Yealink

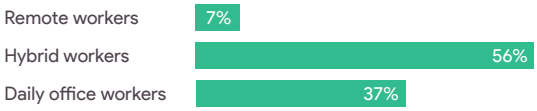
Safeguarding enterprise communications

A focus on best practices in data security and privacy across the data journey

Table of contents

Overview

Enterprise communication systems have long been central to progress and innovation, and with changes in recent years to the way we work, they are even more important than ever. Since 2020, office attendance has partially rebounded but remains 30% below pre-pandemic levels, according to McKinsey & Co. Currently, more than half (56%) of workers have hybrid work arrangements, while only 37% work in an office daily.



In this new, decentralized landscape, maintaining productivity can be challenging.

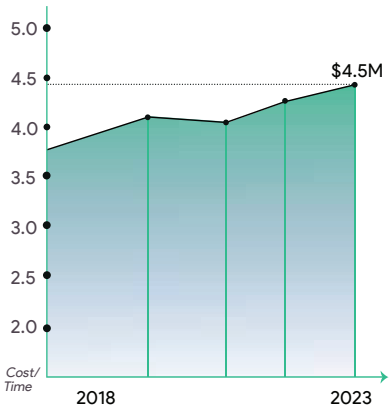
Enterprise communications systems fill an increasingly important role in facilitating efficient knowledge sharing, streamlining operations and fostering robust collaboration.

However, the more reliant we become on sharing information over distances and digital channels, the more the issue of data security comes into sharp relief.

Communication device security is an important part of the enterprise threat management landscape. Protecting sensitive information and conversations, maintaining data privacy, securing against data leaks, and safeguarding intellectual property (IP) are essential for enterprises to function securely and efficiently.

This whitepaper will demonstrate the importance of data security standards in enterprise communications technology, the necessity of protecting data across the communications lifecycle, and the effectiveness of validating data security in Yealink Management Cloud Service (YMCS) and Microsoft enterprise communications.

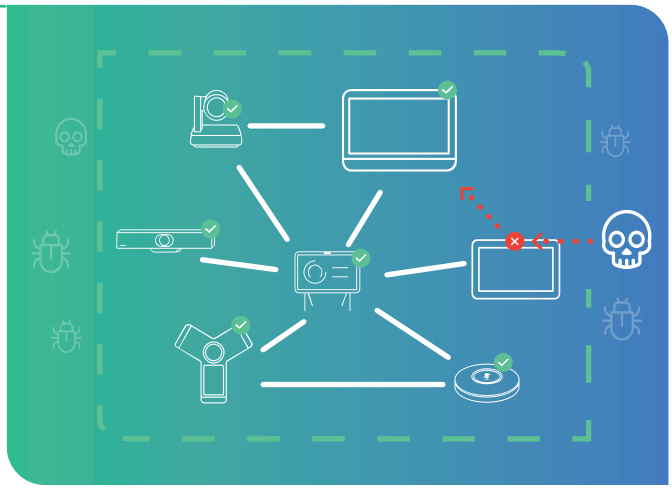
Cost of a data breach



The average cost of a data breach in 2023 was **$4.45M**, marking a **15%** increase over the past three years, according to

IBM Security's Cost of a Data Breach Report 2023.

Key factors in managing information security in enterprise communications



Device management

Unmanaged communication technology assets pose significant risks to data security, as highlighted by the World Economic Forum's (WEF) Global Cybersecurity Outlook 2023: "Many organisations have too many assets on their network to identify the key risk points, or even to map their assets".

Security standards

Compliance with global information security standards, such as ISO/IEC 27001 and SOC2, ensures that data privacy and security are maintained within enterprise communications. These standards involve continuous monitoring and improvement, demonstrating an organisation's commitment to safeguarding sensitive information and building trust with clients and stakeholders.

Trusted partnerships

Equally important is the close cooperation between OEMs, software providers, and cloud vendors. This collaboration is essential for protecting data throughout its lifecycle, both in transit and at rest. Each party must ensure robust security in their respective domains - hardware, software, and cloud infrastructure. This coordinated approach fortifies every link in the data chain, reducing vulnerabilities and enhancing overall data security.

Let's now examine how an enterprise can successfully navigate the complex information security landscape in their enterprise communications.

Data security standards in enterprise communications technology

The evolving threat landscape

Given the current proliferation of cyber threats, organisations cannot afford any weak links in their data security. Every aspect, from hardware to software to transport to cloud, must be considered, tested, and secured.

> Protecting an organisation against intrusion remains a cat and mouse game, in which the cyber criminals have the advantage.
>
> Allianz Commercial Cyber Security Trends 2023

Cybercriminals need only to identify a single vulnerability to exploit, whereas defenders are tasked with securing all potential entry points simultaneously against multiple threats. This facilitates more opportunity for attackers, enabling them to identify and exploit weak points more swiftly than organisations can fortify their defences.

Many enterprises have more entry points than they realise due to the growing number of smart, internet-enabled devices, including enterprise communication systems. Devices, such as VoIP phones, video conferencing equipment, and IoT devices, can all serve as potential entry points for cyber attackers. It can be a stark challenge for organisations to be confident in their overall security posture.

> You might be 99% cyber safe, but if there is one open door, it's likely that attackers will find it.
>
> **Michael Daum,**
> **Global Head of Cyber Claims, Allianz Commercial**

Trusted security standards

Recognised frameworks, such as ISO/IEC 27001 and SOC2, represent the gold standard in data security and privacy protection. Adherence to these standards provides enterprises with confidence in their security measures, as they are based on extensive research and established methodologies that surpass what a single organisation could develop independently.

By implementing these standards, enterprises ensure they meet a baseline of security best practices while also laying the foundation for further customisation and enhancements tailored to their specific environment. Understanding and applying these standards can significantly bolster an organisation's security posture and help mitigate potential risks. Beyond testing at a single point in time, these standards enable organisations to become risk-aware and proactively identify and address weaknesses. The reports generated from these standards can assist organisations in developing strategies for identifying, managing, and remediating security risks well into the future.

Example:

SOC2 - Beyond one-time compliance

SOC 2, developed by the AICPA (American Institute of CPAs), defines criteria for managing user organisations' data based on the Trust Service Criteria. These criteria cover essential aspects of data security, including security, availability, processing integrity, confidentiality, and privacy-related controls.

A SOC 2 report provides service organisations with the assurance that their data privacy and security measures are robust during processing or storage. It guarantees that specific controls related to confidentiality and privacy of information are in place, and data accessibility is maintained at all times. This comprehensive approach offers a robust framework for managing and protecting sensitive data, giving organisations confidence in their IT security capabilities.

Importantly, SOC2 compliance is not a "set and forget" solution.

For example, SOC2 Type 2 compliance requires continuous reporting over time rather than a single point in time. This on going process includes regular, independent penetration testing to stay vigilant against new threats, ensuring that the organisation's security measures are consistently updated and effective against evolving cyber threats.

Protecting data across the communications lifecycle

Given the complexity of cybersecurity threats, organisations must adopt a holistic approach to data protection. Effective data security demands that all components - from hardware to cloud services - work seamlessly together to protect information throughout its lifecycle. To demonstrate how organisations can succeed in constructing a secure enterprise communications environment, this whitepaper will explore the effectiveness of integrating robust security measures across different platforms in collaboration, using the comprehensive approach to data protection between Yealink and Microsoft.

Multi-layered data protection with Yealink and Microsoft Azure

Yealink's communication and collaboration solutions are secure by design. They protect user data privacy and integrity and use international standards, such as SOC2, to test and validate this posture.

Combining Yealink's capabilities with those of Microsoft Azure further enhances security and privacy. Yealink's secure device management is complemented by Azure's advanced security features including role-based access control (RBAC), encryption at rest, and data isolation, ensuring compliance with international standards. This synergy provides a multi-layered approach to data protection, securing data in transit and at rest, and offering enterprises enhanced visibility and control over their communication devices, all while adhering to international security standards such as SOC2 Type 2 and ISO/IEC 27001.

The role of cloud in enhancing enterprise security

Cloud emerges as a key component in this enhanced security framework. According to the WEF Global Cybersecurity Outlook 2023, most cyber leaders agree that increased use of cloud-based services and digital transformation initiatives will have the most positive influence on an organisation's approach to cybersecurity in the next 12 months.

For any enterprise, using a cloud-linked platform for device management bolsters security in several ways:

1. Centralised oversight:

It allows for real-time monitoring, updates, and troubleshooting of all devices from one central location.

2. Reduced risk:

This centralised control helps reduce the risk of unmanaged and vulnerable assets.

3. Consistent security:

The platform ensures that security policies and updates are applied consistently across all devices.

4. Enhanced protection:

It uses cloud-based measures like encryption and secure data transmission to protect data.

5. Improved security posture:

Overall, this approach strengthens the organisation's security, mitigates risks more effectively, and ensures compliance with regulatory standards.

> In cybersecurity, attackers have a structural advantage: they need to find only one exploitable weakness across an organisation. This means attackers have less ground to cover than a defender and the attacker can often adapt faster than organisations can defend or recover.
>
> WEF Cybersecurity Report 2023

There is now a significant burden on organisations beyond implementation of robust security protocols, to also continuously monitor, update, and adapt their defences to keep pace with the dynamic nature of cyber threats.

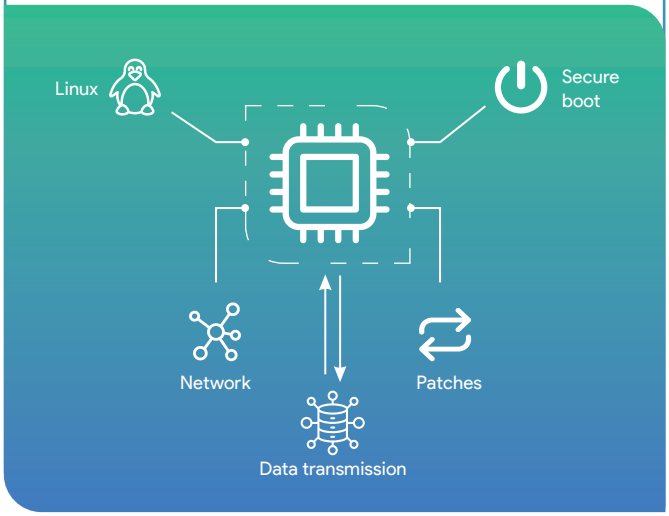
Recognising these challenges, Yealink and Microsoft have collaboratively considered all layers-hardware, software, transport, and cloud-ensuring comprehensive coverage of the complete data lifecycle.

Visibility and manageability: The cornerstones of hardware security

Yealink's hardware security is enhanced by visibility and manageability of assets through its Management Cloud Service (YMCS) tools. These tools enable enterprises to centrally manage assets, including Bluetooth devices, allowing for remote upgrades, monitoring, and troubleshooting. This comprehensive asset management is crucial, as unmanaged assets can become security vulnerabilities.

To ensure hardware security:

- Devices are configured with security-enhanced Linux.
- Secure boot processes are implemented.
- Quarterly security patches are applied to maintain up-to-date protection.
- Data transmission is secured using TLS 1.3 and AES256 encryption.
- Network access is controlled through 802.1x authentication.



Advanced software security protocols

Yealink's devices, certified for Microsoft Teams, have met the stringent security criteria established by Microsoft. This certification indicates that Yealink's devices have undergone rigorous testing and validation to ensure compliance with Microsoft's high standards for data privacy and security. By achieving this certification, Yealink's devices are endorsed by Microsoft as meeting robust security requirements, thus ensuring that they are deemed secure for enterprise use.

As part of its collaboration with Microsoft, Yealink integrates its devices into the Microsoft Device Ecosystem Platform (MDEP), enhancing security measures across its product line. MDEP, based on the Android Open Source Project (AOSP) and backed by Microsoft's Security Architecture, is designed to improve the security, reliability, and manageability of devices, ensuring they meet Microsoft's high standards for data protection and performance.

Adopting MDEP highlights Yealink's commitment to security in partnership with Microsoft, showcasing their ongoing efforts to ensure customer data remains secure.

YMCS maintains data privacy and security by requiring express user permission to connect to the platform and manage or send data. Customers retain control over their own data, with telemetry data used solely for equipment operation and maintenance, containing no personal or sensitive information.

"Penetration security testing is regularly executed by leading independent labs to meet the toughest security standards," explained **Dawson Cai, head of product for modern workspaces at Yealink**."Before any of our products are released, security testing is the most crucial step."

Ensuring data integrity in transit

Data transmission poses significant risks, as information can be intercepted or tampered with during transfer between devices and the cloud. Protecting data during transmission is critical to maintaining the integrity and confidentiality of sensitive information. To address these risks, several robust measures are implemented:

HTTPS authentication and TLS 1.2+ protocols:

Data from YMCS is secured during transmission using HTTPS authentication and TLS 1.2+ transport protocols. These protocols encrypt data, ensuring it remains secure against interception and tampering.

Microsoft Azure security enhancements:

Microsoft Azure further bolsters this security by securing connections with an Open VPN or Azure ExpressRoute. This setup creates an isolated and highly secure environment for YMCS operations.

Protection from malicious attacks:

The combination of these protocols and security measures ensures that all data transmitted between devices and the cloud is protected from malicious attacks and data tampering.

By employing these comprehensive security measures, organisations can ensure the integrity and confidentiality of their data during transmission.

Protecting customer cloud data

Microsoft Azure supports and enhances data security in YMCS through its well documented and highly robust security posture. The following measures ensure comprehensive data protection:

Data storage:

Data is stored in data centres located in Virginia, USA, and Paris, France, adhering to local legal and regulatory requirements.

Role-based access control (RBAC):

Azure employs RBAC to manage who has access to data and resources, ensuring that only authorised personnel can access sensitive information.

Encryption at rest:

Data is encrypted while stored to protect it from unauthorised access.

Data isolation:

Idividual customer data is isolated to prevent cross contamination and ensure privacy.

Access and audit protocols:

Stringent access and audit protocols are in place to monitor and control data access, ensuring transparency and security.

By implementing these measures, Microsoft Azure provides a secure environment for YMCS, ensuring that customer data is protected at all times.

Validating data security in YMCS and Microsoft enterprise communications

Third-party validation and certification are crucial to ensure compliance with the latest international standards and to maintain a vigilant security stance. YMCS and Microsoft Teams (as part of MS365) adhere to SOC2 Type 2 and ISO/IEC 27001 standards.

ISO/IEC 27001 is renowned as the world's best-known standard for information security management systems, promoting a holistic approach to information security by vetting people, policies, and technology. An information security management system implemented according to this standard serves as a tool for risk management, cyber-resilience, and operational excellence.

YMCS undergoes rigorous independent penetration testing to ensure its security posture remains robust. This includes:

- **Static and Dynamic Vulnerability Scans:** To identify potential weaknesses in the system.
- **Penetration Tests:** Conducted by both internal teams and independent external testing organisations to simulate attacks and evaluate the effectiveness of security measures.
- Regular Testing: Performed on the production site and internal corporate networks to continuously identify and addresspotential vulnerabilities.

Summary

By following these best practices, organisations can measure their security measures against the high standards set by Yealink and Microsoft. Managing assets effectively, considering security across the data journey, and ensuring regular third-party testing and adhering to internationally recognized standards like ISO/IEC 27001 and SOC2 Type 2 can help maintain high standards of security and resilience.

Organisations should consider integrating best practice security measures:

- **Adopt international standards:** Implement ISO/IEC 27001 and SOC2 Type 2 standards to ensure comprehensive information security management.
- **Engage in regular testing:** Conduct static and dynamic vulnerability scans, as well as penetration tests, regularly.
- **Utilise third-party validation:** Ensure independent external organisations validate your security measures.
- **Maintain continuous improvement:** Regularly update and improve security measures based on testing results and evolving threats.

Effective management of enterprise security communications is essential for maintaining a robust security posture Implementing a sophisticated and secure device management platform is a strategic decision that provides the necessary intelligence and control.

The integration of Yealink hardware and YMCS with Microsoft Teams and Microsoft Azure exemplifies a comprehensive and resilient security framework. This approach adheres to best practices for data security and privacy, as validated by rigorous international standards such as SOC2 and ISO/IEC 27001. By emulating this model, organisations can confidently manage their smart enterprise communication systems, ensuring thorough protection and secure operations.

October 2024

Yealink