



# Security of MicroConvergent Portal and Appliance in a Converged Telephone System Environment

# Table of Contents

- Executive Summary .....3
- Open Toolbox (OTB) Appliance Features .....4
  - Levels of Data Gathering .....4
  - OTB Security.....4
- MicroConvergent Portal Features .....5
- MicroConvergent Portal Security .....5
  - Administrative Practices .....5
- Conclusion .....5

## Executive Summary

This summary and the discussion that follows puts MicroConvergent security into perspective by clarifying deployment options and the mechanisms by which MicroConvergent functionality is delivered in a telephone system environment.

The MicroConvergent Open-Toolbox Appliance (OTB) acts as the data gathering and processing device that supplies data to the MicroConvergent portal which enables remote management of converged communications environments. The combination of the OTB and the portal allows us to deliver a full range of functionality.

The appliance, the portal, and the transport between the two are designed with security in mind. Logs record that accesses the portal, and all Granted Access activities. At no time does the MicroConvergent OTB appliance capture the “payload” content of IP data streams, and thus no confidential information ever reaches the portal. Rather, MicroConvergent’s analysis and reporting is based on metrics derived from IP envelopes and the technical content of system-level log files. These metrics are purged at pre-defined periods while the administrative logs are retained and archived.

In a converged telephony environment, an IP server and TDM Cards or a TDM KSU with IP Gateway, MicroConvergent provides the following capabilities:

- QoS Monitoring
  - Summary – of Quality of Service
  - Time of Day – QoS by Time Hour of the Day
  - Passive Summary by Time of Day – Summarized Quality by Time of Day
  - Passive Detail record by Source – Call Details by Source Phone
  - Degradation by Time of Day – Degradation Drivers for Poor QoS
  - Top Applications – Bandwidth Usage by all Applications
  - Top Talkers – Top Bandwidth Usage by source IP Address
  - Ping Statistics – Network Devices Ping Results
  - Syslog Statistics - Network Devices Syslog’s
- Infrastructure Device Monitoring
- VoI P/LAN Troubleshooting – Drill down to see call set-up, connectivity and performance of very IP Phone. Having complete visibility of the LAN/WAN can also determine if a competing application is causing the problem.
- On/Off conditions on all ports
- All diagnostic information available on the system’s COM Port.

# OTB Appliance Features

## Levels of Data Gathering

- **Device Monitoring:** ICMP Ping, Syslog, SNMP Trap, SNMP Get
- **QoS Monitoring:** Active Call Generation (All major Codecs), Passive Data Gathering (SNMP), Passive Stream Analysis
- **Application Traffic:** Passive Data Gathering (SNMP), Layer 2 through 3 Packet Capture via SPAN port or network TAP

## OTB Appliance Security

**Appliance Operating System:** Hardened XPe operating system, stripped down to the kernel plus basic shell, as is the best practice for embedded networking applications. The OS does not require service packs and does not support remote scripting; COM and other layers that best practice dictates could undermine security.

**Appliance Agent Software:** MicroConvergent's standards-based Java code runs within a simplified Sun Java VM sandbox with best-practice security settings.

**Data:** Data processed by the appliance is limited to performance metrics. Outputs for real-time display via the MicroConvergent portal and for reporting are encrypted and compressed as XML transported via SSL. Hacking the output would require cracking SSL, cracking our internal encryption, cracking our obfuscation, decompressing the data and the result would be only XML data representing metrics such as Delay, Jitter and Loss, etc.

**Communications:** By default the Appliance software *communicates outbound over SSL to a single predefined secure address*, the MicroConvergent portal, where the information can be viewed and reported.

**Packet Capture:** The Appliance can utilize one of its three network interfaces for packet capture to generate rich metrics on application bandwidth usage as well as passive call -by-call QoS statistics. Packets can be sent to the appliance through a SPAN port or network TAP, exactly as you would to perform protocol analysis using tools like Ethereal/Wireshark. *At no time is anything above Layer3 analyzed; our proprietary technology needs only header information in Layer 2 and 3 and no business information is stored, parsed or reviewed in any way.* Please note that SPAN port or network TAP deployment is required only to enable these optional packet-capture-based features.

## MicroConvergent Portal Features

The MicroConvergent Portal is the mechanism by which we remotely manage a converged communication system.

The Appliance securely transmits all of the calculated metrics; log files and other performance monitoring data to the MicroConvergent portal for real-time viewing and reporting. Secure access from the Portal allows MicroConvergent T to perform protocol analysis on packets captured by the Appliance. Once again, *nothing above Layer 3 is analyzed; MicroConvergent's advanced technology needs only header information in Layer 2 and 3 to ascertain the health and performance of converged communications and no business information is transmitted to the MicroConvergent Portal.*

## MicroConvergent Portal Security

As described in the opening section of this paper, security is maximized for the level of functionality chosen through such mechanisms as outbound connection only from the Appliance to the MicroConvergent portal, several levels of encryption, and full audit trails for remediation efforts using the Appliance's Granted Access capability.

Functionality hosted in the portal assists MicroConvergent in isolating and analyzing the performance data provided by the Appliance.

### Administrative Practices

Per normal best practices, no administrator of the MicroConvergent portal can view IDs and passwords. Email address is used as a unique User ID, and password resets are handled via email to the user in question.

The MicroConvergent system records all logins, reporting activity, configuration and administrative changes. Those logs require privileged access. They are maintained for 90 days onsite and archived offsite.

Comprehensive security systems and procedures are in place for privileged access to all critical portions of the MicroConvergent portal. Controls include segregated access via multi-factor encrypted authentication.

## Conclusion

The MicroConvergent solution comprising Appliances that link back to the MicroConvergent portal to enable management of client's converged communications environments is extremely secure. In all cases the Appliance, portal and surrounding administrative procedures were developed with security and simplicity in mind.