The hybrid cloud represents a new generation of computing. Inevitably, advancements in infrastructure bring new requirements for security solutions. We’ve identified three core capabilities essential to successful Next-Generation Privileged Identity Management.

1. **Comprehensive Integrated Control Set (No Point Products)**
   - **Strong Authentication/Identity as the Perimeter**
     - Identity is defined in multiple systems—next-generation solutions must bridge and federate with existing identity stores to avoid creating new ‘islands of identity.’
     - Provide high assurance capabilities such as smart card and other multi-factor support to improve authentication and comply with mandates.
   - **Password/Credential Management**
     - Supporting privileged users of all kinds via consoles and underlying management APIs, with support for application-to-application password controls.
     - Vaulting in an encrypted credential safe.
     - Automated management of passwords and credentials, including creation, presentation, and change.
     - ‘Break Glass’ delivery of credentials for approved emergency access.

2. **Full Hybrid Cloud Protection**
   - **Protect New Cloud and Virtualization Management Consoles**
     - AWS Management Console and management APIs
     - VMware vCenter Server Console
     - Microsoft Online Services
   - **Role-Based Access Control**
     - Limit to authorized systems
     - Limit to authorized commands
     - Prevent execution of black-listed commands
     - Prevent ‘leapfrogging’ to unauthorized systems
   - **User Monitoring, Activity Logging, and Reporting**
     - Alerts on attempted policy violations
     - User warnings and notifications, including session termination and account suspension
   - **Session Recording**
     - RDP/VNC
     - SSH
     - Web Applications

3. **Dynamic Architecture**
   - **Privileged Identity Management must keep pace with the rapidly changing hybrid cloud environment to avoid becoming a drag on operations**
     - Automated discovery of resources
     - Automated policy provisioning – e.g., typing in policies for 100 new servers is a non-starter
   - **Scale and Availability - Supporting massive cloud/virtual deployments**
     - Built-in clustering/high availability across environments.

<table>
<thead>
<tr>
<th>Next-Generation PIM Required Features</th>
<th>Xsuite®</th>
<th>Traditional PIM Software</th>
<th>Traditional Password Management Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive Integrated Controls</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Full Hybrid Cloud Support</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Architected for Dynamic Virtual and Cloud Environments</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

Xceedium Xsuite provides comprehensive Next-Generation Privileged Identity Management and Protection.
About Xceedium

Xceedium, Inc., is the leading provider of privileged identity management solutions for hybrid-cloud enterprises. Xceedium helps large companies and global government agencies reduce the risks privileged users and unprotected credentials pose to systems and data. Xceedium’s Xsuite vaults privileged account credentials, implements role-based access control, and monitors and records privileged user sessions. With unified policy management, the Xsuite platform enables the seamless administration of security controls across the hybrid cloud, protecting systems in traditional data centers, virtual private clouds, or public cloud infrastructure.

Xceedium’s solutions enable organizations to comply with security and privacy mandates such as PCI DSS, FISMA, HIPAA, and NERC CIP. Our products provide industry-leading reliability, availability, and scalability, and include the most highly certified products in the market, with designations including FIPS 140-2 validation, Common Criteria EAL4+ certification, and inclusion on the U.S. DOD Unified Command Approved Products List (UC/APL).

For more information, please visit www.xceedium.com.