

# Xceedium Xsuite™



## Zero Trust Access Control Platform



Xsuite is designed to defend organizations against insider threats. It protects organizations from the severe risks that system and network administrators, or *privileged users*, and their administrative accounts pose to corporate networks and data.

Xsuite integrates three award-winning software modules on a highly scalable, hardened appliance. The platform goes far beyond the popular “least privilege” concept, enabling your team to implement the full complement of security controls necessary in today’s dynamic business and technology environment. We call it **Zero Trust Access Control**.

With Xsuite, you can orchestrate eight essential *Zero Trust* controls through a single, unified policy management system and achieve enterprise-level, role-based access control with ease. These modules run on the Xsuite platform:



**GateKeeper™** — granular access control, containment and session monitoring



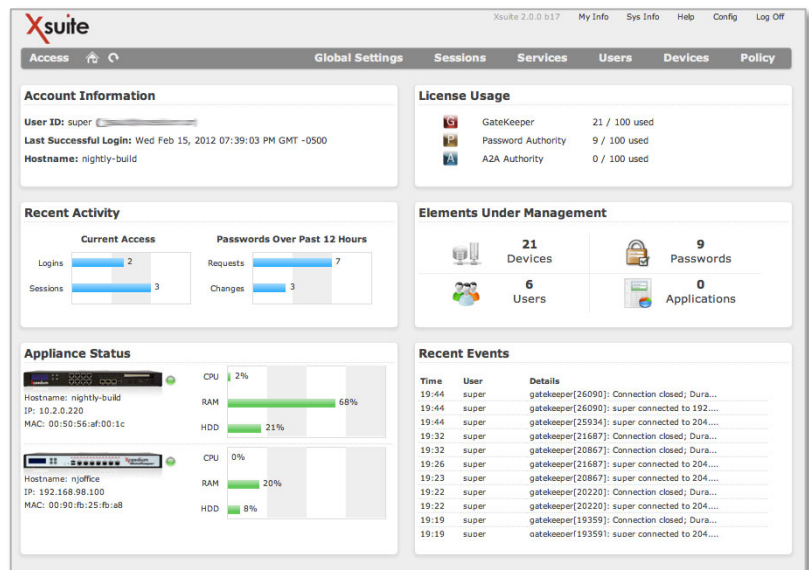
**Password Authority™** — vaults and manages privileged user credentials



**A2A Authority™** — vaults and protects the passwords needed for scripts and applications

### Xsuite Use Cases:

- Privileged user access control
- Third-party access control
- Regulatory compliance
- Secure remote management
- Logical network segmentation
- Session monitoring
- User password vaulting
- Application password vaulting

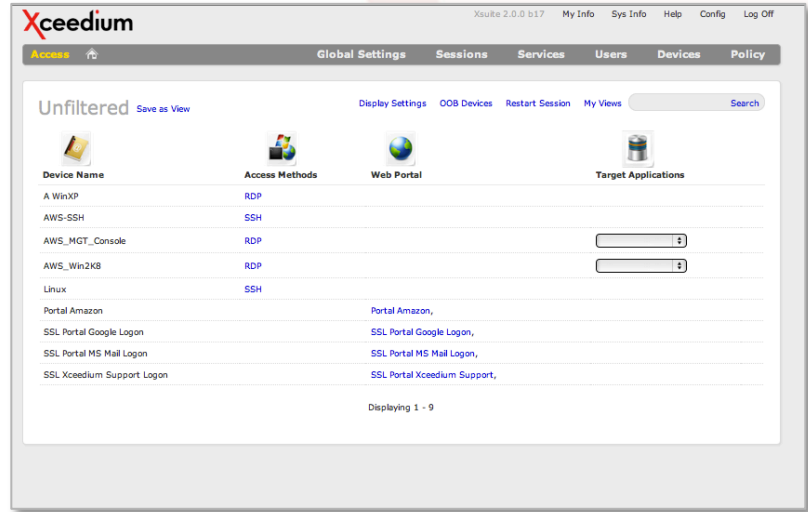


# Xsuite: Eight Essential Zero Trust Controls



**Control Access.** DAPE (Deny All Permit by Exception). A personalized web portal reveals only the target devices and access methods for which users are explicitly granted permission.

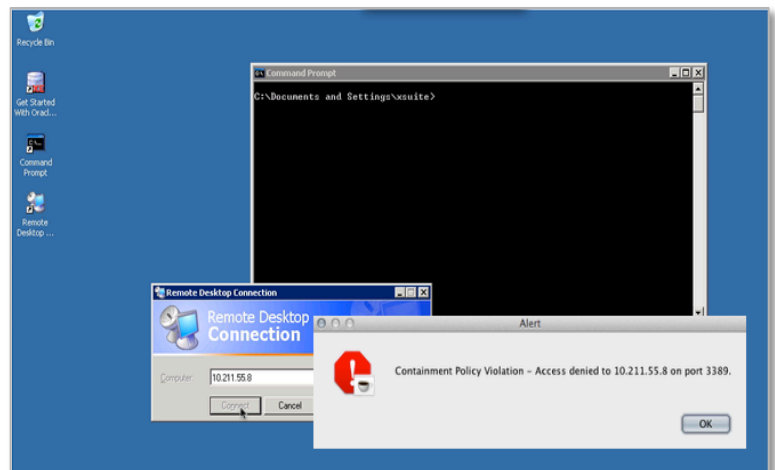
The portal provides secure single-sign-on access, so busy system and network administrators can quickly access resources. Xsuite grabs passwords from the vault and presents it to the target systems behind the scenes. Xsuite keeps passwords off end devices; users don't know the passwords and malware can't snatch them.



**Protect and manage credentials.** Passwords and their credentials are stored in a secure vault and remain encrypted when traversing the network. This includes both privileged user and application-to-application or application-to-database passwords. Credentials can be kept off end-nodes, kept out of applications and scripts, and kept out of sight from users and developers. Passwords are created and controlled by policy through their full lifecycles; one-time or time-limited "break glass" passwords are available in case of emergencies.

**Prevent anonymous activity on shared accounts.** Each user is securely authenticated to Xsuite before he or she is able to access systems, providing fully attributed use of each target system. Xsuite requires ID/password and integrates with strong authentication systems. Privileged users are specifically identified and tracked. If a target device supports only a single admin account (e.g., a root account), you still know exactly who was on the system, what they did and when they did it.

**Contain users.** Xsuite prevents users from exploiting access to one server to gain entree to other devices on the network (i.e., "leapfrogging" or "RDP Hopping"). And even if a user has logical or physical access to a device, he or she doesn't have the password for entry.



```

File Edit SmartButton Terminal Help
Warning: Activity is being monitored
Linux debian508 2.6.26-2-686 #1 SMP Sat Sep 17 16:52:11 UTC 2011 i686

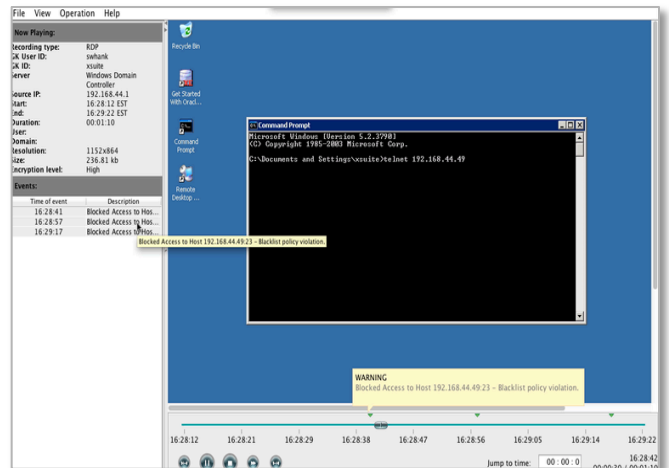
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 4 15:42:59 2012 from 192.168.44.47
xsuiteash@debian508:~$ pwd
/home/xsuiteash
xsuiteash@debian508:~$ whoami
xsuiteash
xsuiteash@debian508:~$ as
Warning: ssh is an unauthorized command.
You have 1 violations. Your session will be terminated and account deactivated if
you have 3 more violations continue.
Please contact the administrator if you have any questions
xsuiteash@debian508:~$ restart
Warning: restart is an unauthorized command.
You have 2 violations. Your session will be terminated and account deactivated if
you have 1 more violations continue.
Please contact the administrator if you have any questions
xsuiteash@debian508:~$ reboot
xsuiteash@debian508:~$ reboot
Warning: reboot is an unauthorized command.
You have 3 violations. Your session will be terminated and account deactivated if
you have 0 more violations continue.
Please contact the administrator if you have any questions
Violation limit reached: 3
terminating session
  
```

**Control commands.** Implement whitelist- or blacklist-based policies to limit what commands administrators can execute.

**Record sessions.** Record graphical and terminal sessions. Alert and warning tags are inserted into the stream, enabling simplified forensic analysis. Xsuite supports thousands of simultaneous recordings with a single appliance.

**Log everything.** Xsuite logs everything privileged users do when accessing target network devices. It also logs all activities that the Xsuite administrator and other Xsuite users do (e.g., changing configuration settings, setting policies, reviewing log entries or viewing recordings). Logs are kept in tamper-proof files.



Start DateTime	End DateTime	User	Groups	Device	Type	Size	Status
2012-01-04 16:28:12	2012-01-04 16:29:22	swhank	Xsuite	Windows Domain Controller	RDP	236K	View Recording
2012-01-04 16:18:39	2012-01-04 16:20:13	swhank	Xsuite	Database Server	CLI	1K	View Recording
2012-01-04 15:40:14	2012-01-04 15:41:01	swhank	Xsuite	Database Server	CLI	1K	View Recording
2012-01-04 15:36:37	2012-01-04 15:38:38	swhank	Xsuite	Windows Domain Controller	RDP	275K	View Recording
2012-01-04 15:36:09	2012-01-04 15:36:17	swhank	Xsuite	Windows Domain Controller	RDP	230K	View Recording
2012-01-04 15:02:24	2012-01-04 15:04:50	swhank	Xsuite	Windows Domain Controller	RDP	699K	View Recording
2012-01-04 15:01:50	2012-01-04 15:02:08	swhank	Xsuite	Database Server	CLI	1K	View Recording
2011-12-27 15:04:20	2011-12-27 15:36:54	swhank	Xsuite	Windows Domain Controller	RDP	OK	Encoding In-Progress
2011-12-27 14:38:23	2011-12-27 14:39:04	ExternalUser	Xsuite	Windows Domain Controller	RDP	180K	View Recording
2011-12-27 14:07:45	2011-12-27 14:10:37	swhank	Xsuite	Windows Domain Controller	RDP	109K	View Recording
2011-12-27 14:02:22	2011-12-27 14:03:33	swhank	Xsuite	Database Server	CLI	1K	View Recording
2011-12-27 13:06:55	2011-12-27 13:08:23	swhank	Xsuite	Windows Domain Controller	RDP	101K	View Recording
2011-12-27 13:05:42	2011-12-27 13:05:55	swhank	Xsuite	Database Server	CLI	1K	View Recording
2011-12-27 13:01:53	2011-12-27 13:01:56	swhank	Xsuite	Web Host	CLI	1K	View Recording
2011-12-27 12:37:03	2011-12-27 12:37:07	swhank	Xsuite	Windows Domain Controller	RDP	58K	View Recording
2011-12-27 12:36:58	2011-12-27 12:37:35	swhank	Xsuite	Windows Domain Controller	RDP	106K	View Recording

**Alert for policy violations.** Send alerts to the Xsuite dashboard and to other systems via email, log integration and SNMP for immediate action.



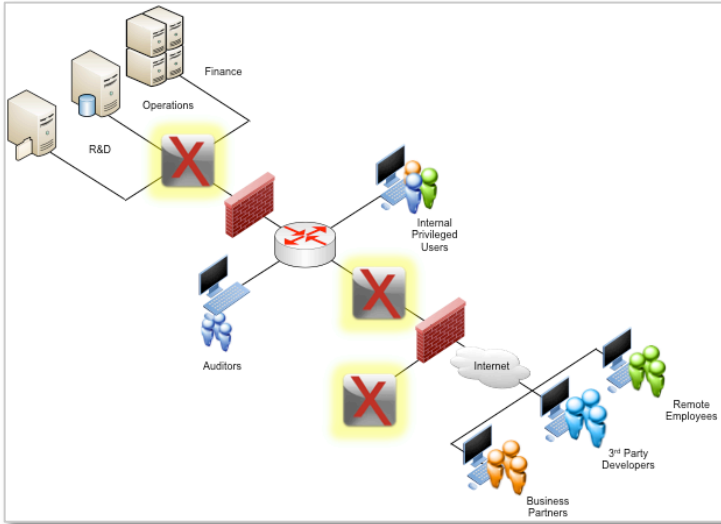
## Xsuite: Features and Benefits



Features	Description	Benefits
<b>Eight Essential Zero Trust Controls</b>	<p>Full spectrum of controls for prevention, detection and response/forensics in a single, integrated solution.</p> <p>Controls are turned on as needed and managed at the group or individual level.</p> <p>Enforces least privilege, separation of duties and role-based access control.</p>	<ul style="list-style-type: none"> <li>• Comprehensive protection for enterprise customers</li> <li>• Flexibility to support multiple use cases and configurations</li> <li>• Improved security and compliance</li> </ul>
<b>Unified Policy Management</b>	<p>Controls users and their devices through a single policy-management regime.</p>	<ul style="list-style-type: none"> <li>• Reduced total cost of ownership</li> <li>• Clarity regarding which controls are in place and for whom — reduces gaps in protection and ensures proper compliance documentation</li> </ul>
<b>Single Sign-on</b>	<p>After secure authentication, privileged users have “one-click” access to the resources that they need to manage.</p>	<ul style="list-style-type: none"> <li>• Increases productivity for busy systems, network, database and application administrators</li> <li>• Access provided without end user (or malware) knowing credentials</li> </ul>
<b>Clustering</b>	<p>Active/active clustering support.</p>	<ul style="list-style-type: none"> <li>• High performance, availability and reliability</li> </ul>
<b>Integration</b>	<p>Integration with key security and network management infrastructure:</p> <ul style="list-style-type: none"> <li>• AD/LDAP</li> <li>• X.509/PKI</li> <li>• Authentication systems (Radius, PIV/CAC, etc.)</li> <li>• SIEM &amp; log management</li> <li>• SNMP</li> </ul>	<ul style="list-style-type: none"> <li>• Leverage current investments to improve security and reduce operational costs</li> <li>• Strong authentication integration ensures the “keys to the kingdom” are well protected</li> <li>• Ensures that IT Security and SOC team members know about important events in real time</li> </ul>
<b>Hardened Appliance</b>	<p>A purpose-built system that includes the security performance and reliability features necessary for its key role in the network.</p>	<ul style="list-style-type: none"> <li>• Reduced implementation time — Xceedium routinely has multi-thousand node customers up and running in less than a week</li> <li>• Minimize total cost of ownership — Xceedium manages, secures, tests and delivers updates for the whole solution stack, so you don’t have to worry about it</li> </ul>
<b>Highly Certified Solution</b>	<p>Xceedium solutions have been validated to meet highest levels of security regulations in programs such as:</p> <ul style="list-style-type: none"> <li>• FIPS 140-2, Level 2 Certified</li> <li>• Common Criteria, EAL 4+ Certified</li> <li>• U.S. DOD Unified Command Approved Products List (UC/APL)</li> </ul>	<ul style="list-style-type: none"> <li>• We take security as seriously as you do. You can rest assured that your systems maintain the highest levels of protection</li> <li>• Government customers can select Xsuite for their most critical systems</li> </ul>



## Xsuite: In Enterprise Networks



Xsuite appliances can be placed in the DMZ, behind the corporate firewall, or at the juncture of physical network segments, depending on the use case. Communications to and from Xsuite are over port 443.

## Xsuite: Broad Platform Support

**A2A Authority development language support** (“requesting” applications can be coded in the following languages):

- C
- C++
- C#
- Visual Basic
- VB.Net
- VC
- VC++
- VC#
- Java
- Perl
- Korn Shell

**A2A Authority client support** (“requesting” applications can be run on the following systems):

- Windows XP, Windows Server 2003 / 2008R2
- Solaris 8/9/10
- Red Hat Enterprise Linux 5
- SUSE
- AIX
- HPUX 11i
- AS/400

**A2A Authority target application support** (“requesting” clients can connect to the following “target applications”):

- SAP
- Oracle
- Sybase
- MySQL
- MS SQL
- DB2
- Many others via Xceedium’s customizable framework



### Password Authority Supports Management For:

- Windows Domain, local administrator and service accounts
- Red Hat SUSE / Mandrake / Debian Linux
- AIX 5.1, 5.2, 5.3
- HPUX 11i
- Solaris 8, 9, 10
- AS/400
- Cisco, Juniper, other Telnet & SSH devices
- LDAP / Active Directory / eDirectory / SunOne
- SAP, Remedy
- Oracle, Sybase, MySQL, MS-SQL, IBM-DB2
- SPML2 compliant interfaces
- Vmware ESX, ESXi
- Weblogic
- Crystal Reports

### Xsuite: Runs on Xceedium's Hardened Appliances

System Components	Branch Office (Model X102P)	Enterprise Data Center (Model X206P)
Chassis	1U IPC	1U IPC
Power Supply	250W Power Supply Unit (PSU) (220W at 50+°C)	Dual Hot-Swap Power Supplies 250W Power Supply Unit (PSU)
System Board	Single Board Computer (SBC) Intel Chipset	Single Board Computer (SBC) Intel Chipset
CPU	Intel Core2 Duo 2.13GHz	Intel Xeon E5 645 Processor (Hexacore, 2.4GHz)
Memory	4 GB DDR2	6 GB DDR3 1066Mhz ECC Memory
Primary Storage	32 GB Solid-State Drive (SSD)	32 GB Solid-State Drive (SSD)
Secondary Storage (backup)	32 GB Solid-State Drive (SSD)	32 GB Solid-State Drive (SSD)
Display	2 Line x 16 Char LCD Display	2 Line x 16 Char LCD Display
<b>Standard Interfaces</b>		
Network	Six (6) 1-Gigabit Ethernet Ports	Ten (10) 1-Gigabit Ethernet Ports
LCD Inputs	Four-Button Control	Four-Button Control
Serial	One RJ-45 Console Serial Port	One RJ-45 Console Serial Port
<b>Physical Specifications</b>		
Height	1.73" (4.4 cm)	1.73" (4.4 cm)
Width	17" (43.18 cm)	17.4" (44.3 cm)
Depth	14" (35.56 cm)	21.9" (55.6 cm)
Unit Weight	14 lbs. (6.3 kg)	38 lbs. (approx.)
Shipping Weight	23.5 lbs. (10.6 kg)	48 lbs. (approx.)
Enclosure	Fits Standard 19" Rack	Fits Standard 19" Rack
<b>Environmental Specifications</b>		
Storage Environment	-20° C to 70° C , 5 – 95% RH	0° C to 70° C , 5-95% RH
Operating Environment	0° C to 50° C, 20 – 90% RH	5° C to 35° C, 20-90% RH
Internal Ventilation	3 x 2.8 cm 24 CFM fans	4 x 2.8 cm 24 CFM fans

