SaltDNA

NEWCOM

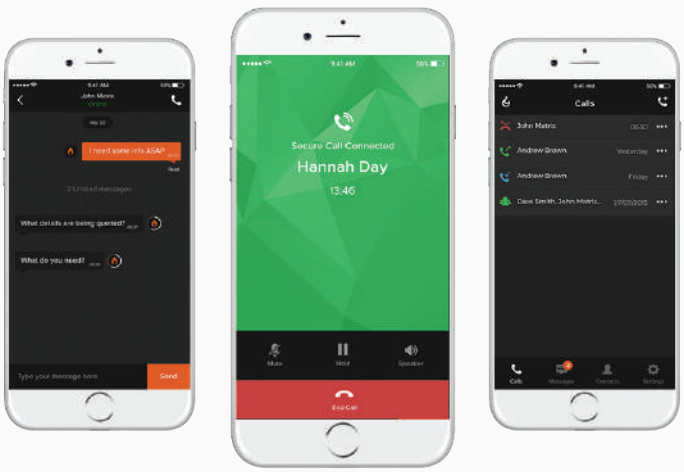
Protect sensitive and valuable information with secure communications – and tight control for the enterprise

In the 21st century, enterprise voice and text communications are loaded with competitive secrets, intellectual property, and sensitive or strategic information. When access to that information is breached, the consequences can be dire.

SaltDNA Enterprise is the best weapon enterprises have to protect trade secrets and other sensitive, strategic and proprietary information. Eliminating your enterprise's mobile communications risks has never been easier, faster or more effective. SaltDNA's rock-solid encryption framework together with its focus on mobile usability, deployment flexibility, and comprehensive control functions make it effortless to strengthen and reinforce your company's security posture.

Mobile communications have greatly increased the risk of information leaks.

The impact of mobile technology on businesses has been profound. The rapid increase in mobility has a dark side; mobile device-related breaches are growing as well. The PwC 2015 Information Security Breaches Study on UK corporations found a 100% increase in mobile device breaches. These statistics highlight the growth of device breaches, and the importance of protecting mobile communications in the enterprise.



The SaltDNA Enterprise Encryption Framework: A Proprietary Architecture using Open Source Encryption

Encryption standards are always evolving. That is why SaltDNA has a unique multi-tier architecture designed to always use the most up-to-date encryption. Unlike some solutions, SaltDNA is a proprietary framework that is easily and quickly updated based on evolving state-of-the-art open source encryption developments. Since it is agnostic to encryption, SaltDNA will never be limited by an encryption legacy.

Why Open Source Encryption?

No one should ever trust proprietary encryption algorithms. Open source encryption algorithms are open to reviews and auditing from security experts around the world. Such openness has two advantages. First, you can be confident that only secure algorithms can stand the test of time while being poured over by thousands of cryptanalysts. Second, if bugs are found, they'll move quickly to fix them. In sum, a good algorithm is public and open, where the only secret is the private key or the password.

To protect mobile communications, enterprises need to secure the mobile endpoint and encrypt the voice and text conversations while in transit. Just like firewalls, intrusion prevention and anti-virus, encrypted mobile communications should be standard in any enterprise security strategy. Secure calling needs are moving beyond just international travellers, top executives, or government officials. Every enterprise that communicates strategic information via mobile devices should have an encrypted mobile communications solution that also provides tight control of users, calling circles, call activity, metadata and call quality.

In an Encrypted Mobile Communications Solution, Enterprise Controls Matter

It's simply not enough to tell key employees to use a consumer based encrypted app. Enterprises need encrypted solutions that allow them to remain in full control of their private mobile communications. Secure enterprise mobile communications solutions must:

Have an adaptable encryption framework – For the strongest protection against information breaches and man-in-the middle attacks, secure mobile communications solutions should always use the most up-to-date encryption from wherever that open source innovation originates. It must never be limited by an encryption development legacy.

Offer deployment ease and flexibility – An enterprise needs to be able to choose the type of deployment that best meets its security, privacy, and compliance needs.

Enhance employee productivity and accelerate internal communications – The best private mobile communications solutions should be simple for employees to use, allow remote provisioning, and should work with current mobile phones. This way employees and trusted partners can communicate with complete privacy wherever and whenever necessary.

Have tight enterprise controls – An enterprise needs to be able to control the numbers of users, their calling circles, and even the quality of those mobile voice communications.

Allow enterprise ownership and control of call metadata – With a network operator-based service, you cannot ever be sure that your voice communications are not available to foreign governments or competing state-owned corporations. With a hosted encrypted mobile communications service, you can never be sure that you are not leaving meta-data within their systems that can leave you vulnerable. Therefore, it's imperative that the enterprise deploy a secure solution where call or text meta-data always remains within its control.

The Only Encrypted Mobile Solution Designed- from the Ground Up - for Enterprise

SaltDNA Enterprise software is a completely secure end-to-end voice and text communications solution that allows an enterprise to communicate privately across any network, anywhere in the world. Comprised of two powerful components that work together, it features the SaltDNA Communication Manager, a web-based portal with enterprise control functions and the SaltDNA Mobile App, a simple-to-use, client-side download.

It's your security, so you should be able to choose how best to implement SaltDNA within your enterprise. To that end, SaltDNA Enterprise has three different deployment options.

- Subscribe to SaltDNA as a service that is hosted on your own virtual instance within SaltDNA's highly secure data center. In the hosted service, the enterprise controls its own SaltDNA Communication Manager just as you would if it were deployed within your environment.
- A trusted managed security service provider can deploy and operate SaltDNA within their infrastructure.
- If your enterprise has the highest level of security requirements and must eliminate the existence of any third-party, you can easily and quickly install SaltDNA onto off-the-shelf hardware within your own infrastructure.

Regardless of which deployment your enterprise chooses, user provisioning is fast and easy. Your administrator simply logs into the SaltDNA Communications Manager and remotely enrolls and provisions devices by adding user names, phone numbers, and emails. Mobile users are then automatically notified via email and authorized to download the SaltDNA Mobile App.

Working on any iOS or Android device, the user installs the application on his or her smartphone. Launch the app, and you are ready for secure and completely private communications to other authorized SaltDNA users in your circles. There is no need to use special phones, to change phone numbers, maintain a virtual number or a calling list for an over-the-top voice service. Using SaltDNA is as simple as using any mobile app, and enables the enterprise to effectively control and manage popular Bring Your Own Device (BYOD) policies.

The Highest-Grade Encryption with the Tightest Controls.

To truly free enterprise mobile communications, the SaltDNA Enterprise solution strikes the right balance between encryption and control.

The highest-grade, rock-solid encryption

While encryption alone is not enough, it is still of paramount importance in an enterprise-grade secure mobile communications platform. SaltDNA uses an encryption mixture using multiple encryption algorithms in three tiers for maximum security. First, SaltDNA creates a Virtual Private Network (VPN) tunnel using IPSEC. Second, at the transport layer, SaltDNA follows the current best practice and uses Transport Layer Security (TLS) version 1.2.

As for keys, SaltDNA currently uses 2048-bit RSA, which provides the highest level of security balancing the computational requirements and power consumptions on based mobile devices. While it's certainly true that longer key lengths are incrementally more secure, they also considerably impact battery usage due to longer CPU usage to complete the handshake. Further, key exchanges are temporary based on Diffie-Hellman and use per-session, temporary keys during that initial TLS 1.2 handshake. This simply means that each communicating party verifies each other's identity before the temporary key disappears. Diffie-Hellman also guarantees perfect forward secrecy where encrypted communications recorded in the past cannot be retrieved and decrypted should long-term secret keys or passwords be compromised in the future. In total, the combination of TLS 1.2 together with 2048-bit keys provides for maximum protection against the most skilled attackers suitable to protect the most sensitive data and applications.

The third and innermost layer of encryption protection is based on the traffic type itself. For voice and voice over Internet Protocol (VoIP) traffic, SaltDNA calls are secured through the cocktail of Secure Remote Transport Protocol (SRTP) with key negotiation using Zimmerman Real-time Transport Protocol (ZRTP).

Working together within the IPSEC VPN, the SaltDNA voice traffic is both efficiently processed and impossible to crack. For texts, SaltDNA secures traffic using Instant messaging security using Off the Record (OTR) cryptographic protocol to allows authentication between and among mobile users, so each one can be confident in a mobile user's message authenticity, but leaves no trace upon completion. This means the message can be completely burned or deleted by either the receiving or sending mobile users, leaving behind no metadata. Texts hold OTR through Axolotl where each message is encrypted with its own key using a 256-bit AES cipher in Counter (CTR) mode. CTR mode performs the encrypt and decrypt processes more quickly on mobile devices than other modes because decrypt is the same transform as encrypt; the result is that it requires half the code and processes more quickly for a high quality mobile experience. Again, moving within the IPSEC VPN, the SaltDNA Mobile App makes your text traffic attack-proof.

Tightest Enterprise Controls Available

Enterprises need to both secure AND control their mobile communications. Specifically, enterprises need to control network access, authentication, application access, and performance as well as provide robust management, audit, and compliance features. Since SaltDNA runs over a private network, the enterprise can control quality for all but the local access portion of the mobile traffic.

Administrators log into the SaltDNA Communications Manager using two-factor authentication. Once there, administrators can define granular levels of access based on client identity, group policies, and pre-access compliance. They can also manage permissions and access to software applications.

When a mobile user logs in to access your network, it also uses two-factor authentication to make sure a user is properly identified. The SaltDNA Communications Manager also checks to see if a mobile device operating system has been altered on the device. Alterations, known as jailbreaking or rooting, generally make the device more open and enable tethering and other unauthorized apps. The mobile device obviously is more vulnerable to stability issues, malicious apps and actors. If SaltDNA detects an altered device, it is automatically blocked from accessing corporate resources or using private communications.

With the SaltDNA Communication Manager, administrators have many other control functions at his or her fingertips. There's real-time reporting for instant detailed security analysis. Administrators can assess which users have good security habits to comply with internal and external regulations and which ones do not, and take appropriate action. You, the enterprise, own and control all communications metadata; if your enterprise requires communications metadata archives, the system makes them available for analysis without compromising individual privacy. If your enterprise does not want to keep communications metadata, then it is wiped, leaving no trail that communication ever existed.

There's also a separate SaltDNA Compliance Manager that remotely provisions devices to split personal traffic from enterprise traffic to allow an employee to simultaneously have personal privacy and access to corporate resources. Further, the SaltDNA Compliance Manager allows compliance with call recording requirements in accord with industry regulations. For example, financial services executives can be assured of secure communications while call recordings are made and archived.

SaltDNA

Eliminate Mobile Communications Security Risks with SaltDNA Enterprise.

SaltDNA develops solutions that leverage multi-layered encryption techniques to secure enterprise mobile communications. SaltDNA Enterprise is the first enterprise-class solution for highly secure communications, with robust central control and optional auditing features to meet regulatory compliance requirements.

For more information visit our website
www.NEWCOMGlobal.com/SaltDNA

NEWCOM

575 Washington Street
Pembroke, MA 02359

781.826.7989

@NEWCOMGlobal