



whitepaper

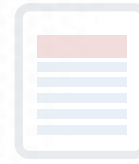
Azaleos SecureX Technology

July 1, 2009



The SecureX Management Console provides Azaleos with instant access to a powerful systems administration toolbox including remote console, remote PowerShell, patch management, and a library of commands. This whitepaper provides a detailed overview of the Azaleos SecureX system and technology.

1938 Fairview Avenue East,
Suite 100
Seattle, WA 98102
206.926.2000
www.azaleos.com



Azaleos SecureX Technology

July 1, 2009

Introduction

What Is SecureX?

SecureX is Azaleos' remote management system for Microsoft Exchange, SharePoint, Active Directory and Office Communications Server. SecureX is a one-of-a-kind tool which provides the Azaleos Network Operations Center (NOC) Technicians with secure, instant, and auditable access to remotely manage customer servers.

SecureX uses industry standard encrypted connections requiring two factor authentication (key and password). SecureX eliminates the need for VPN access, allowing Azaleos to resolve problems faster.

The SecureX Management Console provides Azaleos NOC Technicians with instant access to a powerful systems administration toolbox including remote console, remote PowerShell, patch management, and a library of commands.

The Management Console enables NOC Technicians to manage customer servers with a consistent, repeatable, and efficient remote management process.

SecureX is integrated with the Azaleos ViewX case management system and knowledge base. SecureX records every command in the Audit Database, logging the User ID, command, command output and result, the target customer server, and time issued.

Audit reports are available from the Azaleos ViewX case management system and additional reports can be generated based on customer need.

The primary purpose of this technical whitepaper is to provide Azaleos customers and prospects with a detailed overview of the SecureX system and technology.

SecureX is a one-of-a-kind tool which provides the Azaleos Network Operations Center (NOC) Technicians with secure, instant, and auditable access to remotely manage customer servers.

SecureX uses industry standard Secure Shell Protocol (SSH) to provide strong encryption, making only outbound connections from the customer server to Azaleos.

SecureX Security Overview

SecureX uses industry standard Secure Shell Protocol (SSH) to provide strong encryption, making only outbound connections from the customer server to Azaleos. SSH uses public key cryptography to identify the SecureX Master Control Server and allows the server to identify and authenticate the client server. NOC Technician access control and security policy are enforced by Active Directory Security Groups, first by the SecureX Management console, and then by the SecureX Master Control Server ensuring that only authorized NOC Technicians have access to the SecureX system. All NOC Technician access is recorded in the Audit Database.

The SecureX Agent running on a customer server initiates an outbound connection to the SecureX Master Control Server through cryptographically strong SSH tunnels. SSH tunnels are used to establish a point to point connection directly from the customer server to the SecureX Master Control Server, eliminating the need for VPN access. Only SecureX application traffic is sent through the SSH tunnel, unlike most VPN's that bridge networks and allow general network traffic from any application. The SSH Protocol and asymmetric keys provide assurance of identity on both sides of the connection and prevent a Man in the Middle Attack.

SSH keys are issued from the private Azaleos Public Key Infrastructure (PKI), managed by Azaleos SecureX system administrators. Each customer server and individual NOC Technician are issued a unique asymmetric key pair. Keys are standard SSH RSA Identity keys (SSH key). SSH keys are asymmetric, meaning one key is used to encrypt a message (the private SSH Key) and another key (the public SSH Key) is used to decrypt the message. Public keys are installed on the SecureX Master Control Server and private keys are installed on the customer server

and NOC workstation. SSH Keys identify authorized NOC Technicians and OneServer computers to the SecureX Master Control Server. Access is granted only when the key is valid on both sides. Access to the SecureX system can be blocked by revoking the public key on the SecureX Master Control Server. Azaleos secures administrative access to customer servers using Active Directory security groups in a separate administrative domain from the Azaleos domain used for Azaleos production services. SecureX administrators grant users rights on customer systems by adding them to universal security groups based on their role. NOC Technicians or Professional Services staff configure customer servers into administrative entities called Azaleos Servers. SecureX creates Organizational Units (OUs) for each Azaleos Server under customer specific OUs that are organized into three levels of access. Administrative access is granted to a NOC Technician if they have the same level of access required for the customer server.

SecureX Levels of Access

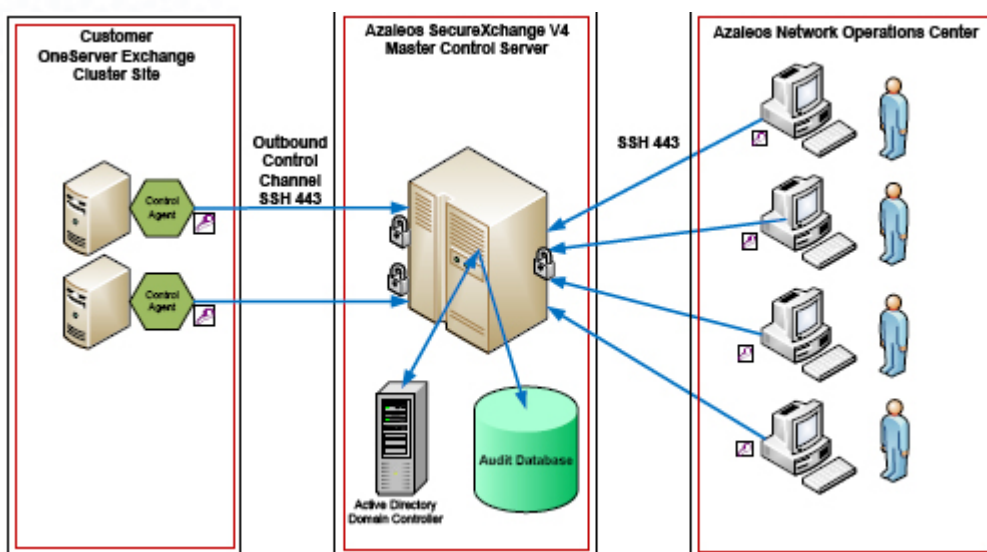
SecureXchange defines the following three levels of access that build on each preceding level:

LEVEL 1	Limited diagnostic access to the system used for problem determination and some customer reporting functions
LEVEL 2	Non destructive maintenance access used for some routine maintenance functions that do not involve significant system configuration changes that might lead to permanent damage
LEVEL 3	Unrestricted access or equivalent to audited administrative shell access

SecureX Security Overview, continued

The SecureX Management Console ensures the NOC Technician has permission to access the system by ensuring they are in the right Azaleos Domain Security Group. Every SecureX command by a NOC Technician is checked for authorization against a specific customer server using the Active Directory security groups described above before being forwarded to the target customer server. SecureX records every command issued by a NOC Technician in the Audit Database logging the User ID, command, command output and result, the customer server hostname, and time issued. Audit reports are available from the Azaleos ViewX case management system and additional reports can be generated based on customer need. Additionally, during a remote console session SecureX logs every program run by the administrator, recording the User ID, executable, customer computer hostname, and time the program was run. SecureX also has the capability to record the screen of the remote console session for customers that require more in depth auditing.

SecureX Deployment Diagram



SecureX In Action

When a customer server boots, the SecureX Agent makes an outbound connection through an encrypted SSH tunnel to the SecureX Master Control Server. The SecureX Master Control Server accepts this connection only if the customer server has a valid key. Once connected, this establishes a SecureX control channel for the SecureX command / response protocol. The customer server remains connected and waits for commands from the SecureX Master Control Server on the control channel. This persistent connection enables instant access to any customer server. The SecureX Master Control Server handles routing commands and responses between the customer server and SecureX Management Console.

Every SecureX command by a NOC Technician is checked for authorization against a specific customer server using the Active Directory security groups before being forwarded to the target customer server.

SecureX has built in commands for specific actions such as deploying patches, and also supports PowerShell scripts providing easy extensibility and flexibility.

SecureX In Action, continued:

NOC Technicians are permitted access to the SecureX Management Console only if they are in the Azaleos Domain NOC Staff Active Directory Security Group.

The SecureX Management Console then uses the individual NOC Technician's SSH key to identify and authorize connections to the Master Control Server. Once online, the technician can select individual or groups of customer servers to perform maintenance and management tasks. The SecureX Master Control Server only allows commands to be sent if the NOC Technician is authorized to administer the specific customer server.

SecureX has built in commands for specific actions such as deploying patches, and also supports PowerShell scripts providing easy extensibility and flexibility. Commands are sent directly over the control channel. For example, if a technician requires a remote PowerShell, the command is sent to the SecureX Master Control Server, and if the user is authorized for administrative access on the target customer server the command is forwarded to the SecureX Agent, which processes the command and sends the results back. A PowerShell session is initiated over the control channel.

The technician can then enter PowerShell commands and scripts that are routed to the customer server through the SecureX Master Control Server. All commands and responses are recorded in the Audit Database. In some cases a NOC Technician requires a remote console to directly access the customer server. In this case, the command is again checked for authorization, and then forwarded to the customer server that will then establish a new encrypted

SSH tunnel for the remote console session.

While connected we record every command executed to our Audit Database, and also have the capability to record the screen during the session. When the technician has completed the management tasks the console and SSH tunnel are closed.

When a NOC Technician uses the SecureX Management Console to resolve a ViewX Monitoring Case, the actions taken through SecureX are appended to the case notes. This captures who performed the maintenance, the problem, the solution, the time it was corrected, and why the problem occurred. This process allows Azaleos to maintain a knowledge base of problems and solutions enabling NOC Technicians to quickly find known solutions.

SecureX Features

SecureXchange Agent

- Agent runs as a Service on every OneServer computer
- Connections encrypted using OpenSSH11 tunneling protocol12 authenticated by 128 bit SSH asymmetric RSA identity keys
 - PKI managed by SecureX system administrators
 - Administrators can revoke SSH keys on Azaleos side for retired servers
 - More secure than a VPN connection - Never bridges networks
- Agent initiates direct outbound connections on port 443 to SecureXchange Master Control Server
- Agent is self updating allowing Azaleos to rapidly fix bugs and introduce new features

Remote PowerShell access for managing Exchange and the host Operating Systems

- Interactive PowerShell sessions created on demand
- Power Shell Scripts and output are logged to Audit Database
- Azaleos PowerShell Scripts take full advantage of Exchange 2007 PowerShell Script API
- PowerShell Maintenance Tasks can be scheduled

Remote Console Access via SSH Tunnels and UltraVNC

- One click access to remote console login - No VPN required
- UltraVNC used for remote console - well managed open source project
- Two Factor Authentication: Requires SSH Key and Administrative Account (Domain or Local) to access the customer server
- Administrative accounts can be in the customer Domain and Local Machine
- Remote console sessions are established through dynamically created SSH tunnels
- SSH Tunnels are always outbound connections initiated from the customer server to the SecureX Master Control Server
- All commands and executed programs are recorded to the SecureX Audit Database
- Capability to record the screen of the console session
- Access controlled by Active Directory Security Policy

Server Patch Management

- Patches can be applied simultaneously to multiple customer servers ensuring work is completed within established maintenance windows
- NOC Technicians provided with consistent, repeatable, and auditable application for deploying and scheduling patches with clear indication of patch success or failure
- Large Patches can be trickle downloaded to stage before maintenance windows, ensuring minimum server downtime

Prescriptive PowerShell Script Library for managing customer servers

- Script Library integrated with Azaleos Knowledge Base, linking issues and solutions
- Scripts can be scheduled to run as maintenance tasks
- Provides NOC technicians with consistent, repeatable, automated, and auditable tools for customer server administration
- Maintenance and Reporting Scripts can be executed on many servers simultaneously

SecureXchange Audit Database

- Records the User ID of Azaleos NOC Technician that initiated the action
- Records every command
- Records the results of every command
- Records the customer server command target



Conclusion

The Azaleos solution combines the “simplicity” of the old corporate e-mail world with the ease of management of the recent outsourcing/hosting wave coupled with great security and control of data by offering to keep the servers and most importantly the actual data on-premise, in the customer’s datacenter! The differences begin at the top with the overall Azaleos approach to the messaging business.

We are not a provider of Hosted Exchange services AND we are not just a standard outsourced services company. Azaleos is the only true provider of remote managed services for Microsoft Exchange --- the Exchange Server stays In-House and on-premise and Azaleos provides a “software plus services” model to help to proactively monitor and manage that end to end messaging system 24 hours a day, 7 days a week, 365 days a year.

Azaleos has discovered a unique and quickly growing niche between the Hosted Exchange providers that target the small business and the large messaging outsourcing companies which target the very large enterprises. The Azaleos hybrid on-premise solution targets the sweet spot between these two models and offers a solution that brings great value to midmarket and enterprise companies and which is totally distinctive --- no other company matches it today.

About Azaleos

Azaleos Corporation provides the benefits of hosted e-mail and collaboration services for organizations that can’t or won’t allow their data to reside outside the datacenter.

Azaleos’ 24X7 remotely managed services for Microsoft Exchange, SharePoint, Active Directory, Office Communications Server, and BlackBerry Enterprise Server keep information on-premise and under IT control, while uptime, maintenance, and support is handled by experts in its network operations centers.

More than 150 companies from Fortune 500 to mid-market enterprises rely on Azaleos and its patented ViewX technology to manage their collaboration infrastructures and address issues before users ever know they exist.

Azaleos is a Microsoft Gold Certified partner, and one of Microsoft’s top 35 partners in the US.

For more information visit www.azaleos.com.