

CytexOne Stratus

Security Details White Paper

This document details the various security features that are implemented by CytexOne, and provides an overview of how the CytexOne Stratus complements and integrates with the BlackBerry® security architecture. Remember, the CytexOne Stratus is, at its heart, a fully-functional BlackBerry Enterprise Server, and thus you enjoy all the benefits of a pure BlackBerry Enterprise Server, but with many added benefits, as detailed below. For details on the security benefits a BlackBerry Enterprise Server brings to your organization, see their white paper: http://www.blackberry.com/products/pdfs/bb_rsa_whitepaper.pdf

This document describes both the CytexOne Stratus with BlackBerry Enterprise Server 4 and the CytexOne Stratus with BlackBerry Enterprise Server 5. These security features and safeguards are also universal to all CytexOne Stratus versions and configurations, unless otherwise stated. See the official Research In Motion (RIM) documentation for detailed BlackBerry Enterprise Server specifications and comparisons between BlackBerry Enterprise Server 4 and BlackBerry Enterprise Server 5.

See the CytexOne Stratus Acronym Glossary for the full terms substituted by the acronyms in this document.

You may notice the similarities between this document and the RIM white paper referenced above. This is intentional, as CytexOne worked directly with RIM to perfect the CytexOne Stratus, and we have their full backing and support as an Elite Tier BlackBerry Alliance Member.

CytexOne Stratus Device Redundancy

The CytexOne Stratus devices were designed with data security at the forefront of our minds. CytexOne employs numerous levels of redundancy in our devices, and these can be scaled up or down in accordance with client requests. CytexOne uses only the highest quality DELL PowerEdge servers to build our CytexOne Stratus devices. These devices come with the following redundant features:

Feature	Description
Dual Redundant Power Supplies	<ul style="list-style-type: none"> All CytexOne Stratus devices have two individually removable hot-swappable power supplies that are each able to fully sustain and power the system in case of critical failure.
Raid with Battery and Global Hot Spare	<ul style="list-style-type: none"> All CytexOne Stratus devices have hardware RAID cards installed with a backup battery and global hot spares. With a hardware-based raid card with battery, you're guaranteeing that, in the event of a dual power supply critical failure or system-wide power loss, your data will not be corrupted. By using RAID, even in the event of hard drive failures*, your data stays secure and accessible, and with a Global Hot Spare, the response time necessary for a hard drive failure is lengthened, further decreasing the risk of data loss.
ECC Mirrored RAM	<ul style="list-style-type: none"> ECC Ram detects single-bit errors in data that would otherwise cause a crash. Ram Mirroring takes this one step further by copying data seamlessly and automatically to a second mirrored DIMM so that, in the event of a multiple-bit error, the data is read off the mirrored DIMM instead of crashing the system. This greatly increases uptime and data security by preventing data loss and/or corruption due to system crashes.
Multiple Hot Swappable Fans	<ul style="list-style-type: none"> While fans are technically not a redundant feature, component overheating is a critical issue for any server. All CytexOne Stratus devices come with multiple hot swappable fans for increased cooling reliability and decreased risk of component failure.
Multiple Redundant NICs	<ul style="list-style-type: none"> All CytexOne Stratus devices have at least two Intel or Broadcom Gigabit NICs that are redundant and bonded network connections. This ensures an uninterruptible network connection and always-on access to your CytexOne Stratus device.

* Even multiple simultaneous hard drive failures are protected, depending on the raid version chosen.

CytexOne Stratus Data Center Security and Redundancy

At CytexOne, we consider data security and data protection one of our highest priorities. This is why our CytexOne Stratus Data Center, like the CytexOne Stratus device, has multiple levels of redundancy and protection.

Feature	Description
Closed Circuit Television recording and 24 / 7 / 365 monitoring	<ul style="list-style-type: none"> Our Data Center is protected by around-the-clock CCTV monitoring and recording, including onsite 24/ 7 /365 security personnel ready to respond to any emergencies.
Identity Verification, Logging, and Escorting of all Visitors	<ul style="list-style-type: none"> No visitors are allowed into the data center without both positive identification and signing in on the log. Even then, a Data Center employee escorts the visitor wherever he/she needs to go and restricts his/her access to only equipment he/she is authorized for.
SAS 70 Type II Certified Physical Data Center Security Controls	<ul style="list-style-type: none"> Our Data Center is SAS70 Type II Certified, more information on which can be found here : http://www.sas70.com/
State of the Art Fire Suppression System	<ul style="list-style-type: none"> CytexOne's data center is protected by a Pre-Action Fire Suppression system consisting of the release of chemical agents that eliminates the fire's ability to burn and spread while protecting electrical devices.
UPS Battery Backup Systems with Redundant Power Feeds from Separate Power Grids	<ul style="list-style-type: none"> Our Data Center's power is protected by multiple UPS Battery Backup Systems that draw power from separate power grids. This ensures that, even in the event of an entire city power grid losing power, our network infrastructure will stay up and responsive.
Generator Backup for entire building with Automatic Transfer Switch	<ul style="list-style-type: none"> Even in the event of multiple power grids losing power, or a city-wide power loss, our data center is equipped with a generator able to power the whole building, and an automatic transfer switch that reroutes power from the generator to the data center and back on the fly.

CytexOne Stratus Device Components

Each component in the CytexOne Stratus device utilizes multiple levels of protection and security to ensure that at no point can an unauthorized user access your data. There are dedicated safeguards in place that prevent intrusion, encrypt data sent over the internet, authenticate users, and authorize systems that connect to the CytexOne Stratus device. Each of these safeguards were individually researched and chosen to create a virtual abyss that separates and protects the CytexOne Stratus device from unauthorized access.

Astaro Features	Description
AES-128-CBC Encryption	<ul style="list-style-type: none"> AES encryption is the encryption standard adopted by the U.S. Government, and is considered sufficient to protect Classified Secret information. 128-bit Block Ciphers are immune to related-key attacks, and are used worldwide in many applications requiring secure encryption
MD5 Authentication	<ul style="list-style-type: none"> MD5 Authentication prevents the user password from being sent over the Internet via clear text. This protects against unauthorized users gaining access via packet sniffing Md5 also provides message integrity and confidentiality protection after initial authentication.
Stateful Inspection Firewall	<ul style="list-style-type: none"> The integrated firewall on the Astaro is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state are allowed; others are rejected.
Intrusion Protection	<ul style="list-style-type: none"> Allows for in-depth filtering to protect against over seven thousand different attack vectors.
<p>For a complete list of all the features that the Astaro Security Gateway offers, please see their data sheet here: http://www.astaro.com/content/download/2903/23691/file/Astaro_Security_Gateway_Overview_us.pdf</p>	

F5 FirePass Features	Description
Group Policy Enforcement	Provides an exclusive mechanism to apply and enforce group policies on the client side, computers not part of the network domain. Policies, in the form of templates, restrict user authority and access on the client while enforcing compliance with PCI, HIPAA, and GLBA.
Integrated Endpoint Security	Delivers a secure virtual workspace, pre-logon endpoint integrity checks, and endpoint trust management.
Safe Split Tunneling	Safe Split Tunneling protects against backdoor attacks when accessing the network with split tunneling, CytexOne provides a dynamic firewall that protects Windows 2000/XP/Vista, Mac, and Linux users when using the full network access feature. This eliminates the ability for any hackers to route through the client to the corporate network or for the user to inadvertently send traffic to the public network.
Client Integrity Checking	Client Integrity Checking increases security by detecting the presence of required processes (e.g. virus scan, personal firewalls, OS patch levels, registry settings, etc.) and the absence of other processes (e.g. key logger) on the client PC before allowing full network access.
Broad Interoperability	Supports existing network infrastructure and identity management systems via Active Directory, Radius, LDAP, PKI, RSA ACE, and more. Delivers web portal integration with support for Java applets, JavaScript rewrite, and more (VPNC certified).
Broad Client Support	FirePass offers broad multi-platform support for secure network access from Windows (2000, XP, Vista), Linux, Mac, Apple iPhone, Windows Mobile, and other smart phones.
For a complete list of all the features that the F5 FirePass offers, feel free to download their overview at : http://www.f5.com/pdf/products/firepass-overview-ds.pdf	

CytexOne Stratus Network Infrastructure

The CytexOne Stratus Network Infrastructure was planned and deployed as a self-contained, separate back end to administrate, maintain, and monitor the CytexOne Stratus devices. Our infrastructure is fully scalable and expandable, multi-homed, battery protected, and designed from the ground up for security, redundancy, and reliability.

Feature	Description
Private IP addresses	<ul style="list-style-type: none"> CytexOne Stratus Network Infrastructure uses private IP ranges to prevent any unauthorized users from directly accessing the device.
Remote User Administration	<ul style="list-style-type: none"> Any remote access can be granted or revoked immediately and propagates instantaneously across the entire network. This ensures that unauthorized users have access when they need it, and it can be removed immediately in the case of leaked or stolen passwords. Identity Management systems supported includes Active Directory, LDAP, PKI, RSA ACE, and many others.
Redundant 24 / 7 / 365 Network and Systems Monitoring	<ul style="list-style-type: none"> The entire CytexOne Stratus Network Infrastructure is redundantly analyzed twenty-four hours a day, seven days a week, by two separate monitoring systems. Each monitoring system has the ability to analyze warnings, alerts and failures down to the component level. CPUs, Memory, Hard drives, and controller cards are just some of the components that are individually monitored. Each monitoring system is configured for critical failure email alerts, daily and weekly reporting and each is also independently monitored by technicians through a secure remote web site.
VMware Virtualization	<ul style="list-style-type: none"> CytexOne's Stratus Network Infrastructure consists of a High-Availability VMware Cluster with DRS.

Feature (continued)	Description (continued)
Redundant 48-port Gigabit Switches with Dual Redundant Hot Swappable Power Supplies	<ul style="list-style-type: none"> • Our network infrastructure employs sets of 48-port gigabit switches that automatically fail over in case of critical failure or loss of power. • Each switch is protected by dual redundant power supplies that are individually hot swappable in case of power supply failure.
Multiple SANS with Raid 50, Global Hot Spare, Dual Redundant Hot Swappable Power Supplies and Dual Redundant Hot Swappable RAID Controllers with Battery	<ul style="list-style-type: none"> • Each SAN is protected by Dual Redundant Hot Swappable Power Supplies that are each able to fully sustain and power the system in case of critical failure. • Each RAID Controller is individually hot swappable so that, in the event of a critical raid controller failure, no data is lost and no downtime takes place. • Each RAID controller has a battery, so that in the event of a critical power supply failure or power loss, no data is corrupted or lost. • Raid 50 with Global Hot Spare ensures that, even in the event of multiple hard drive failures*, no data is corrupted or lost, and system remains online. The global hot spare ensures that, in the event of hard drive failures, the response time necessary for replacing the drive is lengthened, ensuring that data is still protected and secure.
<p>* Raid 50 allows for as many simultaneous hard drive failures as there are nested RAID 5 arrays, so long as the hard drives in question are spread equally among said nested RAID 5 arrays.</p>	

CytexOne Stratus Policies and Procedures

The CytexOne Stratus device is installed alongside your business infrastructure, and is joined directly to your domain. Because of this, certain safeguards were developed and implemented to ensure that your data is secure, even from CytexOne.

Feature	Description
No Domain Admin Access Necessary	<ul style="list-style-type: none"> • CytexOne developed the CytexOne Stratus device explicitly without the requirement of the domain administrator password. • All maintenance, troubleshooting, and support requests are done without knowledge of your domain admin password, so that your IT team can continue their domain maintenance without adversely affecting the CytexOne Stratus side.
Group Policy Administration	<ul style="list-style-type: none"> • Group Policy administration is handled as normal by your IT Team, however, CytexOne has the ability to restrict and/or change policies if such policies would adversely affect the CytexOne Stratus device.
Internal Security Policies	<ul style="list-style-type: none"> • CytexOne staff is restricted from viewing or saving any user data without authorization. • All violations are logged, and violators are strictly disciplined. • Gross or repeat violations of this policy results in immediate dismissal.
Support Queue Policies	<ul style="list-style-type: none"> • All support requests are tracked, monitored and audited throughout the entire support process. • All requests not fitting a standard "Support" scope are authorized by the account holder before work is performed. • Clients can set up restricted access to their own devices, allowing only selected employees access while enforcing compliance with PCI / HIPAA / GLBA and others.
0-day Intrusion Detection System	<ul style="list-style-type: none"> • Our intrusion detection system prevents unauthorized traffic from attempting to reach the CytexOne network.
Redundant Security Auditing Software	<ul style="list-style-type: none"> • Multiple auditing systems actively scan CytexOne's Internal Infrastructure and the CytexOne Stratus network infrastructure for any missing patches and updates, security holes and alerts, and / or exploits.

A Visual Representation of The CytexOne Stratus device

Figure 1 is the Research In Motion diagram detailing the End-to-End Encryption capabilities of the BlackBerry Enterprise Solution. Similarly, Figure 2 shows the CytexOne Stratus device End-to-End Encryption capabilities.

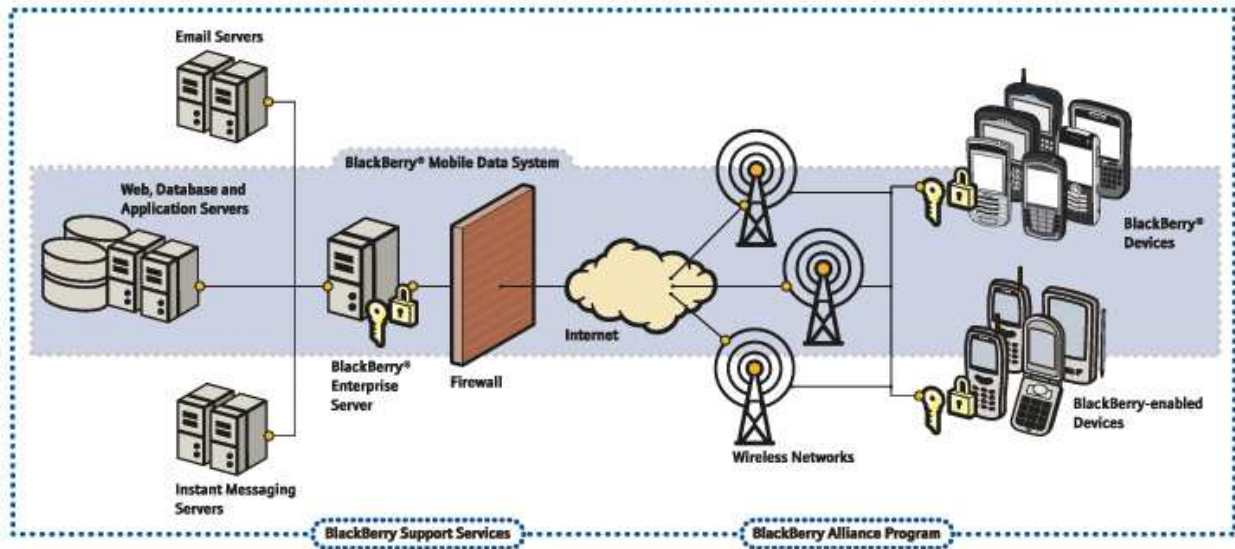


Figure 1. BlackBerry End-to-End Encryption Diagram

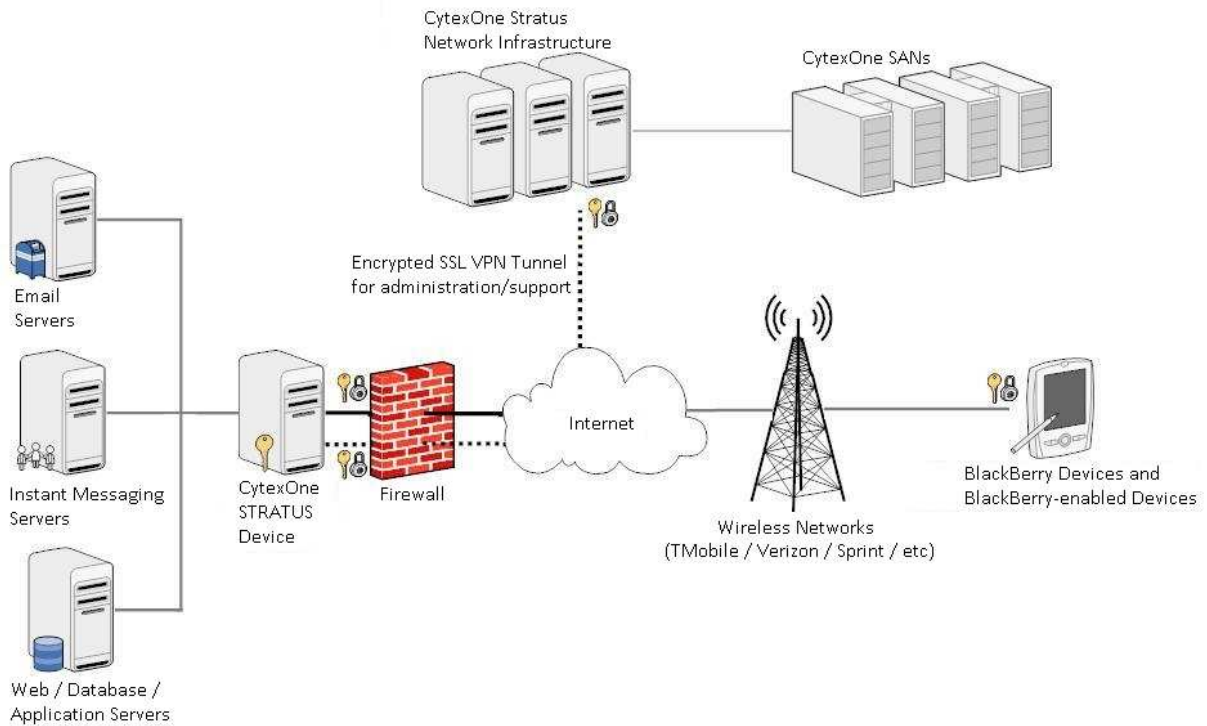


Figure 2. CytexOne Stratus End-to-End Encryption Diagram
(includes Encrypted VPN Administration / Support tunnel)