



TRANSACT
TRANSFORM
RUN
RECYCLE



Cloud Security



Centric cloud security and unified threat protection

Digital transformation is accelerating the adoption of cloud based services and applications across every industry sector. This has led to the volume of attacks on cloud services more than doubling in 2019, as cybercrime criminals transition to the cloud to blend in, increase success rates and evade detection.

Generally the hackers target the most popular cloud services and apps, knowing that its easier to abuse the implicit trust that users and admins place in the market leading products and platforms.



Centric Cloud Security & Unified Threat Protection

Addressing the evolving security needs driven by digital transformation

However often the biggest threat to cyber security isn't an external attack. Over 80% of security and data breaches are internal, often caused by poor working practises or malicious / negligent staff.

The nature of collaborative working and modern applications for comms, cloud storage, file sharing, finance tools and social media all encourage the free flow of data which adds to the risk of a security breach. Digital transformation and the influx of remote working practices has expedited this, as more people, devices, applications and data are now outside of the enterprise network perimeter than inside it.

This means that legacy security technology and practices leave organisations blind to the majority of data loss risks and cyber threats.

A different approach is needed to reduce the new and evolving set of risks associated with the cloud.

Netskope

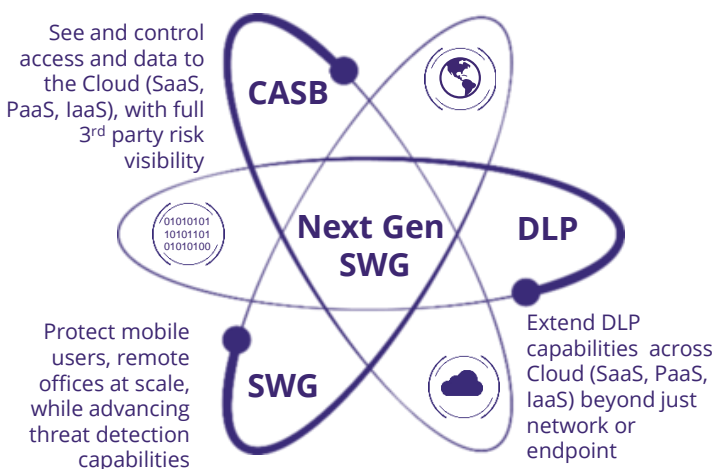
The Netskope Security Cloud provides unrivalled visibility and real-time data threat protection when accessing cloud services, websites, and private apps from anywhere, on any device.

Netskope enables enterprises to extend their data security and threat protection policies to users and data, wherever they may be.

This includes managed and unmanaged cloud apps, public cloud environments, websites, and an enterprises' private apps hosted either in their data centers or in public cloud.

Taking a new approach to securing cloud services and web traffic. The Netskope platform enables you to apply policy controls to thousands of cloud services and web traffic via their Next Gen Secure Web Gateway.

Netskope Provides Converged In-Line Security Architecture



Traditional secure web gateways are limited:

- Appliance-based approach with limitations of scale, focusing on legacy URL filtering
- Lack of visibility into inline SaaS requests and shadow IT apps
- Limited policies beyond "allow / deny"
- Lack integrations to adjacent security tools

Netskope's approach:

- 100% cloud-based, including SSL Decryption
- Inline visibility and security controls for all web traffic and cloud services
- Advanced, granular DLP controls
- Ability to integrate with SIEM, EDR, and EUBA tools

A single platform for SaaS, IaaS, Web and Private access

Next-Gen Secure Web Gateway (SWG)

Netskope provides a cloud-based web security gateway that understands cloud applications in addition to filtering web usage. The SWG protects users accessing the web by detecting threats such as malware, phishing sites, and drive-by exploits. It also protects an organisation's data from exfiltration or exposure due to risky user activities within cloud applications, or the uploading of sensitive data to Shadow IT. Netskope Secure Web Gateway is built to meet the needs of the largest of organisations, providing a low latency service with full SSL inspection of traffic.

Market-Leading Cloud Access Security Broker (CASB)

The CASB quickly identifies cloud application usage and secure data in managed or unmanaged cloud applications. This prevents sensitive data from being exfiltrated to Shadow IT by risky users, or exposed to the internet from an organisation's cloud storage platform. Netskope's CASB secures and protects Office 365, G Suite, Salesforce and many other enterprise applications.

Cloud Data Loss Prevention (DLP)

Users can protect sensitive company data from loss and exposure with one of the most advanced cloud-based DLP in the industry. Capabilities including 3,000+ data identifiers, support for more than 1,000 file types, custom regular expressions, proximity analysis, international support using double-byte characters, fingerprinting, OCR, and exact data match.

Private Access

Netskope Private Access provides users with seamless and secure remote access to applications in both public cloud and private data centre environments. This scalable solution avoids the need for remote users to VPN through the corporate network. Providing a low-latency end user experience for accessing private applications.

Contact

LONDON

12 Moorgate
London
EC2R 6DA

T +44 (0) 2392 825925

PORTSMOUTH

New Hampshire Court
St Pauls Road
Portsmouth
PO5 4AQ

T +44 (0) 2392 825925

STEVENAGE

Suite 204
Kings Court Business Centre
London Road
Stevenage
SG1 2NG

T +44 (0) 2392 825925

WOKINGHAM

Oaklands Business Centre,
Saxon House,
Oaklands Park,
Wokingham
RG41 2FD

T +44 (0) 2392 825925

PORTSMOUTH

Unit 8 Discovery Voyager Park
Portfield Road
Portsmouth
PO3 5FN

T +44 (0) 2392 825925

SINGAPORE

Bell Group Asia Pte Ltd
30 Cecil Street 14-01
Cecil Street Equity Plaza
Singapore 049705

T +44 (0) 2392 825925

GLASGOW

Suite 11, Sky Hub
Skypark management Suite
Skypark 1, 8 Elliot Place
Glasgow, Lanarkshire
G3 8EP

T +44 (0) 2392 825925

HYDERABAD

Bell Integration T/A
Choose Portal Pvt Ltd
1st Floor, Krishe Sapphire
Madhapur Hyderabad,
Telangana, 500081

T +44 (0) 2392 825925

SINGAPORE

Bell Group Asia Pte Ltd
109 North Bridge Road
05-21 Singapore
179097

T +44 (0) 2392 825925

KRAKOW

Bell Integration sp. z o.o.
Kurniki 9,
31-156 Kraków
Poland

T +44 (0) 2392 825925

See how Bell integration can help your business succeed.
Please contact us on marketing@bell-integration.com or
visit www.bell-integration.com