whitespider®

Managed Network Identity & Access Services

Service Definition

Executive overview

Modern organisations no longer operate within a clearly defined network perimeter. Users, devices, applications, and data are distributed across campuses, branch locations, cloud platforms, and remote environments. As a result, identity has become the primary control point for securing access to digital services.

WhiteSpider's **Managed Network Identity & Access Services** provide a comprehensive, managed approach to controlling who and what can access the network, from where, and under what conditions. Building on the principles of Zero Trust and Secure Access Service Edge (SASE), this service extends beyond connectivity and edge security to deliver consistent identity, access, and policy enforcement across the entire estate.

The service incorporates leading technologies including **Cisco Identity Services Engine (ISE), Cisco Duo, Meraki Access Manager, Juniper Access Assurance**, and SASE capabilities, delivered through WhiteSpider's proven Professional and Managed Services model.

The shift to identity-centric networking

As highlighted in WhiteSpider's existing SASE service description, traditional perimeter-based security models are no longer effective in a world of cloud applications and remote users filecite turn1file0. While SASE provides a powerful framework for secure connectivity and edge-based security, it must be underpinned by strong identity and access controls to be truly effective.

Managed Network Identity & Access Services extend the SASE model by ensuring that access decisions are continuously informed by user identity, device posture, location, and risk. This enables organisations to move from implicit trust based on network location to explicit trust based on verified identity and context.

Core service capabilities

Network Identity and Policy Control (Cisco ISE)

Cisco Identity Services Engine (ISE) provides centralised identity-based access control across wired, wireless, and VPN environments. WhiteSpider manages the full lifecycle of ISE, enabling organisations to define and enforce granular access policies based on user identity, device type, and security posture.

This capability allows CIOs to implement consistent access controls across campuses, branches, and data centres, improving security while simplifying operational management.

Strong Authentication and User Trust (Cisco Duo)

Cisco Duo delivers multi-factor authentication (MFA) and adaptive access controls to protect users and applications. Integrated into the wider identity framework, Duo strengthens security for remote access, cloud applications, and privileged users.

By incorporating device trust and contextual signals, Duo supports Zero Trust access models without introducing unnecessary friction for end users.

Cloud-Managed Access Control (Meraki Access Manager)

Meraki Access Manager enables simplified, cloud-managed identity and access enforcement across Meraki-based networks. WhiteSpider manages policy configuration, integration with identity providers, and ongoing optimisation to ensure secure and seamless access for users and devices.

This capability is particularly well suited to distributed environments where operational simplicity and rapid scalability are key requirements.

Policy Assurance and Continuous Validation (Juniper Access Assurance)

Juniper Access Assurance provides continuous validation of access policies and network behaviour, helping organisations ensure that intended security policies are consistently enforced.

WhiteSpider uses this capability to provide ongoing assurance that identity and access controls remain effective as networks evolve, reducing configuration drift and improving auditability.

Secure Access Service Edge (SASE)

SASE remains a key component of the service, providing secure connectivity, Zero Trust Network Access (ZTNA), and cloud-native security services for users and locations. Identity services integrate tightly with SASE to ensure access decisions are consistently enforced across networks, applications, and cloud services.

Cisco Umbrella

WhiteSpider Managed Services

whitespider®

Simplifying security threat Management

With an ever-evolving cyber landscape, businesses are facing increased and more complex threats. Attacks are happening at a far greater rate which means that organisations are having to navigate an ever-changing threat landscape, often without skills or knowledge at their disposal.

Ciscos Umbrella

Cisco's Umbrella offers flexible, cloud-delivered security when and how you need it. It combines multiple security functions into one solution, automatically uncovering current and emerging threats and enabling protection of devices, remote users, and distributed locations anywhere. Umbrella is a simple way and effective way to protect users everywhere.

Our Umbrella managed service

WhiteSpider's Umbrella managed service helps organisations of all sizes maintain a more secure environment. Combining all the benefits of Cisco's Umbrella service with our 24x7 support from a team of industry experts, we ensure that your organisations responds rapidly to security threats.

We deliver round the clock support and management of your Cisco Umbrella. With our managed service- you can utilise ongoing support from experienced consultants and protection from state-of-the-art security tools. We will help you to detect and respond to security threats before they impact your business.

Key benefits

24x7 monitoring and response

Our round the clock support means that security events are continually being monitored and responded to.

Ongoing support from expert consultants

Our specialists will manage events and provide support, taking the day-to-day overhead away from your internal teams.

Advanced security controls with threat intelligence

Our log management captures all events which helps us understand and analyse machine generated data.

Detailed reporting

Our service provides real-time in-depth insight into the security of your systems and offers operational intelligence reports into your security posture.

Service offerings

Essentials

- DNS Layer security
- Web filtering by domain
- Custom domain list filter
- Discover & block shadow IT
- Reporting and log management

Advantage

- Full DNS Layer security
- Secure web gateway
- Umbrella investigate
- Shadow IT management
- Reporting and log management

Secure internet gateway

- All Advantage features
- Full secure web gateway
- Cloud delivered firewall
- Cloud access security broker
- Integration into Cisco SD-WAN.

Proactive threat protection

WhiteSpider's Umbrella managed services delivers secure, reliable, and fastest internet experience to business users everywhere. As a provider of network security and recursive DNS security Cisco Umbrella enables connectivity to the internet with confidence on any device.

Visibility and protection everywhere

Umbrella provides the visibility needed to protect internet access across all network devices, office locations, and roaming users. All internet activity is logged and categorised by type of security threat or web content, and the action taken — whether it was blocked or allowed. Logs of all activity can be optionally retained for investigation.

Block malware without latency

Umbrella is a cloud-delivered security service built into the foundation of the internet. It enforces security at the DNS layer and blocks requests to malicious domains before a connection is even established.

Easily enforce content web filtering

WhiteSpider can manage your user's internet access using a wide range of Umbrella's category-based content filters. We work with you to create custom allow/block lists, and block domains with unwanted content. This enable you to enforce and comply with acceptable use policies.

Key features

Block domains associated with phishing, malware, botnets, and other high-risk categories

Prevent web and non-web callbacks from compromised systems

Proxy and decrypt risky domains for deeper inspection of URLs and files (DNS Advantage or above required)

Enable web filtering using 85+ domain categories

Create custom block / allow lists

Pinpoint compromised systems using real-time security activity reports

Discover and block shadow IT (based on domains) with the App Discovery report

Use Investigate web console for interactive threat intel access and the on-demand enrichment API to integrate intelligence into other systems (DNS Advantage or above required)

Protect mobile and roaming users who are off-network

Create policies and view reports by user, network, network device, or roaming device

Use customisable block pages and bypass options

Firewall Services

WhiteSpider Managed Services

whitespider®

Next-Generation Firewalls (FirePower) / IPS / IDS / Threat Protection

As our business-critical applications are a blend of cloud and on-premises based and users need secure access to resources from everywhere, the traditional firewall approach no longer works. The single network perimeter has evolved to multiple micro-perimeters. For many organisations the application is the new perimeter, and traditional firewall deployments have evolved to a mixture of physical, virtual and cloud-native appliances.

Secure Firewall gives integration between core networking functions and network security, resulting in a complete security portfolio that protects your applications and users everywhere

WhiteSpider's service benefits

Proactive monitoring

WhiteSpider provided firewall management and maintenance, including persistent eyes-onglass with security event monitoring and 24/7 escalation.

Achieve superior visibility

Regain visibility and control of your encrypted traffic and application environments with Cisco Firepower next-gen IPS.

Make zero trust practical

Secure Firewall makes a zero-trust posture achievable and cost-effective with network, micro-segmentation and app security integrations

Stop more threats

Contain known and unknown malware with Cisco Advanced Malware Protection (AMP) and sandboxing.

Detect earlier, act faster

The Cisco Annual Security Report identifies a 100-day median time from infection to detection, across enterprises. Reduce this time to less than a day.

Drive efficiency at scale

Secure Firewall supports advanced clustering, high availability and multi-instance capabilities, enabling you to bring scalability, reliability and productivity.

WhiteSpider professional services

WhiteSpider Professional Services support the design and deployment of identity and access solutions aligned to organisational security strategy and business outcomes.

Engagements begin with discovery and assessment activities to understand existing identity systems, access models, network architecture, and security requirements. WhiteSpider then designs an integrated identity and access architecture incorporating Cisco, Meraki, Juniper, and SASE components.

Implementation services include platform deployment, integration with directories and identity providers, policy definition, and controlled migration from legacy access models. This structured approach ensures a smooth transition to identity-centric access control with minimal disruption.

WhiteSpider managed services

WhiteSpider Managed Network Identity & Access Services provide ongoing operational management and optimisation of identity platforms and access policies.

The service includes continuous monitoring of identity systems, authentication services, and policy enforcement points. WhiteSpider proactively manages configuration, updates, and lifecycle activities to ensure platforms remain secure, resilient, and compliant.

Access policies are regularly reviewed and optimised to reflect changes in users, devices, applications, and risk. Incidents related to access, authentication, or policy enforcement are handled through WhiteSpider's service desk, with clear escalation and reporting processes.

This managed approach reduces operational risk and complexity while ensuring identity and access controls remain aligned to business needs.

Key features and benefits

For CIOs, Managed Network Identity & Access Services provide a consistent and auditable control plane for access across the organisation. Centralised identity management reduces security risk, supports Zero Trust initiatives, and simplifies compliance with regulatory requirements.

Operationally, the service reduces the burden on internal teams by offloading the complexity of managing multiple identity and access platforms. End users benefit from secure, seamless access experiences that support modern working practices without compromising security.

Use cases

Organisations adopting Zero Trust architectures use the service to enforce identity-based access across networks, applications, and cloud services.

Distributed enterprises benefit from consistent access control across campuses, branches, and remote users, reducing reliance on network location as a security boundary.

Public sector and regulated organisations gain improved visibility, governance, and auditability of access decisions, supporting compliance and security assurance.

Why WhiteSpider

WhiteSpider combines deep expertise in networking, security, and identity platforms with a proven managed services capability. Our technology-agnostic approach ensures solutions are aligned to organisational outcomes rather than constrained by individual products.

By partnering with WhiteSpider, organisations gain a trusted provider capable of designing, delivering, and operating identity-centric access services that support secure digital transformation.

Next steps

Managed Network Identity & Access Services can be tailored to organisational size, complexity, and security maturity. Engagements typically begin with an assessment to define scope, priorities, and service alignment.

whitespider®

Telephone: +44 20 3773 2380
E-mail: info@whitespider.com
Website: www.whitespider.com

/whitespider

CYBER ESSENTIALS PLUS

bsi ISO/IEC 27001 Information Security Management CERTIFIED

bsi UKAS MANAGEMENT SYSTEMS 0003