

Managing Remote User Threats

Solution Brief

In an effort to reduce operating costs companies have made changes to their business plans that require secure remote access for users who are considered high risk.

- Increased outsourcing in the form of application developers, database administrators, the outright management of parts or all of their IT operations centers and help desk organizations
- Increased use of contractors for peak load situations
- The need to automate remote access and policy enforcement to enable vendors to meet more stringent SLA's
- Reduced travel budgets which require administrators and other employees to work remotely or to administer distributed environments

Concurrently there are increased pressures from auditors, agency mandates and compliance requirements to protect critical infrastructure and sensitive data. Heightened levels of risk are introduced by allowing these new outsiders with unmanaged endpoints inside the datacenter or protected enclaves. To mitigate these risks and still provide the access levels needed to operate efficiently, companies are seeking next generation technology to meet these new requirements for Controlling Access and Auditing remote high-risk users.

High risk can be very skilled technical users who can circumvent security controls and often have elevated privileges across the broad infrastructure. High risk can also be non technical users who are working in or around highly sensitive areas. Most often they connect using un-managed endpoints significantly increasing the risk potential.

The Xceedium GateKeeper provides organizations the ability to easily and cost-effectively reduce the complexity and cost of controlling and auditing high-risk users accessing critical infrastructure from any endpoint. Using a feature-rich, hardened appliance the GateKeeper is an all-in-one solution. It is centralized in the network and is easy to deploy and maintain. With a blue chip customer base in both government and commercial sectors, the Xceedium GateKeeper delivers a unique solution for controlling access and auditing high-risk users and provides the following benefits:

Key Benefits

Zero Footprint Access

- User is granted no physical footprint on the network
- No client side installation. User only needs a supported Java enabled web browser
- No ability to propagate viruses or malware
- No ability to copy files or print locally

Compartmentalization

- Provides integrated applets which allow policy to restrict users to fine grained compartments and limit visibility to authorized areas
- Gain visibility to source IP address despite the use of NAT IP groupings for complete accountability

Containment

- Patented Leap Frog Prevention™ keeps high-risk users from traversing between authorized work areas and other areas within the IT infrastructure
- Uses a white/black list approach at the server level and command line to prevent users from leaving authorized areas

Monitoring, Remediating, Alerting

- Monitors policy and enforces containment to authorized areas
- Empowers companies with the ability to deny access and alert on violations
- Provides corrective action capabilities based on customer defined thresholds

Tracking and Logging

- All command line activity is monitored, recorded and archived for audit purposes
- Agent less, RDP Graphical session recording allows all remote high-risk user activities to be recorded and policy violations to be bookmarked and linked back to specific controls
- Provides an end-to-end view of activity, in one central place, at the source IP and unique ID level
- User event activity is tracked and logged, including the date and time the user logged into a specific device as well as the access method used. Drilldown to specific session detail is available for audit and forensics purposes
- All log data is easily exportable to Syslog, SIEM, and event correlation engines

Targeted Reporting

- Custom and ad hoc reports created from all user events and activities can be run in real time or saved for later viewing
- Automated creation, delivery and distribution of reports via email