

HCLTech | Supercharging
Progress™

HCLTech Integrated Secure Access Service Edge (SASE)

Powering the future of secured connectivity

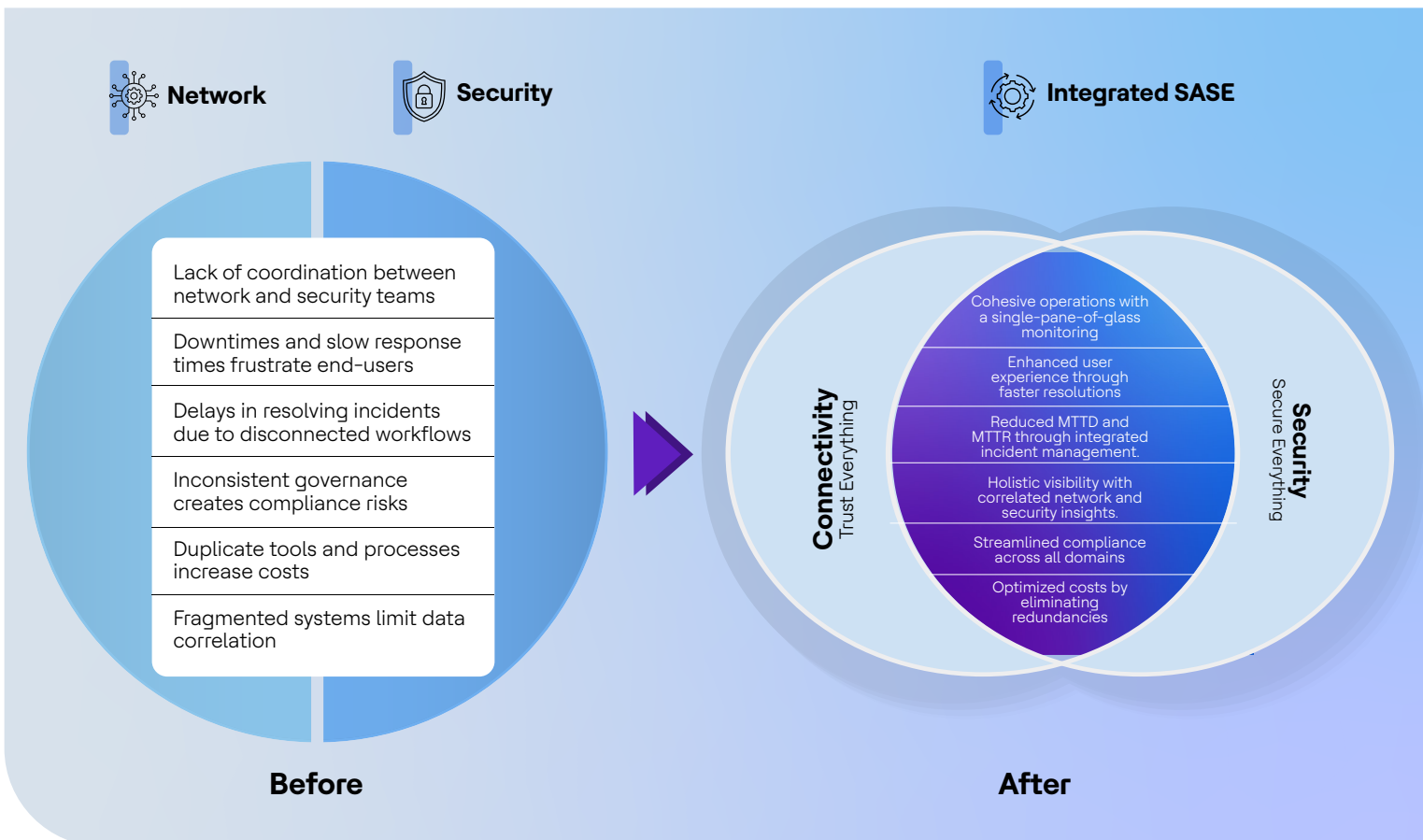


Overview

Traditional network and security operations approach no longer suffice in today's fast-paced, ever-evolving digital landscape. Historically, network and security functions operated in silos, resulting in fragmented management and overlooked security vulnerabilities. This separation was manageable earlier, but as cyber threats have become more sophisticated, these siloed processes have proven increasingly inefficient. Enterprises now face heightened cost pressures, the urgent need to counter next-generation cybersecurity threats and the demand for streamlined operations. Organizations are consolidating their service providers to meet these challenges and merging the Network Operations Center (NOC) and Security Operations Center (SOC) into a unified, integrated operation. This shift not only optimizes management but also enhances security, provides greater visibility, and accelerates threat response.

Integrated SASE (Secure Access Service Edge) represents a transformative evolution from traditional, fragmented security solutions. By converging essential networking and security functions—such as SD-WAN, firewall-as-a-service, secure web gateway, cloud access security broker and Zero Trust Network Access (ZTNA) into a unified, cloud-native architecture, integrated SASE ensures seamless integration. This flexible, cohesive approach empowers enterprises to boost efficiency, drive business agility and simplify complex IT operations. Integrated SASE equips organizations to address modern cybersecurity needs effectively, providing scalable and resilient network protection in today's dynamic digital world. It is particularly valuable for secure remote access, branch internet connectivity, and multicloud environments.

The diagram below shows Integrated SASE bridging the gap between network and security operations.



Breaking down silos: The challenges of network and security fragmentation

In traditional IT environments, network and security operations often run in isolation, leading to fragmented workflows and inconsistent policies. This lack of integration creates visibility gaps, delays threat response, and complicates troubleshooting, especially in hybrid and multicloud setups. As cyber threats grow in complexity, the need for seamless collaboration between these teams becomes critical. To bridge this gap, organizations need a unified approach to address the pressing challenges highlighted below:

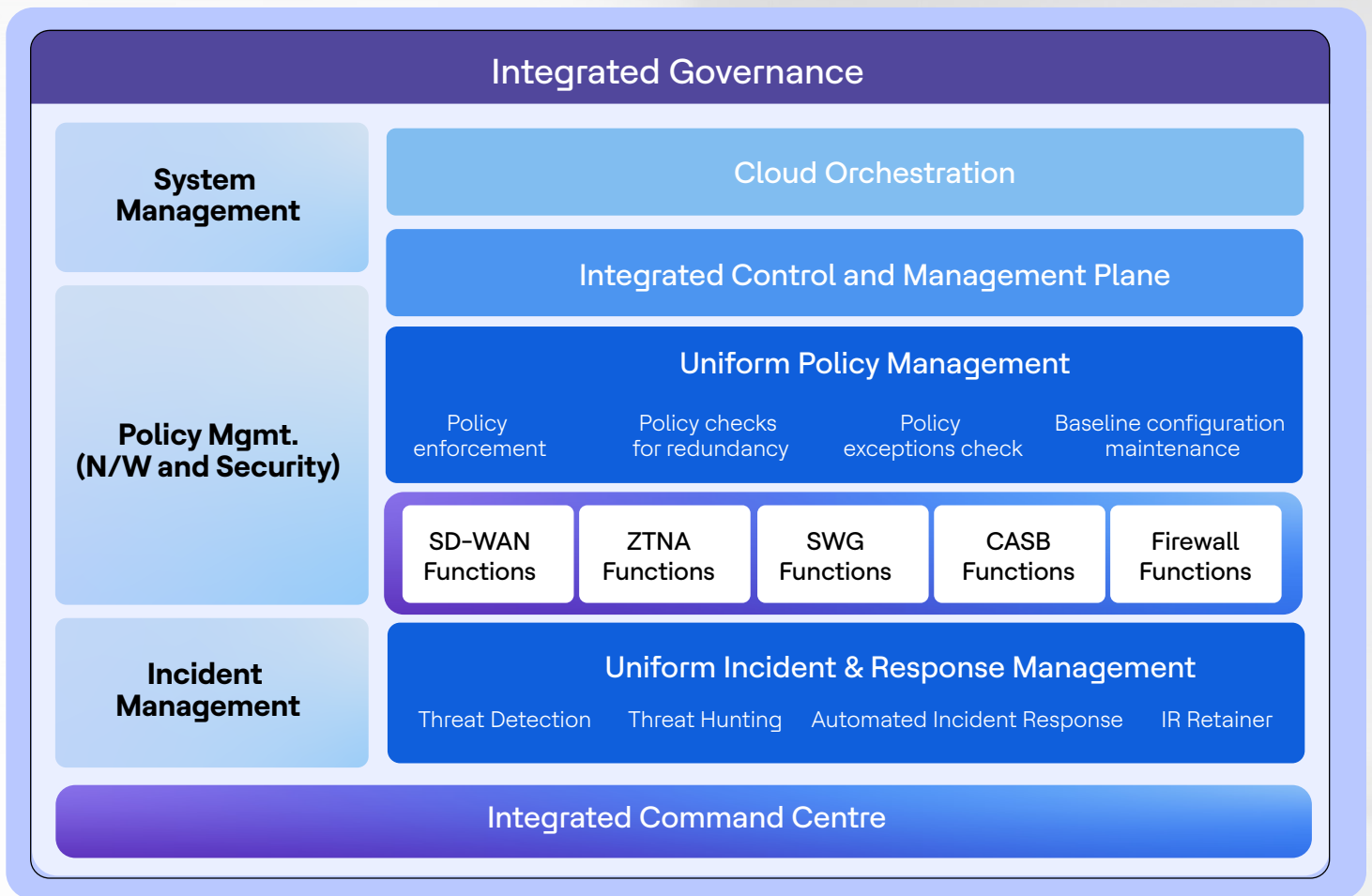
- 1 Disconnected NOC and SOC operations** hinder collaboration, causing delays in resolving cross-domain issues and increasing risk exposure.
- 2 Manual incident handoffs** prolong detection and resolution, leading to extended downtimes and service disruptions.
- 3 Duplicate tools and overlapping processes** inflate operational costs, draining resources and reducing efficiency.
- 4 Separate compliance management** for network and security creates regulatory gaps that might lead to penalties and reputational damage.
- 5 Duplication of efforts** leads to redundant investigations, wasting resources and slowing decision-making across teams.
- 6 Misaligned objectives between NOC and SOC** prevent unified business outcomes, impacting performance and risk mitigation.
- 7 Fragmented data storage** limits operational visibility, complicating root cause analysis and reducing threat response effectiveness.
- 8 Disjointed processes** degrade user experience, causing frequent downtimes and dissatisfaction among customers and partners.

Our solution

HCLTech Integrated SASE framework

HCLTech Integrated Secure Access Service Edge (SASE) provides a unified platform for managing network and security services. By combining key components like system management, policy management, incident management and an integrated command centre, our approach delivers operational efficiency, robust security and reduced complexity. Our integrated Network and Security Operations Center (NOC and SOC) eliminates silos, offering customers streamlined operations with proactive threat detection, faster incident response and comprehensive visibility across their network-security landscape.





Key components of Integrated SASE include:

Integrated governance: Ensures seamless oversight and control across the network and security domains. It enables strategic alignment and provides consistency in policies, incident resolution and monitoring

System management

- **Cloud orchestration:** Simplifies the management of multicloud environments, ensuring agility, scalability and optimized resource utilization.
- **Integrated control and management plane:** Provides a single pane of glass for centralized control, reducing operational overheads and ensuring synchronization across network and security systems
- **Uniform policy management:** Offers a unified approach to enforce security and network policies. Features include Policy enforcement and redundancy checks, exception handling and baseline configuration maintenance

Incident management

- **Uniform incident and response management:** Combines threat detection and hunting to identify issues and automated incident response for proactive risk mitigation proactively
- **IR retainer:** Ensures dedicated incident response resources for critical scenarios, minimizing downtime and damage.

Our unified SASE framework enables businesses to stay ahead of threats while optimizing network performance, ensuring a future-ready, streamlined digital infrastructure.



Service catalog

HCLTech Integrated SASE service catalog offers a balanced mix of must-have features and advanced add-ons to meet your organization's evolving needs, ensuring scalability, security and an enhanced user experience. With a modular design, businesses can leverage essential capabilities right out of the box while seamlessly adding premium features as their network and security requirements grow.

- **Standard features: The essentials you can't do without**

Our standard service offering provides the essential building blocks to optimize network performance, streamline traffic and enhance security. With advanced traffic flow analysis, policy creation and native SSE integration, we simplify network management and enable secure access. Enterprises can gain insights with WAN utilization analysis, real-time analytics, monitoring and comprehensive reporting, ensure seamless connectivity with user experience monitoring and secure application access through ZTNA. User protection is enabled with advanced SWG features and strengthened security with cloud-delivered firewall-as-a-service (FWaaS). These foundational elements deliver a robust and reliable integrated SASE experience tailored to meet your organization's "must-have" operational and security requirements.

- **Add-On features: Unlock advanced capabilities**

Enhance your Integrated SASE deployment with premium add-ons that unlock advanced capabilities and drive efficiency. Integrate third-party SSE solutions for flexibility, streamline processes with automation and ensure seamless connectivity with cloud traffic forwarding. Gain superior control over cloud applications with advanced CASB, protect sensitive data with advanced DLP and deliver exceptional user experiences through user digital experience management. These advanced features act as "value accelerators," enabling deeper security, enhanced performance and seamless scalability to help your business thrive in an ever-evolving digital landscape.

Whether you're looking to address immediate needs or future-proof your network with advanced capabilities, our comprehensive service catalog is tailored to meet your unique business requirements. Together, let's build a secure, high-performance and seamless digital experience that drives your organization forward.



HCLTech | Supercharging
Progress™

hcltech.com