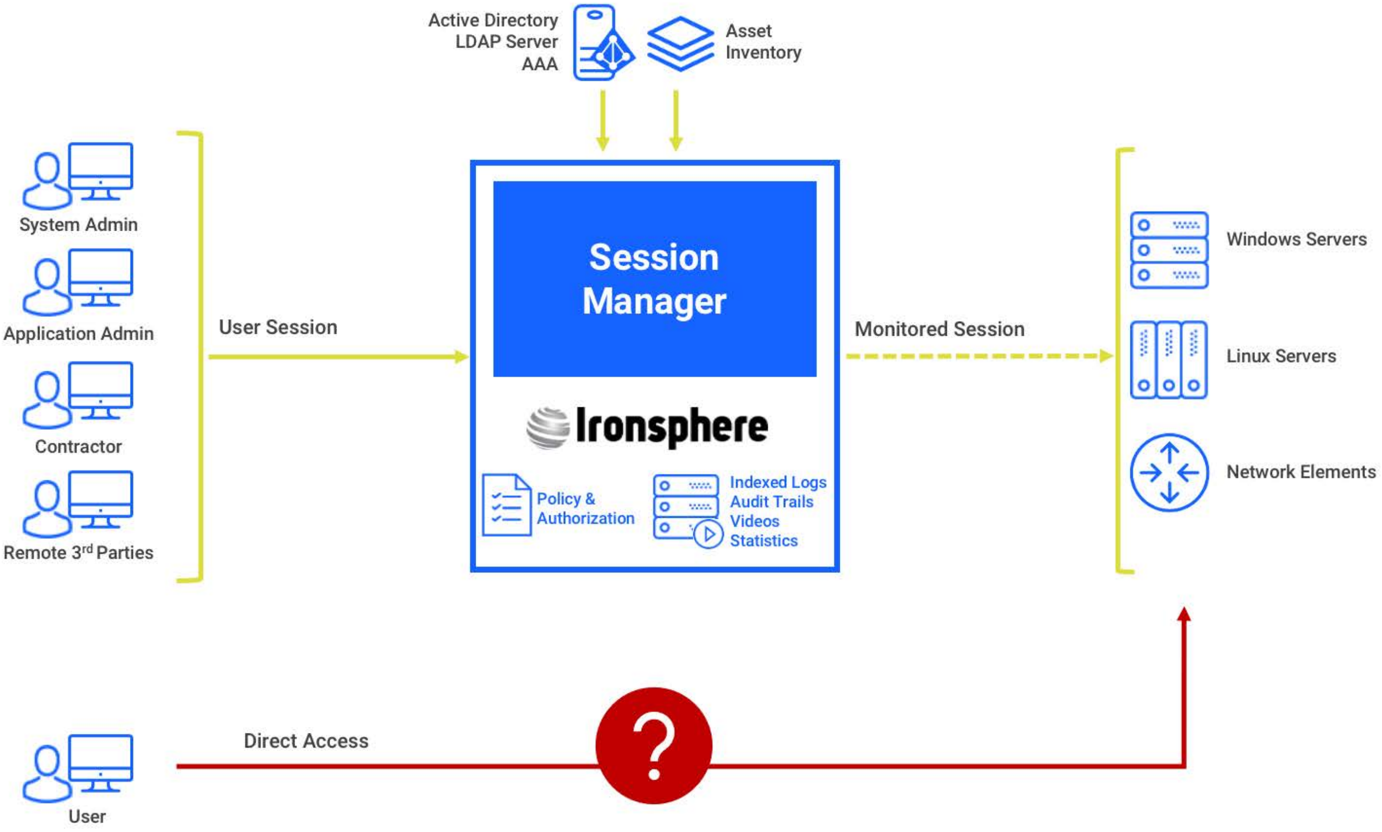

Figure 2 — Users Log in to Remote Hosts Directly

Below we detail the available solutions organizations can select from to mitigate this risk.

Solutions

Approach 1: Changing the Owner of the Privileged Credentials (from Users to Ironsphere)

Ironsphere's Dynamic Password Controller eliminates personal privileges on target hosts, securely stores shared/non-personal super-user accounts in its encrypted digital vault, and automatically changes them at regular intervals. Once a super-user account is vaulted and updated by Ironsphere, users will no longer have direct access to the new credentials, effectively making Ironsphere the single owner of that super-user account. When privileged users need the credentials for legitimate business purposes, the only available access is through Ironsphere, or by getting the password from Ironsphere for direct access. This prevents unsupervised direct user access to target hosts, allowing Ironsphere to centrally track/monitor the usage of privileged credentials, and enabling personal accountability based on which specific user accessed which credentials and for what purpose.

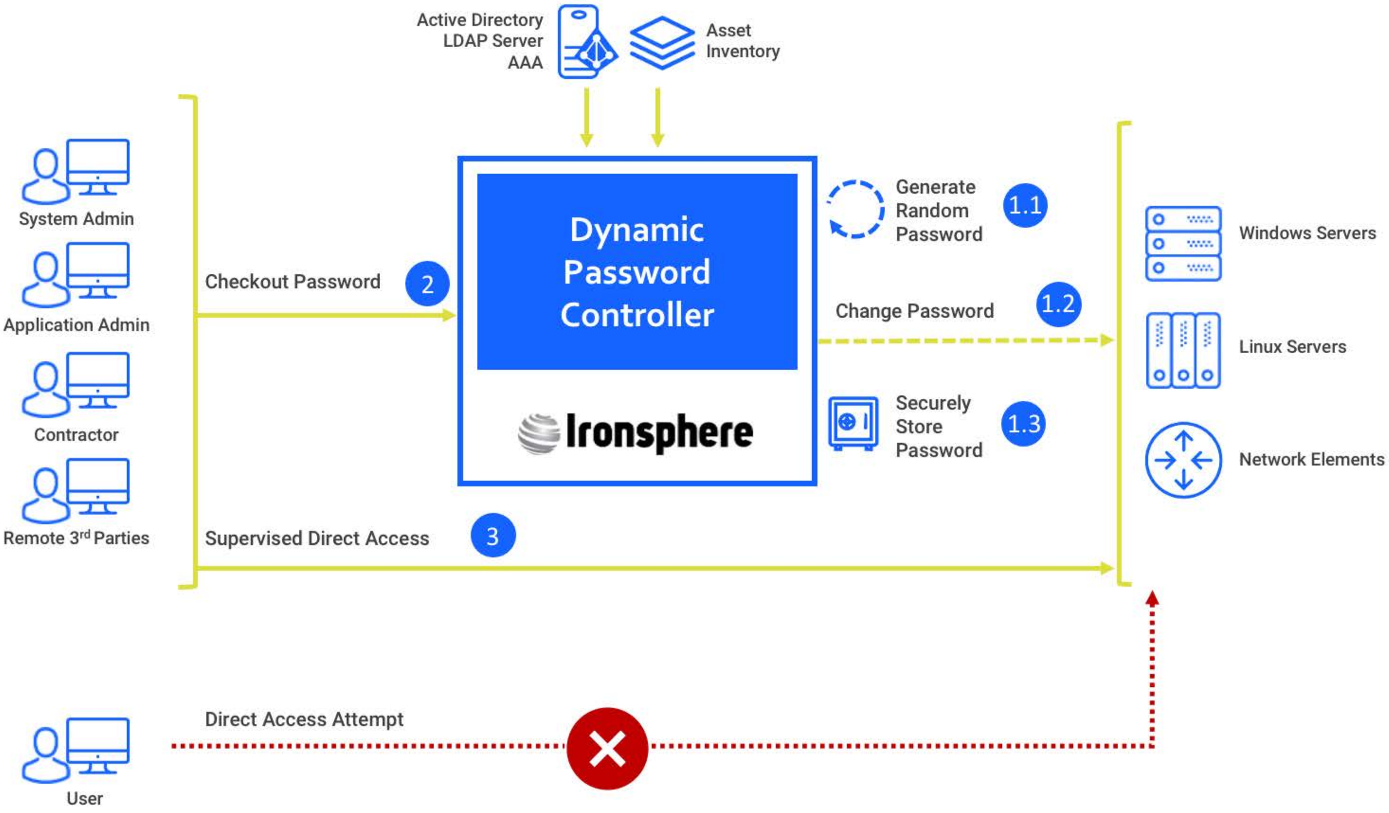

Figure 3 — Ironsphere Dynamic Password Controller – High Level Topology

Solutions

Approach 2: Blocking Direct Access at the Network Level

Configuring rules in network devices to only allow Ironsphere to access target hosts and blocking all other sessions will prevent any unsupervised privileged access. Such rules can be configured as ACLs (Access Control Lists) on network elements, or as Access Rules on firewalls.

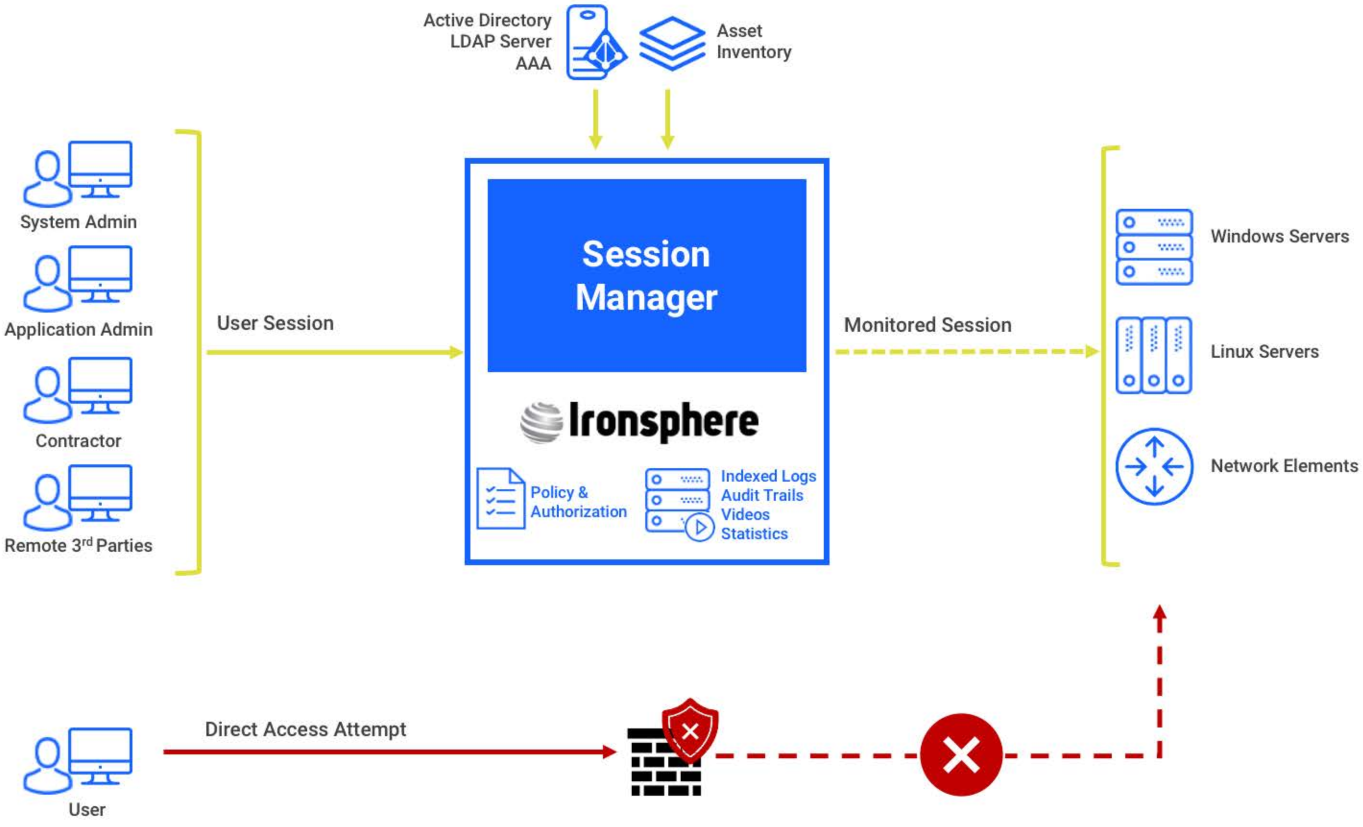

Figure 4 — Blocking Direct Access at the Network Level

Solutions

Approach 3: Detect and Respond to Direct Access Attempts

SIEM (Security Information and Event Management) products have become a core part of identifying cyber attacks. Organizations that have a SIEM product in their enterprise infrastructure and collect access logs from target hosts, can design a workflow on SIEM to detect unsupervised direct access attempts (i.e., source IP address of a session is NOT Ironsphere) and respond accordingly, such as sending a notification/alarm to Security Operations for further process.

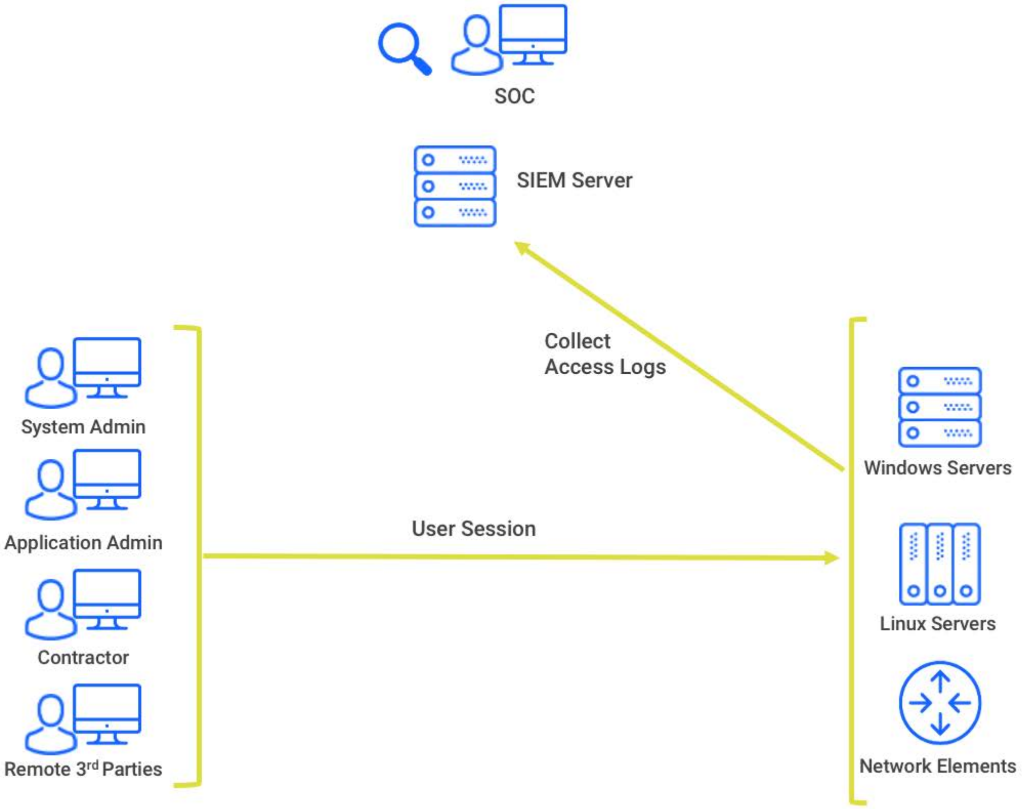

Figure 5 — SIEM Server Collects Access Logs from Hosts for SOC Team to Investigate

Solutions

Approach 4: Deploying Access Controller Software on Hosts/Servers

Access Controller software agents can be installed or enabled on target hosts to manage user direct access. Access Controller software agents handle remote user authentication through a centralized server, by forwarding user access attempts, along with user credentials, to a centralized server in order to determine whether access will be allowed or not. Ironsphere handles both policy decisions and policy enforcements while running based on its man-in-the-middle architecture. In an Access Controller software agent architecture, although Ironsphere continues to run as a centralized server and handling policy decisions, policy enforcements are handled by agents running on hosts.

Ironsphere provides agent software for Windows and Linux servers, to be run as policy enforcement points on target servers. While network elements (e.g., routers, switches) do not allow custom software applications to be installed, they do provide built-in TACACS or RADIUS access controller software agents, which can work through a centralized server. For network elements, Ironsphere runs as a policy decision server, and the network elements' built-in TACACS/RADIUS agents run as policy enforcement points.

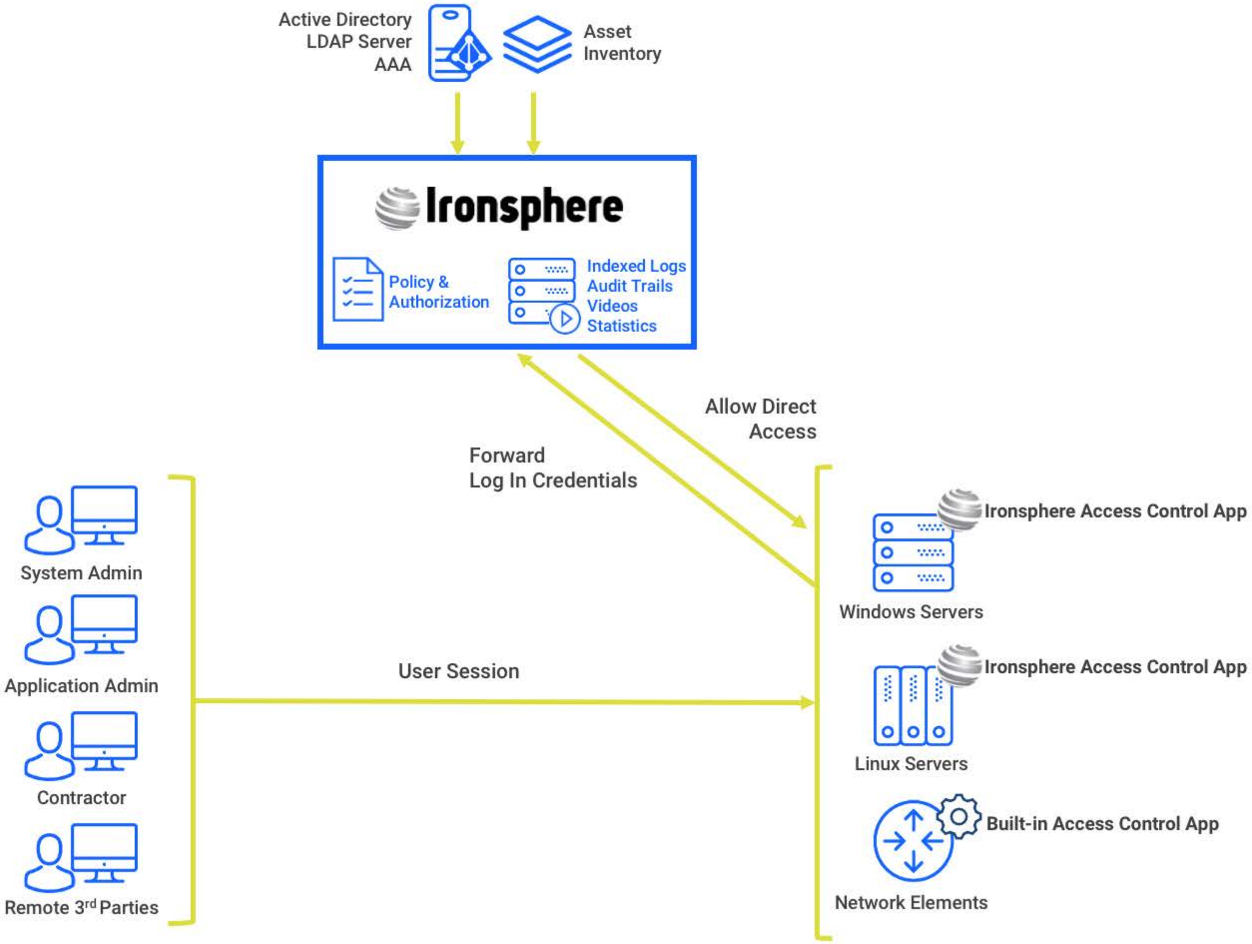

Figure 6 — Deploying Access Control Agent Software on Host Servers

Conclusion

Ironsphere provides multiple solutions to manage direct access, for a flexible approach depending on the organization's specific requirements. The available options can be used individually or combined in a single deployment. This decision will be primarily driven by the nature of the infrastructure and the desired level of control/security. Please refer to our system-based solutions briefs (Windows, Linux, Network Elements) for detailed use case coverage. As an example, here are two simple use cases:

Example 1

If network level restrictions are feasible, create a bottleneck between users and hosts in order to funnel all users to the Ironsphere platform for their access needs to the remote hosts. This approach works particularly well when most of the host/servers are located in a datacenter, while most users are in a separate office, so that the required network level control capabilities are already in place, making this scenario easy to implement. As an additional security layer, alerts can be setup via SIEM to detect any access attempts not originating from Ironsphere.

Example 2

In some situations, network level restrictions may not be feasible. A good example is a large office where all users and servers are on a single flat network. The simplest approach would be to vault all servers/network elements super-user account credentials in the Ironsphere Dynamic Password Controller. This will grant control and visibility of all accounts through a single pane of glass, even for the most diverse mix of infrastructure setups.

All vaulted passwords can be automatically changed at regular intervals utilizing the Password Rotation feature, taking it a step further. This process ensures that there are no stale passwords, misplaced and forgotten by users, or left unchecked in automation scripts, creating potential vulnerabilities.

Ironsphere
A Krontech Company