SAFETY FIRST.
Then innovation

Enable secure automation that gives your business access to a world of digital business opportunities

WHAT IS BCX CISCO END-TO-END SECURITY SOLUTIONS?

A suite that offers end to end security solutions from Cisco, ranging from Endpoint to Edge and Data Centre, on Premise, Cloud, or Hybrid. These solutions include hosted, shared and dedicated security devices and services based on client business needs, with the key support service offerings within the Enterprise Cloud and centralised management platform.

WHAT IT DOES

We use Zero Trust Verefication:
- Verifying your user is who they say they are.
- Ensuring they have access to only the applications they need.
- Establishing that their device is secure and trusted.

We verify trust for workloads by:
- Identifying what applications are running.
- What is communicating your applications and data.
- Verifying that communication between workloads is secure and trusted.

We verify trust for the workplace by:
- Ensuring users and devices need to authenticate before connecting to your network.
- Tracking what they're allowed insight into.

HOW IT WORKS

Cisco Zero Trust allows you to:

Secure the workforce with Duo by ensuring only the right users and secure devices access your applications. We do this by verifying user identities with multi-factor authentication (MFA) and ensuring the trust of their devices by checking their security hygiene and posture.

Secure your workloads with Tetration by securing the connections within your applications, across the multi-Cloud. We do this with application micro-segmentation that ensures the right applications, servers, databases, containers and more can access or speak to each other, within your Data Centre and Cloud infrastructure.

Secure the workplace with SD-Access by securing the connections across your local network, including interconnected devices and OT (operational technology) like printers, cameras, badge scanners and more. We do this with network segmentation by ensuring only the right users and devices can access components across your network.

Finally, Cisco Zero Trust provides comprehensive visibility, policy enforcement and reporting capabilities across your workforce, workloads and workplace to help you better prevent, detect and respond to any risks, and provide secure, trusted access across your entire IT environment.

WHY CHOOSE BCX?

We offer peace of mind to clients, knowing that their company's security assets are protected and managed by a team of highly skilled security experts.

FEATURES AND BENEFITS

FEATURES

Our portfolio and threat intelligence empower our clients to achieve comprehensive protection across the entire threat kill chain, the defined phases of cyber-attacks. Attacks can be disrupted by having the right technologies at each phase. The Cisco Security portfolio offers layered security that can stop attacks at virtually every step of the kill chain. We've made sure our portfolio integrates meaningfully, by sharing key security information between products.

- We share threat intelligence across the portfolio to improve threat efficacy.
- Event visibility is shared to decrease the time to detect threats.
- Sharing context across products decreases investigation times.
- Lastly, automating policies decreases time to remediate.

This integration delivers automation that improves security and speeds responses.

BENEFITS

- We start with best of breed products, protecting the network, endpoint, applications, and Cloud.
- We use trust verification as a foundational piece to ensure only the right people gain access
- Each product is backed with the largest industry-leading Talos threat intelligence, that blocks more threats, see it once protect everywhere.
- We provide automated responses to advanced threats and streamline operations with integrated threat and security management throughout our portfolio.
- Lastly, we build our products to work with the other technologies you have in place for integrated security responses – even 3rd party products.

PRODUCT OPTIONS

IDENTITY SERVICES ENGINE:

Market-leading security policy management platform that unifies and automates secure access control.

ISE enforces role-based access to networks and network resources and delivers superior user and device visibility that enables streamlined enterprise mobility experiences. Cisco ISE now uses Cisco Platform Exchange Grid (pxGrid) to share dynamic contextual data with both network and security partner technology integrations to accelerate their capabilities to identify, mitigate, and remediate threats.

STEALTHWATCH

Cisco Stealthwatch collects and analyses network data to automatically detect threats that manage to infiltrate the perimeter and even the ones that originate from within. Using advanced security analytics, Stealthwatch can quickly and with high confidence, detect threats such as C&C attacks, ransomware, DDoS attacks, illicit cryptomining, unknown malware, as well as insider threats. With a single, agentless solution, you get threat visibility into every part of the network, including encrypted traffic, across data centre, branch, endpoint, and Cloud.

UMBRELLA

Cisco Umbrella unifies multiple security functions in a single Cloud service to secure internet access and control Cloud app usage from your network, branch offices, and roaming users. Delivered from the Cloud with 100% business uptime, Umbrella integrates secure web gateway, DNS-layer security, Cloud-delivered firewall, Cloud access security broker (CASB) functionality, and threat intelligence for the most effective protection against threats.

By enabling this from a single service and dashboard, Umbrella reduces the time, money, and resources previously required for deployment, configuration, and integration tasks. And, Umbrella is backed by one of the world's largest threat intelligence teams, Cisco Talos, and provides interactive access to threat intelligence (Umbrella Investigate) to aid incident response and threat research.

AMP FOR ENDPOINTS

Endpoint Protection Platform (EPP) delivers next-generation antivirus that stops today's complex attacks. Endpoint Detection and Response (EDR) offers more advanced capabilities like detecting and investigating security incidents, and the ability to remediate endpoints quickly. We bring EPP and EDR capabilities together for a unified and more complete solution, called Cisco® Advanced Malware Protection (AMP) for Endpoints. AMP for Endpoints leverages multiple protection engines fuelled by Cisco Talos threat intelligence to block threats before compromise. New EDR capabilities make threat hunting easy. Together with Cisco SecureX, you gain better visibility and automation across an expanded set of security telemetry beyond your endpoints so you can respond to threats completely with security that works together.

TETRATION

The Cisco Tetration platform addresses these requirements using unsupervised machine learning, behaviour analysis, and algorithmic approaches. It provides a ready-to-use solution to accurately identify applications running in the data centre and their dependencies and the underlying policies between different application tiers. The platform is also designed to implement a zero-trust model using whitelist policy and segmentation, monitor the behaviour of the processes running on the servers, and identify software-related vulnerabilities and exposures. With this approach, the Cisco Tetration platform provides a multidimensional security approach across virtualized and bare-metal workloads running in a multi-Cloud environment.

EMAIL SECURITY

Cisco Email Security includes advanced threat defence capabilities that detect, block, and remediate threats in incoming email faster. Simultaneously, it protects an organisation's brand, prevents data loss, and secures important information in transit with end-to-end encryption.

MANAGE AND EXECUTE IT ALL ON SECUREX

SecureX is the mortar that multiplies the power of your security solutions.

SecureX connects the breadth of Cisco's integrated security portfolio and your entire security infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoint, cloud, and applications. The result is simplified security, built into the solutions you already have.

SERVICE LEVEL OPTIONS

Service levels are coupled to the Managed Service option selected.

PRICING AVAILABILITY

The BCX Cisco End-to-End Security Solutions is available nationwide. For more information and specific pricing details, contact your account manager or send an email **ITSS2@bcx.co.za**.