

Building Security Resilience

Best practices and best technology
to protect your business.

outcomex


CISCO
Partner

A robust security strategy

for protecting your business is vital

As the rate of cyber attacks are on the rise, including the complexity of these attacks, having a defense system in place that provides complete visibility is paramount. Businesses today operate with multiple security layers, often leading to fragmented threat detection and delayed incident response. Having a modern solution that provides end-to-end visibility, monitoring, automation and AI-driven analytics can greatly increase investigation and response times.

Average cost of cybercrime per report, up 14%:



small business:
\$46,000



medium business:
\$97,200



large business:
\$71,600

Nearly **94,000** cybercrime reports, up 23%:



on average a report every
6 minutes



an increase from 1 report every
7 minutes

Zero Trust

As hybrid work, BYOD (bring your own device), cloud adoption and IoT continue to expand the enterprise attack surface, security teams face growing challenges in managing identity and access management across diverse endpoints, users and applications.

Zero Trust is a security model that takes the guesswork out of understanding who or what is trying to access an enterprise network. The model is grounded on the philosophy of *never trust, always verify*.

“The main principle is providing just in time, just enough access – whether it’s an application requiring access to an API or a user accessing corporate resources,” Arjun De, Outcomex Head of Solution Sales. How that is implemented, and with what tools, technologies and platforms is going to differ.

Cisco Zero Trust: comprehensive protection across three distinct fronts



Zero Trust for Workforce

Establishes trust of people and devices, regardless of their location. Limits network access to the right people via a secure device.



Zero Trust for Workloads

Secure access for applications in the cloud, data centres and other virtual environments. Includes secure connections for APIs, microservices and containers that access enterprise applications.



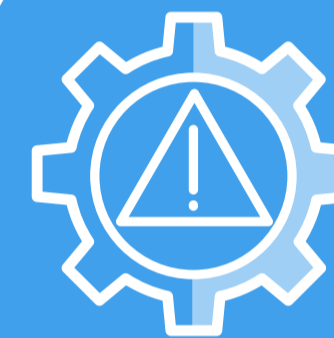
Zero Trust for the Workplace

Access control for all devices that connect to enterprise networks – includes physical and virtual servers, Internet of Things (IoT) and user endpoints like printers and cameras.

Protect your users

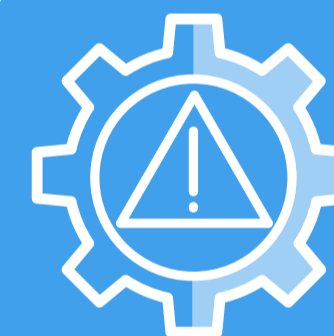
from email phishing, social engineering, MFA bypass attacks, browser-based exploits, malicious websites and stolen credentials

Last year alone, there was a 72% increase in data breaches up from 2021 – around the world, a data breach cost \$4.88 million on average in 2024. While these statistics are alarming, breaches can happen to any organisation. Don't let it be yours. Learn how to keep your business secure and what tools to use to keep on top of and tackle any cyber threats that may threaten your business.



94%

of business have reported email security incidents



\$4.76m

The average cost of a social engineering attack

Source: www.forbes.com

Tool #1: Cisco Secure Access

As one of the best tools in your arsenal, Cisco Secure Access safeguards access to the web, cloud services, SaaS and private applications, while protecting users, data and devices - whether they're working remotely, in the office or on the go.

By providing seamless and secure access from any device to any resource, anywhere, Cisco Secure Access enhances the end-user experience, simplifies IT operations, and reduces risk through granular controls and tighter security.



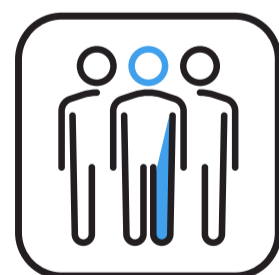
Enable users

to authenticate and go straight to the desired app



Intelligently connect

using the best protocol



Eliminate repetitive

or cumbersome verification tasks



Deliver unmatched

ease for workforce



Tool #2: Duo Multi-Factor Authentication

Most ransomware attacks start with successful phishing campaigns. Companies frequently find themselves exposed to risk because of compromised passwords. Going passwordless can make companies less likely to become victims of ransomware attacks.

Passwordless authentication establishes a strong assurance of a user's identity without relying on passwords, with alternatives such as biometrics, security keys or a mobile device. Duo is innovating towards a passwordless future, that balances usability with stronger authentication.

In an effort to combat hackers who target passwords to access cloud-based applications, passwordless methods that associate users to their devices offer increased security and usability, which is a rare win/win for security.



Identify passwordless

use cases and enable strong authentication



Streamline and consolidate

authentication workflows



Increase trust

in authentication



Provide

a passwordless experience



Optimise

the passwordless toolset

Did you know that with Duo, you get multi-factor authentication, deep device insights, adaptive policies, single sign-on and more – so you can:

Protect logins with two-factor authentication and easily enrol and manage users

Get an overview of device security hygiene

Single sign-on (SSO) for cloud applications

Enforce role-based access policies

Monitor and identify risky devices

Control what endpoints can access apps based on device hygiene

Automatically encourage users to update their own devices

Prevent unauthorised access

Want to learn more about Duo? Reach out to the Outcomex team

Tool #3: Secure Endpoint

Stopping cyberthreats before they disrupt your business operations is the cornerstone of resilience. Secure Endpoint offers advanced endpoint protection across control points, enabling your business uninterrupted productivity without the burden of recovery.

Cisco Secure Endpoint ensures rapid and effective endpoint protection by enabling quick detection, response, and recovery from sophisticated attacks. It features robust Endpoint Detection and Response (EDR), threat hunting, and risk-based security measures.

Enhanced by Cisco XDR and Secure MDR for Endpoint, it offers continuous, expert-driven protection and enhances the efficiency of your security operations.

Secure Endpoint enables customers to detect, respond, and recover from attacks while reducing remediation times by as much as

85%

Cisco Secure Endpoint offers cloud-delivered endpoint protection and advanced EDR across multi-domain control points. It stops threats and blocks malware then rapidly detect, contain, and remediate advanced threats that evade front-line defenses.



Stopping threats and blocking malware



Rapid detection and containment



Remediation of advanced threats that invade frontline defenses

As cyberattacks become more sophisticated, so too, do your security measures need to be. With Cisco User and Breach Protection, providing the ideal combination of security solutions and accelerated responsiveness, its the perfect tool to defend against the rise of sophisticated threats. Cisco Breach Protection Suite unifies threat detection, investigation, mitigation and hunting solutions.

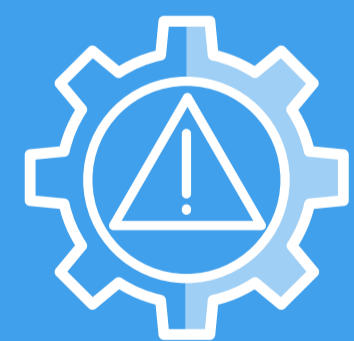
Tool #4: Cisco Secure Email

Considered one of the most financially damaging online crimes, it takes just one click for a business to open itself up to business email compromise.

Safeguard your inbox and your business with proven security solutions – protecting against BEC attacks requires multiple security layers across both technology and people.

Email is simultaneously the most important business communication tool and the leading attack vector for security breaches. In fact, Cisco's Email Cybersecurity Report found that attackers still turn to email as the primary vector for spreading malware.

Cisco Secure Email includes advanced threat defense 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.



35% of malware was delivered by email in 2023



\$2.9bn in losses due to BEC in 2023

Source: www.forbes.com



Detect and block more threats

with global threat intelligence from Talos™ and local intelligence from multiple patented machine learning models.



Combat stealthy malware

that evades initial detection and remediate it fast to reduce its impact.



Drop emails with risky links

automatically or block access to newly infected sites with real-time URL analysis to protect against phishing.



Gain a real-time understanding

of senders and learn and authenticate email identities and behavioural relationships to protect against BEC attacks.



Prevent brand abuse

from attackers using your domain to carry out phishing campaigns with automation of the Domain-based Message Authentication (DMARC) process.



Protect sensitive content

with global threat intelligence from Talos™ and local intelligence from multiple patented machine learning models.



Gain maximum flexibility

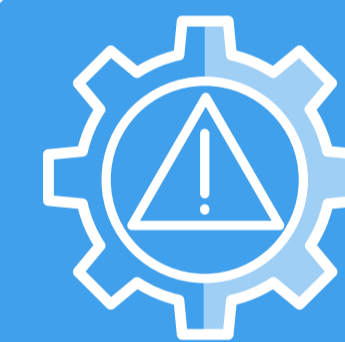
with a cloud, virtual, on-premises, or hybrid deployment or move to the cloud in phases.

Protect your assets

applications, workloads,
networks and clouds

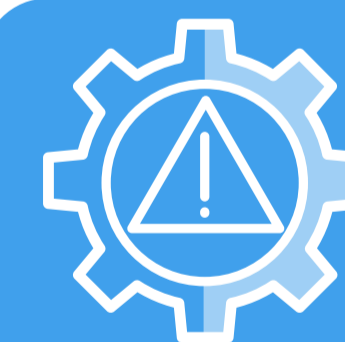
According to *The Cost of Data Breach Report 2024*, 45% of breaches over the past year are cloud based. Utilising security tools that simplify operations, optimise resources, and reduce risk with comprehensive security and pervasive visibility for hybrid and multi-cloud networks, workloads, and applications is essential.

Protecting hybrid and multicloud environments has become more complex as technology changes and cyberattacks increase. This is why having protection that provides end-to-end security for applications, workloads, networks, and clouds for both hybrid and multicloud environments are so pivotal.



\$4.8m

the global average cost of a data breach.



93%

of organisations had two or more identity-related breaches in the past year.

Sources: www.forbes.com and www.ibm.com

Tool #5: Multicloud Defense

Multicloud strategies offer flexibility by combining on-premises, public, private, and hybrid cloud systems, but they introduce complexity and security risks. While multicloud allows tailored solutions for different needs, it increases attack points and security challenges.

While major cloud providers invest heavily in security, human error, like misconfigurations or overly permissive access policies, poses the greatest risk. Partnering with Outcomex and Cisco helps mitigate these risks by providing expert management and comprehensive security solutions that ensure multicloud environments are secure, compliant and optimised for seamless connectivity and reliable operations.

Multicloud Defense: comprehensive security and pervasive visibility for hybrid and multi-cloud networks, workloads, and applications.



Simplifies operations



Optimises resources



Reduces risk and maintains compliance



Protecting your organisation

from ransomware and
malware

Ransomware attacks happen to any business, no matter its size. Unfortunately, these type of attacks are happening more regularly. What can businesses do to ensure that they don't fall victim?

What weapons can you have in your security arsenal that will go beyond rectifying and remediating a ransomware attack?

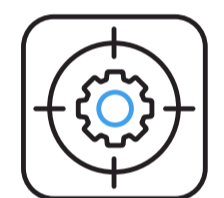
Ensuring a business's exposure to risk is minimised is vital. Your business can have the best security measures in place, but if your employees are not made aware of these, then your best measures are not good enough.

Since a data breach, on average costs \$4.88 million in 2024, employees/users need to be made aware of secure practices and useful tools in place that protect them and the business.

Tool #6: Cisco Extended Detection and Response (Cisco XDR)

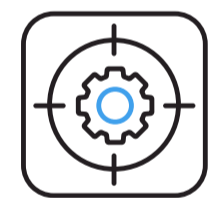
Cisco XDR helps streamline security operations and tools into a unified platform, allowing for faster, more accurate threat detection and response.

The key benefits include:



Enhanced threat detection

through unified global and local context.



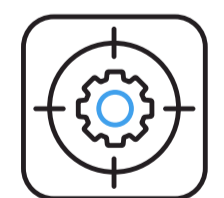
Streamlined operations

with reduced alert fatigue.



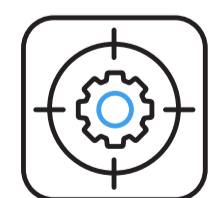
Improved security

posture by consolidating multiple security solutions.



Increased resilience

across complex environments.



Open, cloud-first architecture

for easier integration with existing tools.

As a comprehensive threat detection tool, Cisco XDR provides:



Early Detection

threats are detected sooner preventing potential breaches.



Prioritisation by Impact

allowing security teams to focus on the most urgent issues.



Reduced Investigation Time

and resolution time, allowing security teams to quickly understand and isolate alerts, significantly reducing the time between detection and remediation.



Accelerated Response

automation is leveraged to streamline remediation processes, enabling security teams to respond faster and more effectively to incidents.



Extended Asset Context

providing comprehensive visibility into all assets within the environment, making it easier to identify users and the security posture of the connected devices helping security teams maintain a secure and well-monitored network.

1 in 4

Companies risk a major breach in the next 24 months

206 days

Industry average detection time for a breach

73 days

Industry average time to contain a breach

\$3.9M

Average cost of a data breach

52%

say threat hunting found previously undetected threats

74%

of those implementing threat hunting have reduced attack surfaces

59%

enhanced speed and accuracy of response using threat hunting

*Source: Cisco: Threat Hunting with Securex, stop cyber threats before they start (2023).

Effectively combating cyberattacks

Outcomex's Australia-based SOC team delivers tailored cybersecurity solutions designed to address your unique security challenges and works in close partnership with your business. Our services integrate a holistic blend of leading vendor technologies, proven security frameworks, and the expertise of certified engineers.

Undergoing an end-to-end security assessment is essential for ensuring the security and integrity of any system to help prevent data breaches, system downtime, and other costly security incidents, ultimately protecting the organisation's reputation and bottom line.

11%

of Australian companies are maturely ready to tackle the security risks presented by the hybrid work?

Cybersecurity Readiness Index

<10

11-44

45-75

>76

Beginner

Formative

Progressive

Mature

Where do you stack up?

Outcomex and Cisco partnership

As a Cisco gold partner, we have a deep understanding of the entire Cisco portfolio and are dedicated to pass our experience on to our customers, making sure they receive the best product recommendations and services to meet their requirements. As only one of three partners in ANZ holding the Cisco Master Specialisation, we take great pride in our cyber-security capabilities.

With a dedicated team of security experts to manage and monitor all, or part, of your organisation's environment, whether deployed on-premise, in the cloud or via a secure connection, 24/7, 365 days, you will be able to maximise operational efficiency and enhance security visibility.

outcomex


CISCO
Partner