
NETWORKING
AND YOUR
COMPETITIVE
EDGE

CONTENTS

INTRODUCTION

The future is digital, and the race is on. Businesses across the world are approaching a crucial juncture where those who have the ability to adapt their operations to a rapidly evolving landscape will have the edge over their competitors.

The number of devices communicating across the network has been growing exponentially, but that number is about to explode as the Internet of Things (IoT) continues to become a reality. As a result, it has never been more important to ensure that the edge of a business' network is robust, secure and can be upgraded with the speed needed to capitalise on changing business environments.

Why securing the network edge is so critical

Enterprise networks consist of routers, switches and wireless access points, which are all intelligent devices.

But when these devices are connected to the network edge, it is often to non-intelligent devices like phones, tablets, laptops, printers and IoT sensors, threatening network security. Without a secure network edge, blocking external threats and vulnerabilities becomes very difficult.

Risky business

In today's fiercely competitive marketplace, those who cut corners when investing in their network edge will leave their organisation open to possible data breaches and security threats. They'll also find themselves flying blind when it comes to understanding the needs and wants of their customer, not to mention struggling to keep up with their ever increasing online customer service expectations.

And with most cyber attacks aimed at the network edge, those who fail to invest in secure systems will potentially make their business a target for cyber criminals.

Then there's the ever-spiralling IT costs. Organisations around the world are realising millions of dollars in annual benefits – in both revenue and cost savings – as a result of making their networks more digital ready.

As this white paper will discuss, it's crucial that you don't leave the job half-done when it comes to your business' network edge. Securing your network edge is absolutely critical for your business success and Cisco's DNA will help you create a digital network.

> ***"Those who fail to invest in secure systems will potentially make their business a target for cyber criminals."***

ADVANTAGES OF A STATE-OF-THE ART NETWORK EDGE FOUNDATION

1 **Leveraging the network edge to improve customer experiences and deliver business insights.**

2 **providing critical security at the network edge.**

3 **offering greater opportunity to innovate quickly and better manage future costs.**

CUSTOMER EXPERIENCE AND BUSINESS INSIGHTS

The business world has rarely been more competitive, with transformative disrupters upending entire industries and start-ups carving market share away from legacy behemoths.

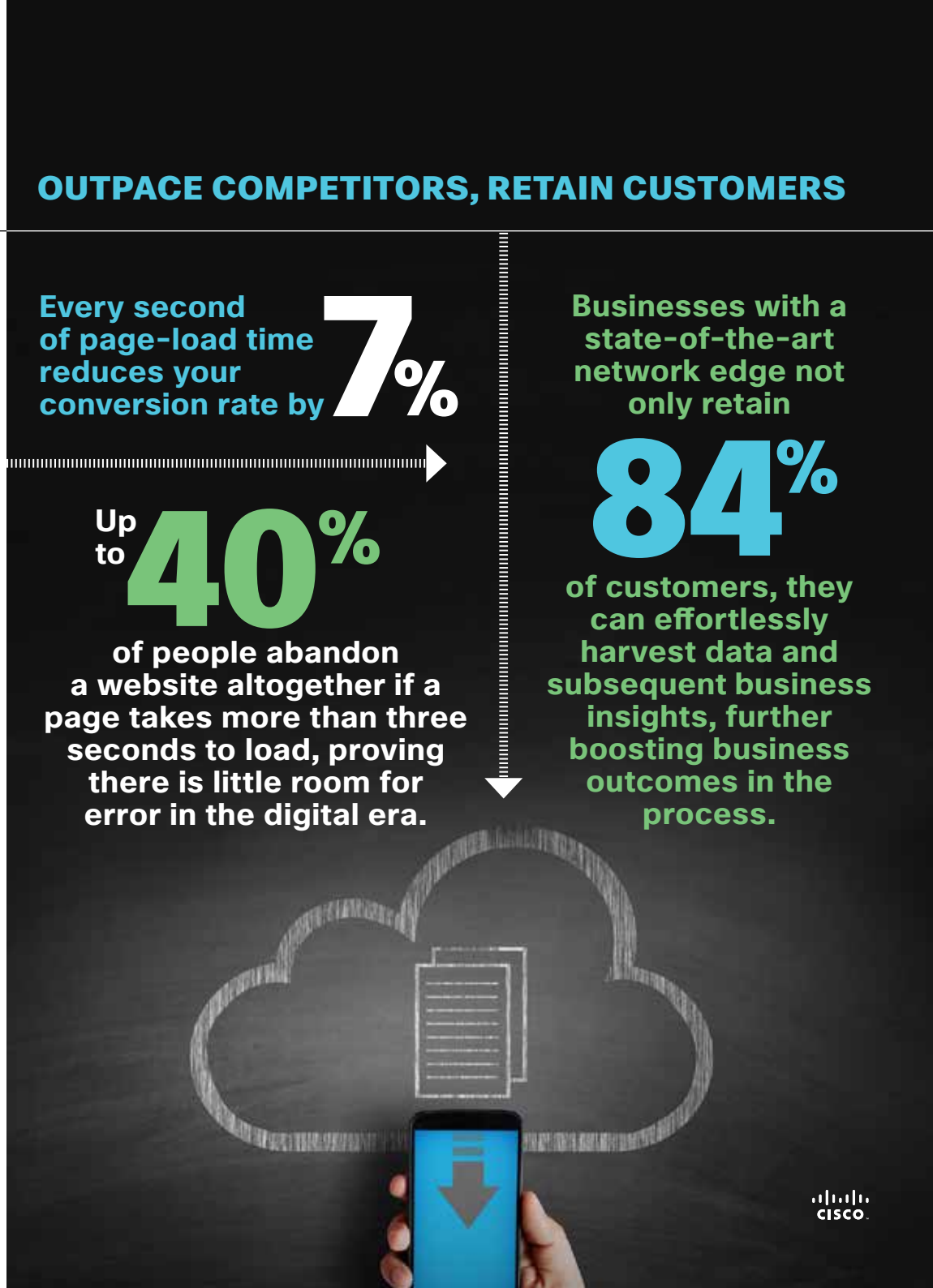
The key to staying afloat is leveraging digital technology to understand one's customers and businesses better than one's competitors, and using those insights to deliver a more enjoyable, more efficient customer experience. And there is no better way to tap into these insights than at the network edge, which is the only platform in any organisation that touches every aspect of a digital business.

Done right, the network edge offers a wealth of knowledge about what's happening within your own organisation. Cisco Digital Network Architecture (DNA) gives you granular insight into your users, the devices they use, and the applications they access.

Outpace competitors, retain customers

If you're not already lining up your ducks for a move to digital, then chances are your competitors are, as 57% of organisations will have pulled the trigger within the next two years. And not without good reason, as ZK Research studies show that digital organisations are 64% more profitable than their more cumbersome counterparts.

By leveraging your network you can bring your company to the fore. Adopting a piecemeal approach to managing your network can result in a poor performing network, which can frustrate customers when engaging digitally with your organisation, resulting in them seeking a more seamless transaction from one of your competitors. Because in the digital world, speed, efficiency and ease-of-use are critical.



Gain business insights

Data analytics plays a huge role in helping keep you one step ahead of the pack, and the network edge is the best place to capture these insights, as all data traffic passes through the network edge.

Through real-time information you can gain an insight into where your traffic is coming from, what devices are being used, and what security threats are putting your business at risk. In a nutshell, that's your who, what and where, covered.

Done right, the network edge offers a wealth of information about what's happening within your own organisation. Cisco Digital Network Architecture (DNA) provides you granular insight into your users, the devices they use, and the applications they access.

It also provides location-based data to better understand how users interact with the environment and your solutions, which in turn allows you to make better business decisions.

> ***Done right, the network edge offers a wealth of information about what's happening within your own organisation.***

Location analytics found in Cisco's Connected Mobile Experience solution (CMX) delivers granular Wi-Fi and Bluetooth Low Energy (BLE) driven location analytics to provide a realistic view of how people interact with their environment.

For example, business-to-consumer (B2C) organisations such as retail, hospitality, and education are able to pinpoint the locations of their customers to within one metre using Wi-Fi + BLE. With this information they can make better business decisions, such as where to place certain products, increasing their revenue opportunities in the process.

But how do enterprises leverage BLE in a scalable, reliable and cost-effective way? Cisco's new Virtual BLE Beacon offers a scalable solution that delivers high accuracy with tremendous operational simplicity. You can place a beacon as easily as dropping a pin on a map. It eliminates costly on-site surveys and the hassle of batteries.

Fruitful partnership

Cisco has recently announced a partnership with mobile device industry leader, Apple, to deliver a better mobile experience. This strategic partnership for both companies leverages the intelligence in the network to provide the best Wi-Fi experience through optimal roaming.

In other words, it's a quick and easy way to improve employee productivity. Enterprises can expect up to eight times faster roaming and 66% more reliable Wi-Fi calling, 50% reduction in network management overhead due to fewer SSIDs, and end users can save their iOS device battery life by 30%.

BOOST PRODUCTIVITY, IMPROVE EMPLOYEE PERFORMANCE

No more flying blind – the future is here.

Companies are increasingly adopting Cisco's unique 'hyperlocation' solution, which allows management and IT to track all devices connected to their network edge to within one metre.

In a nutshell, hyperlocation helps you pinpoint where your staff or customers are, allowing you to run your business more efficiently as a result.

And make no mistake – operational efficiencies have the business world buzzing.

In fact, a recent PWC Global CEO report detailed that 88% of surveyed CEOs think that operational efficiency is showing 'very high' or 'high' value returns on digital investment.

But it's not all about profits. An Australian hospital, for example, has recently been trialling the technology to help fight superbugs and other bacteria.

Doctors and other hospital staff carry a wireless device connected to the network edge, which is then tracked through a new solution called hyperlocation.

If the hospital employee hasn't spent a sufficient amount of time in front of a hand sanitisation unit between seeing patients, they will receive a reminder message to wash their hands. This has enormous health benefits for both staff and patients by reducing the spread of infection as well as cost savings.

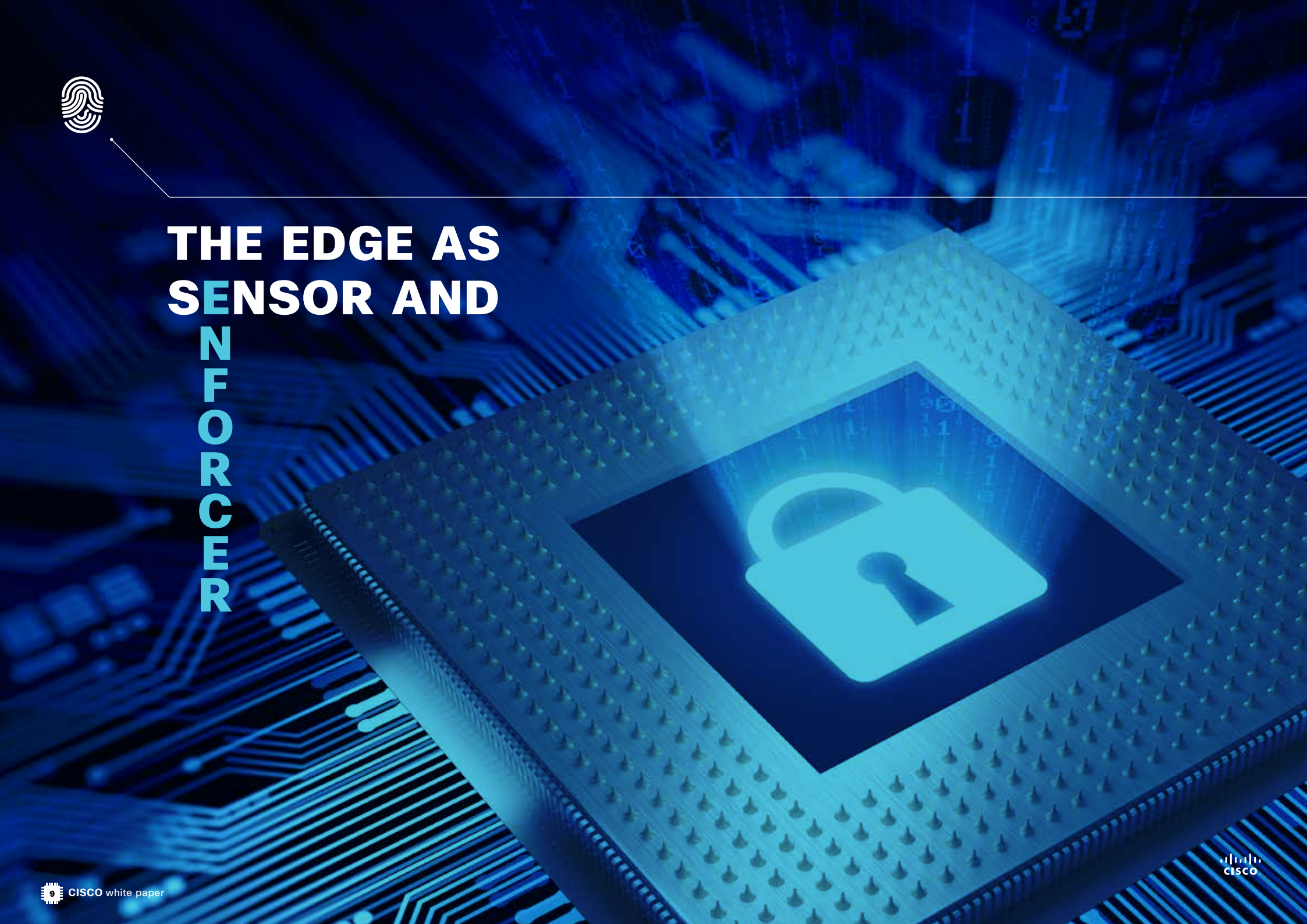
Another way hyperlocation can help a large organisation is by slashing their power bills.

The more people in a room, the harder an air-conditioning unit has to work. But who turns it down once people leave the room?

Hyperlocation can track how many people are in each room of a building and – so long as the air conditioning units are connected to the network as part of IoT – automatically run them as efficiently as possible.

The same goes with lighting. If the network senses there's no one in a room it can automatically turn off or dim the lights in that area.

THE EDGE AS SENSOR AND ENFORCER



Network security is usually thought of as a matter for the network core, but it's an often forgotten fact that many cyber attacks are aimed at the network edge through mobile devices, making it the first line of defence for your business.

Even more concerning: 99% of vulnerabilities exploited will be known by security and IT professionals for at least a year, showing just how hard it can be for IT teams to plug a defensive hole without the right systems in place.

As it takes just a single data breach to jeopardise your organisation, it is critical to have a trusted security solution to identify and control what accesses your network.

A secure network edge is one that boasts real-time threat defence, such as device containment and limitation of access rights, allowing you to instantly detect and shut down anomalous behaviour.

Cyber crime is a booming business, with data breaches estimated to cost companies US $21 trillion globally by 2019

Addressing your vulnerabilities

In a world that is becoming exponentially connected there are more users, more devices and more locations to track and manage. Manually tracking these devices and users one-by-one is no longer plausible, meaning automation is absolutely critical in managing tomorrow's networks.

Organisations are addressing these challenges head-on by moving from fragmented, manual and hardware-centric IT operations that are becoming increasingly vulnerable to hackers, to more adaptive, automated and software-centric networks that are significantly more secure and agile.

In this way, Cisco's network edge products act as both a sensor and enforcer – defending against threats as well as operating as policy enforcer.

As an organisation moves increasingly to a wireless business, where their staff and customers access services through mobile gadgets, these devices become a part of the network edge where highly sensitive data flows back and forth.

This data includes customer purchases and account details, goods and services transactions, medical records, banking, or staff login details – all of which highlight that the network edge needs to be more secure than ever.

WHAT A SECURITY INCIDENT COULD MEAN FOR YOUR BUSINESS:

The average data breach costs companies

US$ 4 million

Half of organisations experience at least a

20%

decline in brand value

It usually takes between

100 to 200

days to detect a security breach

Attackers can compromise an organisation in just minutes

Cyber threats

Cyber crime is a booming business, with data breaches estimated to cost the Australian economy more than $1 billion a year.

Additionally, the impending explosion of IoT devices will throw up new and challenging security concerns.

IoT is expected to create 50 billion endpoints by 2020, according to ZK Research, a dramatic increase on the 10 billion endpoints mobile computing currently creates.

Tracking, monitoring and controlling these IoT devices will be no mean feat. In fact, Gartner predicts that a third of successful attacks experienced by enterprises will be on their shadow IT by 2020, highlighting the importance of an agile network edge.

Cisco's edge

Cisco is heavily invested in developing products and solutions to help move organisations into the digital age by building unique functionality from the ground up, or improving the functionality of existing products.

> ***Being able to deliver reliable service gives your customers a more positive user experience.***

Other key benefits

The benefits of a robust network edge security system aren't limited to mitigating breaches.

An emphasis on real-time threat defence results in rapid resolution of breaches and reduction in unplanned downtime, which improves employee productivity and reduces lost revenue.

And perhaps most importantly, as we will discuss in the next section, having a secure network edge will give your organisation the confidence to roll out new and innovative digital services across the business with minimum risk.

CISCO NETWORK EDGE SECURITY INNOVATIONS INCLUDE:

Network as a Sensor. As all Cisco edge devices include Flexible NetFlow you can have end-to-end flow visibility to discover anomalous behaviours. With commodity technologies you are blinded to behaviours that show you what users do on the network and Internet.

Network as an Enforcer. This is software-defined segmentation embedded in the edge devices that allows for instantaneous and consistent enforcement of security policy in order to control access and contain threats. It works by integrating the Identity Services Engine, StealthWatch (see breakout), and Cisco Security Technology Associate technologies.

Zero-minute defcon policy enforcement. This means you can have preset policies, ready at the push of a button, to respond to catastrophic events such as a day-zero malware or a hacking event.

VITAL SECURITY PRODUCTS TO PROTECT YOUR EDGE

It usually takes most organisations 150 days to detect a security breach. Cisco does it in just 13 hours.

Sophisticated threats can hide in network blind spots, extracting sensitive information and causing millions in damage.

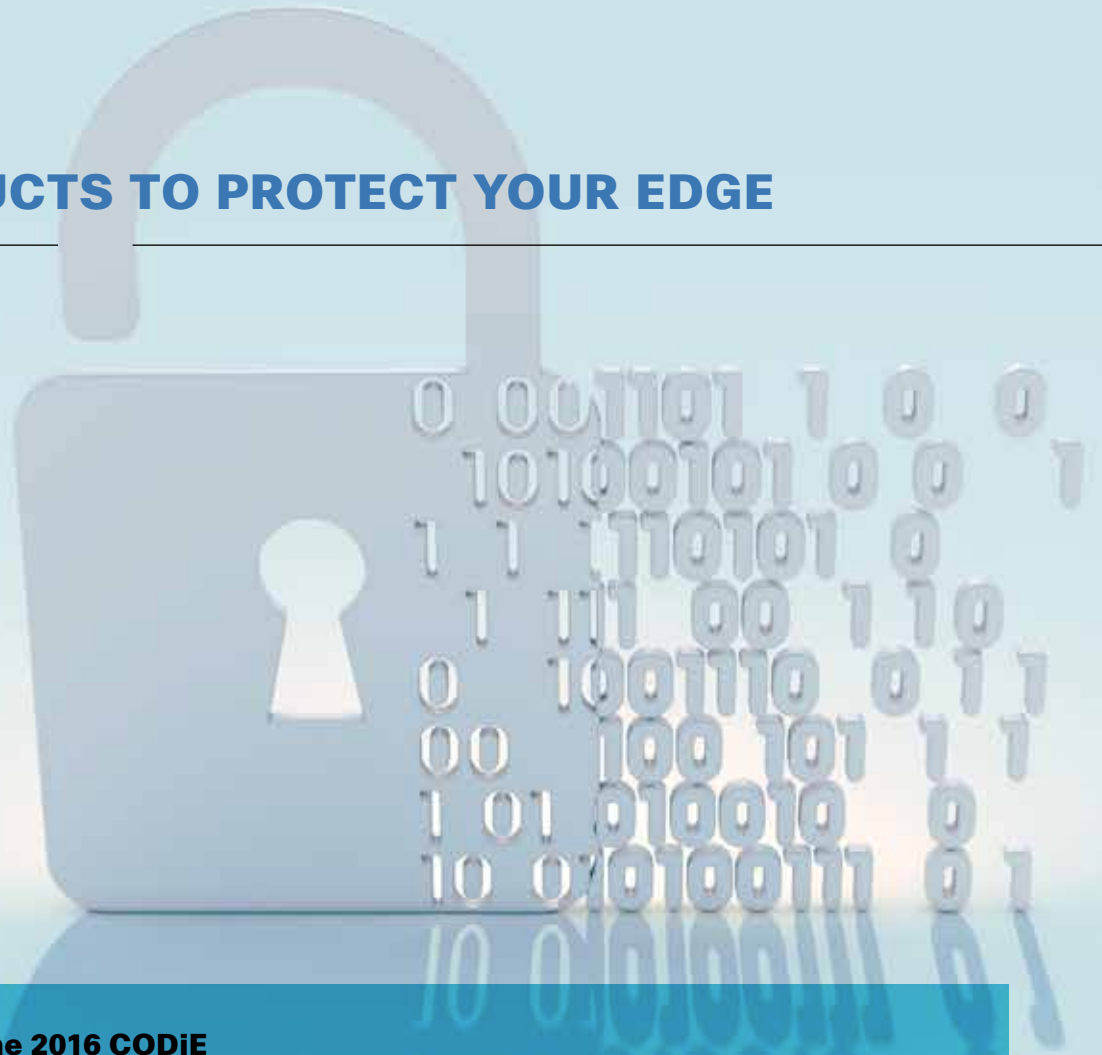
However Cisco security products StealthWatch and Identity Services Engine (ISE) work in tandem to identify and respond to these threats faster.

StealthWatch and ISE are next-generation security solutions that work within Cisco's Digital Network Architecture (DNA), transforming your network into its own security system.

ISE collects the identity of every device and user trying to access your network, while Stealthwatch uncovers threats across the network, even if they bypass perimeter defences.

Together you have an end-to-end sensor and enforcer that can detect and stop sophisticated security issues dead in their tracks.

That means if a breach is unfolding while you're at home having dinner, StealthWatch and ISE are working together to identify, contain and nullify it – all before you walk back into the office the next morning.



PRODUCTS TO PROTECT YOUR EDGE

Cisco security products StealthWatch, TrustSec and Identity Services Engine work in tandem to protect your business from outside threats.

The 2016 CODiE

Winner for best network security solution, StealthWatch goes beyond conventional threat detection by harnessing the data analytical power of NetFlow.
Key features: Real-time threat detection. Incident response and forensics. Network segmentation. Network performance and capacity planning. Regulatory compliance.

Identity Services Engine

Helps IT professionals conquer enterprise mobility challenges and secure the evolving network. It shares data with integrated partner solutions to identify, mitigate, and remediate threats.
Key features: Simplifies guest experiences. Centralises and unifies network access policy management. Provides greater visibility and more accurate device identification. Allows a single point of access policy enforcement across the wired and wireless network.


INNOVATIO
AGILITY AND COST

A successful digital business today thrives on agility and the ability to scale quickly as needed. Most of today's networks have been designed to provide fast, reliable connectivity, but not to meet the new demands that the digital revolution will inevitably make on the network edge.

But Cisco's Digital Network Architecture (DNA) has been designed to specifically help organisations move to a digital business through automation, security and analytics.

Enabling innovation and agility

In order for most companies to successfully innovate, and therefore grow, they must be constantly creating new products and services. However without a secure digital network infrastructure, innovation is generally limited to an on-site business unit or individuals working in isolation.

Enter the importance of the network.

Businesses are now expecting much more from their traditional networks and customers are demanding businesses to provide more and more software applications and services. Networks that are complex, slow to deploy and configure are bottlenecks to business innovation.

Having a digital network enables teams to come together regardless of physical location, device form factor (tablet, desktop, laptop or smartphone) or operating system.

A properly architected networking infrastructure also allows services present in large sites or offices to be extended to home offices and small sites without increasing support costs. Having this flexibility allows organisations to rapidly pivot and pursue new opportunities.

For example, a recent study by IDC showed that by enhancing network edge architecture, network staff were able to reduce the time to market for new services by an average of

41%

which in turn, increased the number of new applications developed and deployed by

178%

Networks today must understand what needs to be done and then do it based on business rules with little on no human intervention. Networks must now be secure, agile and automated.

Automation and virtualisation

With more users, more devices, and more locations to manage, the need to automate processes and new services with day-zero and day-one capabilities is increasingly required.

Networks are transitioning from a customised device-by-device model, where segmentation and access control are added onto a network configuration, to a full policy automated solution.

Cisco DNA, for example, prepares the network to add new functionality and adapt at the speed of change demanded by the customers, the business, or the industry; you can have a network that's open, programmable, and fosters both growth and innovation.

Removing the human element in mass configuration changes provides consistency across the infrastructure, which in turn results in a better user experience and the infrastructure becoming transparent to the end user.

For example, Cisco's Enterprise Network Functions Virtualisation (Enterprise NFV) enables you to turn on network services in just minutes, not months. It provides the compute, storage, networking infrastructure, management, and assurance capabilities to run network services so you can reduce complexity in the branch and enable new services on demand.

False economy of a commodity edge

When measuring cost it's important not to look purely at the upfront capital cost, but also at the costs associated with operation and risk.

While some network infrastructure may boast a cheaper initial price tag, down the track it can begin to have significantly more expensive financial impacts on an organisation, especially where security is concerned.

It is now more critical than ever to ensure that your network edge is secured against cyber threats, particularly given the network edge is where customer data is collected. Your network holds the key to defending your organisation, and as such, a security breach will blow any initial network infrastructure savings out of the water.

In a nutshell: saving a few dollars at the beginning can cost you a lot more in the long run.

Additionally, IDC reports that on average companies reduced their annual costs for physical network infrastructure (switches, routers, firewalls, load balancers, and WLANs) by 43%. These savings often resulted from using more efficient devices, leading to consolidation of hardware and management systems.

Yet much more significant than infrastructure savings was the ability to reduce the time and cost required to administer, maintain, and manage the network environment. In total, companies reduced their average costs associated with deployment, support, and management of network systems by 30% per year.

The network needs to be positioned as the backbone of every organisation. By investing in a Cisco DNA network you can reduce costs by deploying devices faster through automation, provide a programmable network by enabling developers to create new applications and offer a great consistent application user experience for employees and customers.

CISCO DNA

Evolution is born of DNA. Cisco's Digital Network Architecture (DNA) is no different.

Cisco DNA is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations.

The programmable architecture frees your IT staff from time consuming, repetitive network configuration tasks so they can focus on evolving your business.

While every business is different, these days, 99% of them have one thing in common: they need time and resources to innovate and tackle the world head on.

This is where Cisco DNA comes to the fore.

In essence, it brings together virtualisation, automation, analytics, cloud and programmability to build a secure digital network platform for digital business.

Core products that underpin the Cisco DNA story include the new Catalyst 3850 Switches, our wireless product portfolio, controllers and access points, and the Cisco 4000 Series Integrated Services Routers.

Each line of products caters towards the specific needs of individual businesses, no matter your size.

For example, take the Catalyst 3850 Switches – the next generation of enterprise-class, stackable, access layer switches – where there's more than 30 different models to choose from.

Then, for smaller organisations, there are the efficiencies that Cisco DNA can deliver through cloud enabled networking.

Offering true zero-touch provisioning, Cisco can line your business up with switches that can be pre-staged and configured entirely from a web browser. This will accelerate and simplify the work of your network engineer, giving them time to concentrate on helping your business take the next step in its evolutionary journey to becoming a true digital business.

CONCLUSION

Customer experience. Business insights. Security. Automation. Agility. Innovation. Cost reduction. Revenue generation.

The reasons for investing in a modern, secure digital network are as numerous as they are varied.

Between them, however, they all share a common theme: the digital world will not wait for those who sit on the fence.

Customer experience:
Every second is critical when customers are online, and having your site run slow – or worse – go down, can drive thousands of customers to a competitor so it's crucial your network is always performing optimally. By optimising applications in the branch, bandwidth to remote locations and IoT devices can be dramatically increased, improving customer experience.

Business insights:
Through data analytics you have the ability to know what your customer wants before they step through your door or visit your website. Maximise profits and operational efficiencies by tracking where your customers and employees spend most their time in both your physical and online store. Leverage your customer data to create new products and solutions to attract new customers.

Security:
A single cyber breach can cost your company millions. A secure network edge will provide you with a strong first line of defence leading to less downtime, improved employee productivity, and the confidence to roll out new innovative products and services.

Automation:
With IoT set to create 50 billion endpoints by 2020, manually tracking the devices and users on your network edge is no longer plausible. Investing in an automated IT system that can monitor, control, permit and contain devices and users will be key.

Agility and innovation:
Digital businesses thrive on agility. A modern, secure digital network allows your staff to spend less time on operational tasks and frees them up to work together on innovative new products and services no matter their location – be that from home, their office or in transit.

Cost reduction and revenue generation:
The value to be gained from a digital network isn't just significant – it could make or break your business. On average, organisations add AUD$16.25 million in new revenue and reduce costs by AUD$5 million – totalling AUD$21.25 million.

With the digital age well and truly upon us, it's time to get the jump on your competitors before they do.

The temptation to sit on the fence and wait until you are ready will seem an attractive option for some companies. Others who look to cut corners, and budgets, will be forced to play expensive catch up in the next few years when their ailing systems need upgrading. Those who understand the value of their network to their business success will act now to move to a digital network.

Act now and be ahead of your competition. Drive digital transformation in your organisation.


CISCO
Learn more about Cisco's DNA.
www.cisco.com
How digital-ready is your network?
Take this IDC assessment.