\Orchestrating a brighter world NEC

NEC UNIVERGE BLUE® CLOUD SERVICES

Security information

UNVIERGE BLUE® CONNECT KEEPS YOUR BUSINESS COMMUICATIONS SECURE

You can feel confident that your private data is safe with NEC’s UNIVERGE BLUE® CONNECT. Our system utilises state-of-the-art technologies designed to constantly monitor for, and defend against, malicious intruders.

The UNIVERGE BLUE® Security Platform includes these 5 primary security pillars which are constantly evolving in order to respond to, and mitigate, any potential threat. These 5 pillars are regularly examined and reviewed by the NEC UNIVERGE BLUE® security team to ensure our customers receive a secure communications & collaboration experience that can be trusted to protect them and their businesses.

INFRASTRUCTURE & NETWORK SECURITY

DATA PROTECTION & PRIVACY

PHONES, DEVICE & APP SECURITY

MONITORING & DETECTION

SECURITY COMPLIANCE

1 | INFRASTRUCTURE & NETWORK SECURITY

NEC invests considerable human and capital resources to help ensure high levels of security and protection that give you peace of mind. Infrastructure and Network Security is one of the pillars of our Stress Free Experience. We understand that if you're to trust us with your communications and data, you need to understand how we'll protect it. Vigilance is essential to keeping your business safe.

HIGHLY SECURE DATACENTRES

NEC's UNIVERGE BLUE® cloud is hosted in geographically dispersed, highly secure and monitored datacentres by certified tier-three providers.

Each of NEC's UNIVERGE BLUE® world-class datacentres adheres to strict standards in physical security. Each datacentre is closely monitored and guarded 24/7/365 with sophisticated pan/tilt closed-circuit TVs. Secure access is strictly enforced using the latest technology, including electronic man-trap devices between lobby and datacentre, motion sensors, and controlled ID key-cards. Security guards are stationed at the entrance to each site.

INFRASTRUCTURE PROTECTION

System and network security is important to NEC and its customers. In order to maintain a secure infrastructure, NEC's UNIVERGE BLUE® has several layers of security controls in operation. These controls include processes for managing user access to critical systems and devices, formal policies for authentication and password controls, and configuration standards for firewalls.

NEC's UNIVERGE BLUE® has also implemented several monitoring controls to identify potential security threats and notify personnel of the severity of the threat. Firewalls are in place and configured to NEC standards to prevent unauthorised communications. Network-based intrusion detection systems are configured to detect attacks or suspicious behavior, and vulnerability scans are performed to identify potential weakness in the security and confidentiality of systems and data.

We also run multiple Antivirus and intrusion protection systems (IPS) (both host and network) to help detect and deter malicious network traffic and computer usage that often cannot be caught by a conventional firewall. The system monitors for unusual traffic patterns and alerts system administrators of any suspicious behavior.

Antivirus and IPS can also help prevent network attacks against vulnerable services; data-driven attacks on applications; host-based attacks such as privilege escalation; unauthorised logins and access to sensitive files; and malware (e.g., viruses, Trojan horses, and worms).

OTHER NETWORK SECURITY HIGHLIGHTS:

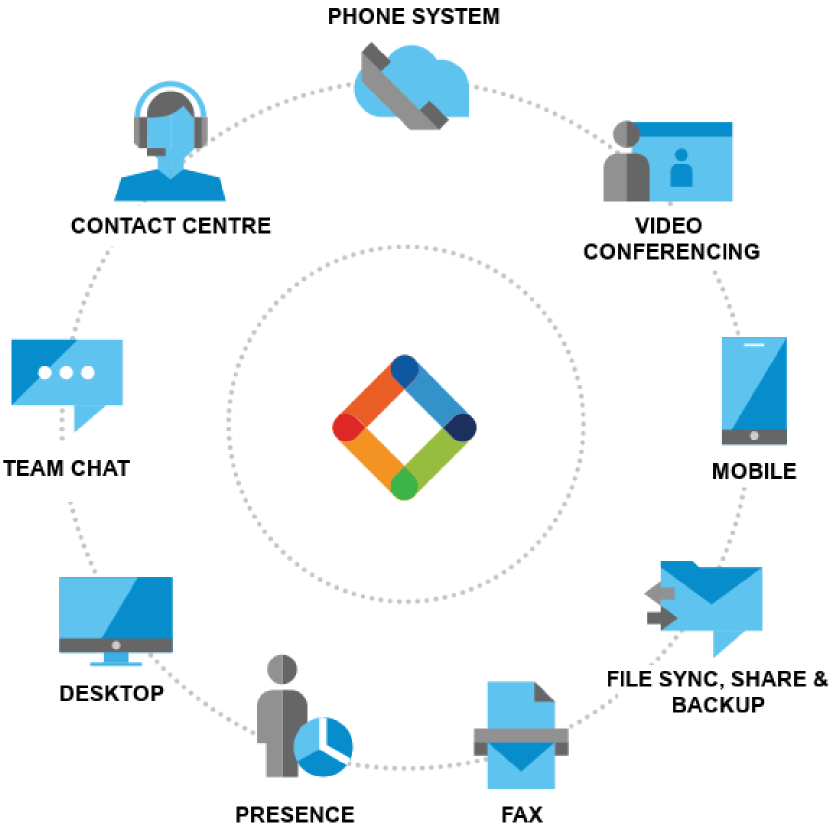
- Commercial-grade edge routers are configured to resist IP-based network attacks
- NEC's UNIVERGE BLUE® subscribes to Distributed Denial of Service (DDoS) protection through a leading provider of network security
- Production network is physically and logically separated with highly restricted access and multiple authentication levels
- Operational functions include: monitoring, system hardening, and vulnerability scans

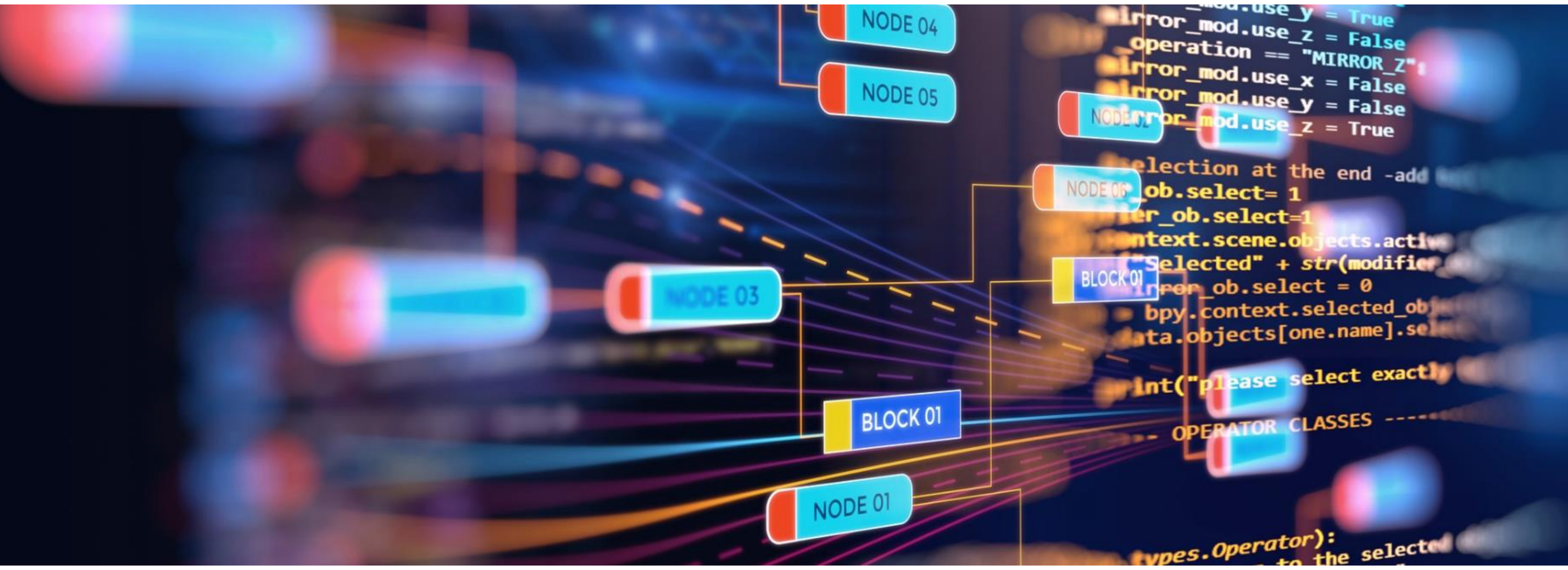
EMPLOYEE SECURITY

Employees for NEC's UNIVERGE BLUE®, regardless of role, undergo rigorous background checks. Employee access to passwords, encryption keys and electronic credentials is strictly controlled using two-factor authentication and role-based access control. Access to servers is restricted to a limited number of authorised engineers and monitored regularly.

DEDICATED SECURITY STAFF AND MONITORING

NEC's UNIVERGE BLUE®, employs dedicated, full-time security staff who are certified in information security. This team is involved with all aspects of security, including log and event monitoring, incident response, managing intrusion detection systems (both host and network), perimeter defense, service and architecture testing, and source code reviews.





2 DATA PROTECTION & PRIVACY

NEC, we’re committed to protecting the privacy of your data and making sure you are in complete control of where and how it’s used. Your cloud contains extremely valuable and confidential content, including intellectual property, customer data, financial information, and sensitive personal data. You need to have confidence in how it’s stored and managed.

PRIVACY POLICY

NEC offers a clearly documented Privacy Policy, which governs our treatment and handling of sensitive data, including personally identifiable information. NEC also adheres to the EU-U.S. Privacy Shield Framework set forth by the U.S. Department of Commerce and the European Commission.

To read NEC’s UNIVERGE BLUE® Privacy Policy, please visit this link.

DATA JURISDICTION / RESIDENCY

Our NEC UNiVERGE BLUE® service uses datacenters located in the Eastern and Western United States, Canada, the United Kingdom, Germany, Australia and Japan.

DATA ENCRYPTION

Data encryption protects sensitive customer and call data from unauthorised access.

In addition, numerous state, federal, and industry regulations regarding customer and patient privacy mandate encryption of data. NEC’s UNIVERGE BLUE® employs encryption, both in-transit (using TLS encryption) and at-rest (using AES 256-bit keys), as an essential component of our “secure-by-design” product architecture to help keep your data private and secure. Data encrypted while at rest includes voicemails, call recordings, meeting recordings/chat/notes, chat and SMS history, chat attachments, and UNIVERGE BLUE® SHARE files.

3 PHONES/DEVICES/APP SECURITY

Encryption technology is important to keep conversations and data secure from prying eyes. However, encryption only tells part of the story. NEC’s UNIVERGE BLUE has several technologies that keep intruders from having the ability to access your internal systems and apps.

SECURE HANDSET PROTECTION

To verify that phones and devices are secure from cyber threats and attacks like eavesdropping, we require strong passwords on all SIP endpoints. Each device is securely provisioned using “HTTPS” with mutual authentication to prevent intrusion.

AUTHENTICATION FOR UNIVERGE BLUE® CONNECT APPS

The Desktop and Mobile Apps from UNIVERGE BLUE CONNECT allow users to use their CONNECT business phone system while working remotely or on the go. These apps can require a login and password and can also be enabled with 2-factor authentication for access. Access to the customers online portal requires 2-factor authentication (it is not optional) to keep company data secure.

GOOGLE CHROMIUM BROWSER SECURITY PLATFORM

The UNIVERGE BLUE® CONNECT Desktop App is built using Google Chromium browser technology. It makes use of the very latest security enhancements available and is updated regularly to keep current with the latest security patches. Chromium’s architecture focuses on preventing attacks from persistent malware, transient keyloggers, and file theft.

UNIVERGE BLUE® CONNECT

4 MONITORING & DETECTION

AUTOMATED 24/7 TOLL FRAUD & THREAT DETECTION

NEC's UNIVERGE BLUE® monitors call patterns to international (and high-cost) locations on a constant basis and consistently looks to improve our fraud monitoring systems. If any customer exceeds the call thresholds for any international areas, NEC's UNIVERGE BLUE® will disable international calling and send an email notification to the customer informing them that international calling has been disabled based on possible fraudulent activity. To protect the customer, we will not re-enable international calling until the account holder has given NEC authorisation.

Additionally, NEC's UNIVERGE BLUE® employs active monitoring to detect and notify customers of suspicious login activity and unrecognised devices on their network.

SPAM CALLER PROTECTION (US ONLY)

Every account is enabled with Spam Caller Protection – helping to keep you and your employees free from calls originated by autodialers and known fraudsters. To learn more, see our UNIVERGE BLUE® Spam Caller Protection Knowledgebase article.

5 SECURITY COMPLIANCE

SOC 2

SOC 2 is a technical audit specifically designed for service providers who store customer data in the cloud. NEC's UNIVERGE BLUE® CONNECT, ENGAGE, MEET and SHARE service provider has a SOC 2 report from an independent auditor that has validated that, in their opinion, NEC UNIVERGE BLUE® CONNECT, ENGAGE, MEET and SHARE service provider's controls and processes are effective in minimising risk and exposure to this data.

CPNI

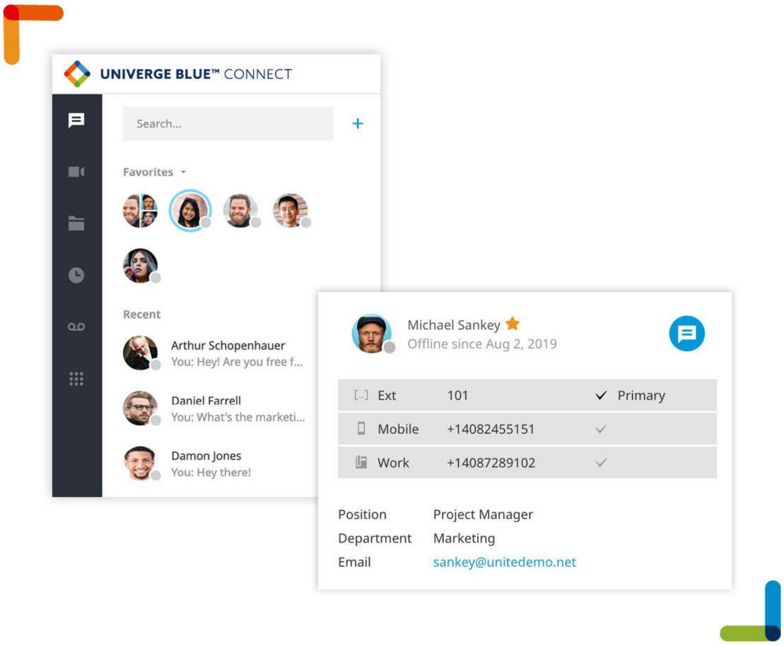
Consumers are understandably concerned about the security of the sensitive, personal data they provide to their service providers. The Federal Communications Commission (FCC) requires carriers like NEC to establish and maintain systems designed to ensure that we protect our subscribers' Customer Proprietary Network Information (CPNI).

Each year, NEC files an annual certification documenting our compliance with these rules.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store, or transmit credit card information maintain a secure environment.

The payment processing system utilised by NEC has passed these strict testing procedures, and is compliant with the Standard. This helps ensure that your payment information will not be accessed by unauthorised parties or shared with unscrupulous vendors.



Arthur Schopenhauer
You: Hey! Are you free f...

Daniel Farrell
You: What's the marketi...

Damon Jones
You: Hey there!

Michael Sankey
Offline since Aug 2, 2019

Ext	101	✓ Primary
Mobile	+14082455151	✓
Work	+14087289102	✓

Position Project Manager
Department Marketing
Email sankey@unitedemo.net

PRIVACY SHIELD AND GDPR

NEC’s UNIVERGE BLUE® CONNECT, ENGAGE, MEET and SHARE service provider has extensive experience managing a highly secure infrastructure and complying with complex regulations. As noted above, they currently self-certify compliance with the EU-US Privacy Shield framework and are committed to comply with the EU’s General Data Protection Regulation (GDPR) across our services. NEC and NEC’s UNIVERGE BLUE® CONNECT, ENGAGE, MEET and SHARE service provider maintains a security environment that meetsthe requirements of the GDPR, and we offer GDPR-compliant Data Processing Addendums (DPAs) to our channel partners and customers to help assure them that our processing and handling of their data will meet the GDPR’s standards.

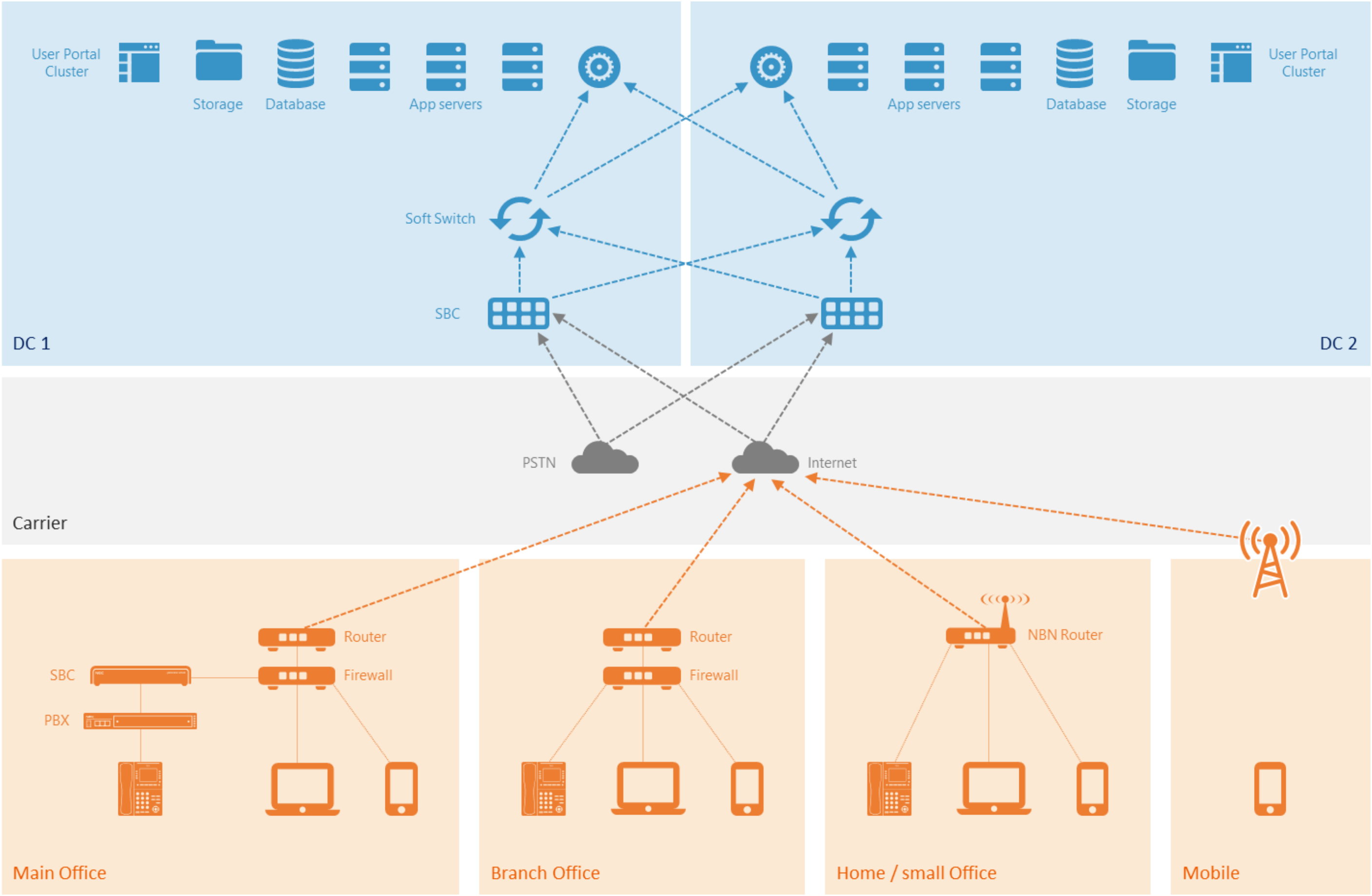
HIPAA

The confidentiality and security or “privacy” rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require entities that engage in HIPAA transactions to protect sensitive health information against disclosure to unauthorised parties.

When combined with your strong internal security policies and procedures, the NEC UNIVERGE BLUE® CONNECT service (using the recommended settings shown below) helps to safeguard Protected Health Information (PHI) by adhering to the required administrative, physical, and technical standards outlined in the HIPAA Security Rule.

NEC can partner with healthcare organisations to help protect your PHI. If you are subject to HIPAA’s requirements, ask your NEC Sales Representative about putting in place a Business Associate Agreement (BAA).

NETWORK TOPOLOGY



MAIN OFFICE

All communications will be performed over the Internet and it is recommended that you use a commercial grade Router and Firewall to limit your network exposure. A list of firewall ports and exclusions is listed on the following pages.

If using UNIVERGE BLUE BRIDGE to connect your NEC phone system and the UNIVERGE BLUE CONNECT applications, then a Session Border Controller should be used to secure SIP trunk communications between the NEC phone system and the UNIVERGE BLUE cloud infrastructure.

BRANCH OFFICE

All communications will be performed over the Internet and it is recommended that you use a commercial grade Router and Firewall to limit your network exposure. A list of firewall ports and exclusions is listed on the following pages.

HOME / SMALL OFFICE

All communications will be performed over the Internet and it is recommended that home routers are configured to limit your network exposure. Disabeling ALG on home routers or enabling TLS for voice will minimise any potential home network configuration issues.

MOBILE

All communications will be performed over the Internet via Mobile internet or Wi-Fi. All communications are encrypted to ensure safe and secure usage even while using public Wi-Fi.

BANDWIDTH

To ensure the best voice quality, it is recommended that the internet services delivered to each location meets or exceeds the required bandwidth for the number of devices in use.

Bandwidth can be measured using our quick bandwidth test.

A detailed network assessment can also be run to ensure the best quality results.

FIREWALL CONFIGURATION

VOIP PHONES / SBC

Service	Port	Protocol
Provisioning (config.telecomsvc.com)	TCP 80, 443, 1443, 2443, 6716, 6718	Varied
Registration	UDP 5060; TCP 5060	SIP
Secure SIP	TCP 5061	SIP TLS
Audio Stream	UDP 35000-65000 (assigned dynamically)	RTP, SRTP
Presence Servers	TCP 5222, 5280	Varied

CLIENTS

Service	Port	Protocol
Web	TCP 80, 443	Varied
Screen sharing	TCP/UDP 3478	STUN / TURN

SERVICES URL'S

Service	URL
UNIVERGE BLUE™ CONNECT API	api.elevate.services
UNIVERGE BLUE™ CONNECT STS	*.serverdata.net
UNIVERGE BLUE™ SHARE	*.myonlinedata.net
IPS+PBX clusters	*.telecomsvc.com
UNIVERGE BLUE™ CONNECT spellcheck library	*.gvt1.com

ACCESSING MORE INFORMATION

- UNIVERGE BLUE's official Australian website https://www.univergeblue.com/au
- UNIVERGE BLUE applications https://univerge.blue/apps
- Knowledge Base articles https://kb.univerge.blue
- Legal docs https://univerge.blue/legal/asia-pacific/