Secure Data Monitoring and Analytics Are Key to Maximixing the Value of Unified Communications

Produced by 

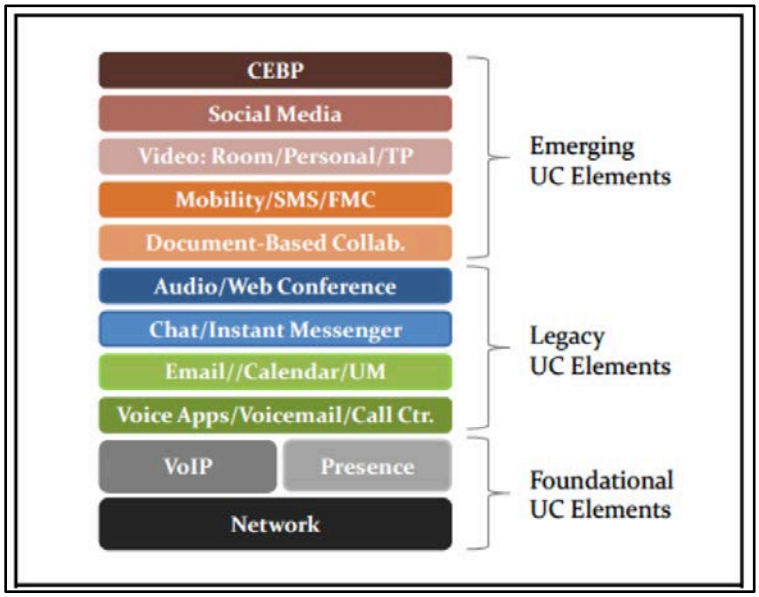
Sponsored by 

By Zeus Kerravala, Founder & Principal Analyst, ZK Research

Section I: It's Time to Take UC Management and Analytics Seriously

Unified Communications (UC) has been a market in the making for over a decade. UC has been a continually evolving market that was initially centered on voice over IP (VoIP) and unified messaging, but has expanded significantly over the past several years. While VoIP remains a foundational element of UC, the breadth of UC services has expanded to include other collaborative applications such as video, mobility and data sharing (**Exhibit 1**).

Exhibit 1: The Growing UC Taxonomy



If implemented correctly, UC is a powerful technology with a multifaceted value proposition. In addition to lowering the cost of communications, UC and related analytical information can improve productivity by streamlining processes, enabling new processes that let enterprises add communications capability to traditional business applications, and exploit new revenue sources. UC can help any organization make better, more accurate decisions faster, no matter where an individual is located or what their preferred collaboration tool is.

UC converges all forms of enterprise-based collaboration to a common IP network and touches all mission critical areas of the business. However, historically communications has been managed in its own silo, separate and apart from the rest of the organization. UC, by its very definition, dictates that it should be treated with the same level of mission criticality and security as the rest of the IT domain.

For a UC deployment to succeed, IT organizations must make secure data monitoring and analytics a core part of the deployment. For this to happen though, enterprises must shift their UC infrastructure monitoring strategies away from the current platforms that were designed for legacy voice. This can lead to many security vulnerabilities and possible data leakage that could significantly impair the value the business is hoping to achieve by deploying UC. Addressing and overcoming these vulnerabilities is a critical feature for any UC management strategy.

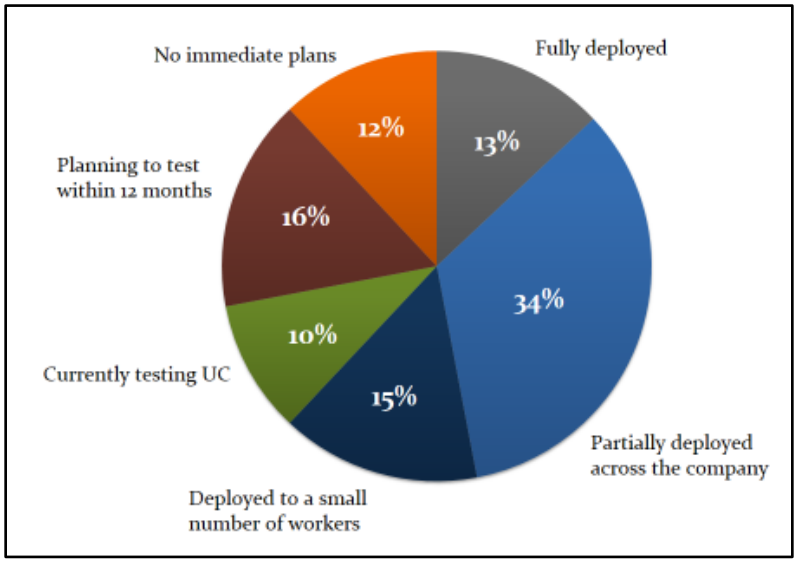
Section II: The Need for UC Data Monitoring and Analytics

Enterprises are well on their way migrating to UC. Exhibit 2 shows that 88% of businesses today have UC deployed or on their roadmap, making it a "must have" for organizations that want to enable a more collaborative workforce.

Exhibit 2: UC is Widely Deployed Today

Source: ZK Research, 2013

What is the status of UC within your organization?



Most organizations today are moving UC out of test and development and into production environments. However, many companies use the same telecommunications group and the same vendor that provided the voice infrastructure to make the shift to UC. This may be sufficient for a few enterprises, but the majority of businesses find that the UC environment is significantly more complex than legacy environments, requiring new skills and tools.

Legacy voice systems were dedicated, fully integrated appliances that were highly reliable but offered little in the way of innovation or flexibility. The closed nature of these platforms held communications back from becoming a strategic business asset capable of creating competitive differentiation. Today's solutions are no longer closed, vertically integrated solutions, but the added flexibility and openness does come with a price.

UC solutions are composed of physical servers, virtual appliances, cloud-based resources, software applications, dedicated endpoints, wireless devices and a number of other components, all running over a common IP network. Each of these components that make up a UC deployment has its own configuration interface, log file and other data associated with its performance.

Maximizing the return on investment for the UC deployment requires understanding how each component works with one another and then optimizing the solution. However, this cannot be achieved with legacy management tools, as the whole environment needs to be securely monitored, analyzed, and adjusted as the UC deployment is rolled out and maintained. Because of the open, multi-component nature of UC, there is a tremendous amount of new metadata available that needs to be collected, correlated and analyzed to allow the infrastructure to operate at peak performance to provide maximum value.

Accomplishing this task of holistic correlation and analysis isn't easy, and requires a shift in thinking about the way UC is managed and secured. The data available is no longer just SNMP traps and alarm codes. To achieve a holistic view of the end to end UC environment, IT leaders must consider the following:

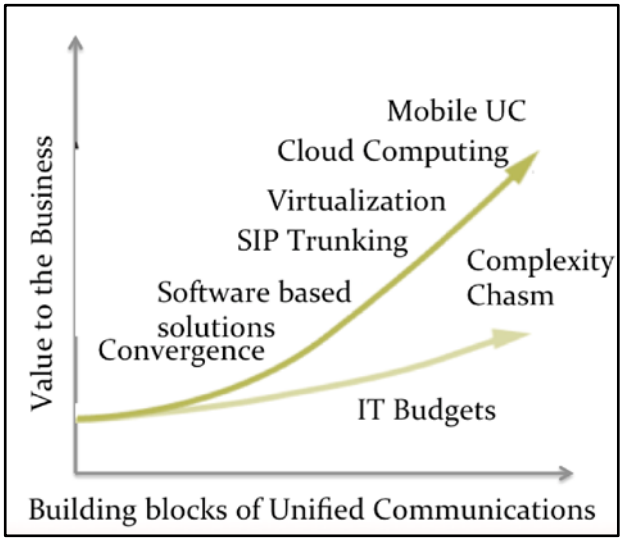
- Data must be collected from every component that makes up the UC solution. This includes network devices, applications, servers and other network-connected resources.
- The data collected needs to be aggregated from premise-based technology, cloud based resources, and multi-vendor environments, so as to not leave blind spots in the analytic engine.

- The data collected must include traditional SNMP traps, but also include log files, flow information, or any other text based information.
- The data includes a large amount of end user information and needs to be treated as sensitive, to protect workers and the company.
- All of the data needs to be correlated and analyzed to detect anomalies, trends, faults, or violations that can indicate a degradation in performance or a security breach.
- All of the metadata needs to be replicated to multiple platforms to protect against the loss of data or to enable monitoring capabilities.
- At least three years' worth of data needs to be stored for regulatory purposes and trending information to optimize performance.

Organizations that choose to implement a comprehensive performance monitoring solution will find their UC solution to be more manageable and secure and capable of providing maximum ROI to the organization. Additionally, the following benefits will be achieved:

- **UC management becomes predictive**. UC deployments are very complex, and managing this environment has become increasingly more complicated. As UC gets more advanced, the complexity chasm between managing the environment and capabilities becomes wider (**Exhibit 3**). Comprehensive data collection and analytics will enable IT to have an established baseline of performance and be able to predict when performance problems will occur. This will enable a higher level of proactivity with respect to the ongoing operations of UC.

Exhibit 3: The Increasing UC Complexity Chasm



- **Maximum security posture**. Historically, organizations had to choose between performance and security and settle for "good enough" in one of these two areas. When it comes to corporate collaboration and the need to be able to make fast decisions accurately, "good enough" is no longer good enough. Secure data analytics will enable the highest level of security without having to compromise on performance.
- **Ability to meet regulatory requirements**. Achieving compliance with regulatory requirements such as SOX, PCI and HITECH/HIPAA can be difficult if not nearly impossible with silo-ed management tools. A holistic management strategy with advanced analytics is the only scalable, cost effective way of meeting regulatory challenges.

Section III: Next Steps to Implementing Secure Data Monitoring and Analytics for Unified Communications

The need for a holistic data monitoring and analytic solution for UC environments has never been higher. UC is a powerful, transformative technology that can save organizations money and raise productivity to new heights. However, how to implement a solution may not be obvious. To help IT leaders get started, ZK Research proposes the following steps:

1. Determine whether the organization has the technical capabilities to deploy and manage the solution internally, or whether a managed service provider (MSP) should be used
2. Choose a solution (in house or MSP) that uses a distributed architecture to collect, store, correlate and analyze the data. The distributed approach will offer maximum flexibility as the UC environment changes.
3. Look for a solution that encrypts the transport of the data to secure the information.
4. Ensure that the data storage is encrypted as well. If an MSP is being used, don't just assume storage encryption, rather insist on it and ask for proof of compliance.
5. **If an MSP is being used, then all metadata, such as log files, traps and flow information, should remain on the company premise. The data needs to stay behind the company firewalls and have maximum protection. Find an MSP that can meet the tough security requirements but also deliver full data monitoring and analytic capabilities.**
6. Choose a solution built on a secure operating system to protect against security exploits and other vulnerabilities.

7. Automate, secure and encrypt the creation and delivery of reports. Also, all archiving of reports should be encrypted for ongoing protection of customer, user and company data.
8. Use VPN connections with multiple encryption methodologies for connecting to the MSP. The ideal connection would be a nailed-up private network connection; this provides the highest level of security that is easiest to manage. This will also enable full audit of all transmissions to ensure data leakage monitoring, while providing the business with complete control of the infrastructure.
9. Choose a solution that is vendor agnostic. Whether deploying the solution in house or through an MSP, a vendor neutral solution is a must. Cross-correlating data from diverse platforms that exist in multiple layers of the OSI stack is critical to the accuracy of information. This will also help the IT staff consolidate the number of tools or views it needs to manage, and improves user satisfaction with faster resolution times.
10. Reporting must be simple and flexible with pre-defined templates for the major UC areas, but allow for customization without having to engage professional services.

Organizations that follow the above steps and choose a solution that meets these requirements will realize the value of secure data monitoring and analytics without the complexity of having to stitch together multiple technologies and solutions. This will help maximize the value of UC and minimize any perceived risks of deployments.

Section IV: Conclusion

Competitive advantage today is no longer based on a single core competency. Rather, the ability to leap ahead of competitors is based on being able to make the best decision with the right people and then act on it faster than any other business. This changing business dynamic has made UC a must-have technology for businesses today. However, as organizations begin to deploy UC across the entire company, IT leaders need to ensure the solution is performing optimally but also securely. Any performance or security issues can rapidly wipe away the ROI the business was hoping to achieve with the initial investment.

A secure data monitoring and analytic solution can help businesses deploy UC and then lets them continually optimize the solution as the environment changes. CIOs and other IT leaders must make data monitoring and analytics a core part of the UC deployment, as legacy management methodologies and tools have far too many blind spots to be practical in today's continually changing world.

About Layer X

LayerX Technologies is a leading provider of advanced data analytics software for the IT industry. LayerX solutions are used across multiple IT domains to provide rich insight into application performance and the underlying network layers.