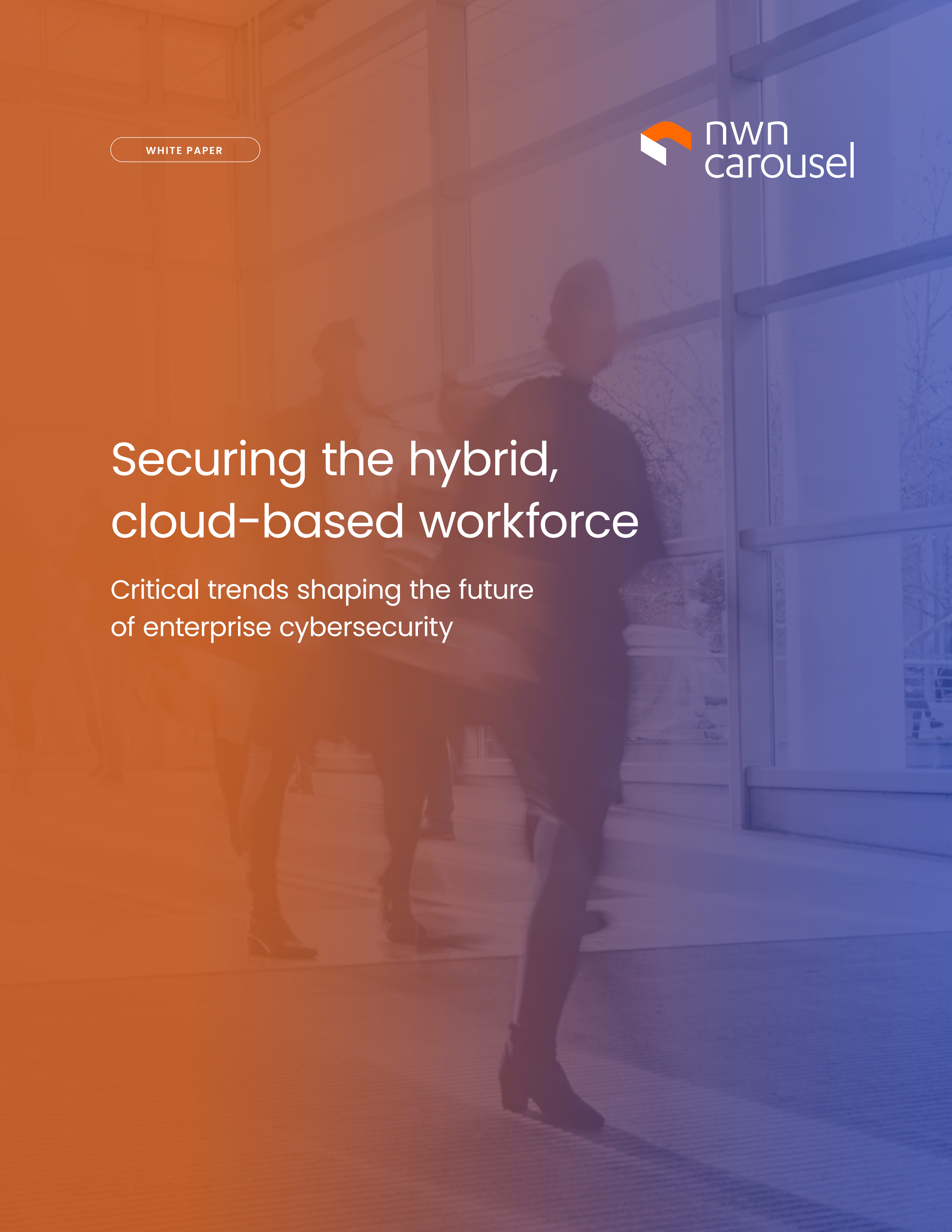

WHITE PAPER

nwn carousel

Securing the hybrid, cloud-based workforce

Critical trends shaping the future of enterprise cybersecurity

CONTENTS

Introduction

Today, 58% of organizations encourage a hybrid work model, and rely on cloud-based applications and infrastructure to drive productivity. While new ways of working and cloud-based systems provide more flexibility for employers and employees alike, they also pose new security challenges.

First, it's become increasingly difficult to protect communications across the typical organization's architecture and ensure compliance with security regulations. Nearly half of all data breaches in 2022 happened in the cloud. Organizations that fail to implement cloud security best practices put themselves at risk.

Second, each work style in a hybrid workforce has varying security needs. A road warrior or home office worker may need to increase their security posture compared to an in-office employee, based on their disparate connectivity options and the security threats that could potentially lie within.

In short, security can no longer be tied to a network perimeter. The old way of thinking was that anything inside the corporate network could be trusted. With bring-your-own-device (BYOD) policies, hybrid work, cloud adoption, and increased collaboration, trust is no longer implicit. As a result, zero trust security models are on the rise. A zero trust model considers all resources as external, and continuously verifies trust before granting only the required access.

The concept of zero trust ties into some of the biggest cybersecurity trends for the modern enterprise, including:

- **Identity** is the new perimeter
- **The cybersecurity talent shortage** is real, transforming the role of security
- **Human error** remains the single biggest threat
- **AI** will scale enterprise security capabilities

Identity is the new perimeter

What's happening

Gartner recently defined identity-first security as a top cybersecurity and risk trend to watch. While this trend is not new, with the rise of hybrid work and cloud computing, it's more important than ever. Attackers often target identity and access management (IAM) systems to gain silent access to systems. From there, they can move laterally through a system, abusing access privileges to compromise even the most sensitive data.

While many enterprises have tried simple methods like multi-factor authentication (MFA) to address these issues, securing the identity perimeter requires a more comprehensive approach.

In a zero trust model, security teams must:

Establish trust by verifying:

- User and device identity
- Device posture and vulnerabilities
- Any workloads
- Application and service trust
- Any indicators of compromise

Apply the principle of least privilege to:

- Cloud and network resources, including Infrastructure as Code (IaC)
- Applications
- Workload communications
- All workload users and administrators

Continuously monitor security posture by:

- Identifying risky or anomalous behavior
- Re-verifying trust levels following a breach
- Verifying traffic is legitimate, and not coming from threat actors

What enterprises can do

A zero trust security model can help teams gain more visibility into users, devices, containers, networks, and applications by verifying their security states across all access requests. By applying the principle of least privilege, teams can reduce the attack surface and make it harder for bad actors to take advantage of potential weak links. This model still allows employees to use the tools and applications they need, without opening up the organization to unnecessary risk.

The cybersecurity talent shortage is real

What's happening

According to statistics from Cybersecurity Ventures, there are more than 700,000 open cybersecurity jobs in the U.S. alone. It may seem optimistic that the global cybersecurity workforce has reached an all-time high, with roughly 4.7 million professionals. However, the 2022 (ISC)2 Cybersecurity Workforce Study shows there is still a major talent shortage of 3.4 million workers.

It's difficult to scale the cybersecurity workforce to meet the needs of this massive gap. As a result, the security role itself needs to evolve. In the past, cybersecurity teams owned enterprise perimeter security. In the modern threat landscape with bad actors doubling down on identity compromise, each and every user in the organization must be diligent. That means everyone "owns" security, and the cybersecurity team serves as an enabler, empowering users to understand their role in the modern enterprise security fabric.

What enterprises can do

To transition to a culture of shared responsibility, security teams must provide training and enablement to the entire organization, including:

Cybersecurity awareness training

One-third of employees feel that cybersecurity is not their responsibility, reinforcing the critical need for cybersecurity awareness training. A recent study from Kasepersky revealed that nearly 90% of employees need basic cybersecurity training, with only 11% of employees proving they had high levels of awareness in testing scenarios.

Clarity and consistency are crucial for cybersecurity awareness training, delivered in a format that any employee can understand. Human error is still the top cause of cybersecurity breaches (we'll cover more on that later). With security's help, employees can understand how to safely manage passwords and accounts, email, web browsing and applications, and avoid other common security traps arising from bad actors.

Secure coding training

In many organizations, shipping software quickly comes at the detriment of security. Shockingly, 48% of developers knowingly ship code with vulnerabilities. It's no wonder, because security courses are not included in many U.S. computer science education degree programs.

To remedy this skills gap, developers, database administrators (DBAs), and server administrators must be trained on secure coding best practices (standards organization OWASP is one great resource). As more and more enterprises become software companies, it's a must to ship secure applications, and keep open source dependencies up to date.

Ongoing enablement

Above all else, security should be seen as a positive, proactive function, rather than a punitive one. Many employees under-report security incidents, either because they fear losing their jobs or are unaware of reporting protocols. To solve this problem, security teams should have an open-door policy and encourage employees to be forthcoming, even if they think they've made a mistake.

What's more, learning about security should be continuous, rather than a once- or twice-a-year event. Ongoing enablement is central to establishing a culture of accountability across the entire organization.

Human error remains the single biggest threat

What's happening

According to SANS Institute, the top three attack vectors in 2022 continue to come from human error. Those include:

- **Phishing attacks**, when bad actors attempt to trick users into doing something nefarious, like downloading malware or clicking bad links via email.
- **Business email compromise** (BEC), a close cousin of phishing where attackers pretend to be someone legitimate, such as a C-level executive, trusted vendor, or partner, to gain access to corporate email accounts.
- **Ransomware**, or a form of malware that renders employee files or systems unusable until the company pays a ransom to the attacker.

Simple things, like weak passwords, cause many of these issues. Hackers guessed 18 out of 20 of the most common passwords of 2022 in under one second. More complex scenarios, like low-code/no-code citizen development, could lead to a major data breach in 2023, according to Forrester.

What enterprises can do

As stated in the previous section, one of the best employee risk mitigation strategies is cybersecurity awareness training. Paired with training and enablement, it's important to ensure that both remote and in-office employees are as secure as they can be.

As much as security professionals may not like it, many employees will continue to use easy-to-remember, yet weak, passwords. One solution is to embrace passwordless authentication. Traditional MFA relies on something the employee has, like a mobile device, and something they know, like a password.

To contrast, a passwordless login still uses something employees have, but it replaces the password with something they are, like a biometric (such as a fingerprint or facial identification). By using passwordless multifactor technology, organizations can leverage their existing identity provider (such as Active Directory) to authenticate users.

Another way to mitigate risk is to standardize infrastructure configurations. Many organizations may be working with new or inexperienced talent but can leverage tools that notify employees of configuration mistakes. Even best-practices like IaC can propagate errors if not done well. Many large and high-profile security breaches have occurred through misconfiguration issues, such as exposed secrets within open Amazon S3 buckets.

How CCSPs provide security solutions for the modern workforce

Cloud communications are internet-based voice and data communications. The telecommunications applications and switching are hosted by a third party outside of the organization and accessed through public internet connections. A Cloud Communications Service Provider (CSSP) leverages the cloud for faster delivery of secure telecom services to organizations.

CCSPs help organizations establish a proactive security posture that meets the needs of everyone — from road warriors to home office workers to those in the office. They achieve these goals with integrated offerings, services, and self-service analytics. Mainly, security for hybrid work use cases starts with standard secure internet connectivity, regularly updated endpoint devices regardless of location, and for Home Office Workers, adopting a Secure Access Service Edge (SASE) framework to secure the home networks.

With this groundwork, organizations can quickly respond to any threats, protect internal and external communications, and meet compliance regulations. Using an integrated administration platform, organizations gain a unified view into the entire cloud communications infrastructure with advanced security analytics, reporting, and proactive alerts.

The bottom line: To improve their secure posture, organizations must have visibility into their integrated environments so they can consistently analyze performance metrics and spot any security gaps that may exist.

AI will scale enterprise security capabilities

What's happening

Often, when an anomaly happens in an enterprise environment, it manifests itself in micro ways that security professionals can't detect with the naked eye. Considering the talent shortage, picking up on every threat becomes an even bigger challenge.

To strengthen their cybersecurity defenses, 93% of IT executives already use or are considering implementing AI and machine learning. Of those, 64% have leveraged AI for at least one of their security lifecycle processes. For example, many financial services firms like Capital One already use machine learning to flag issues such as credit card fraud. They're applying similar home-grown and open source machine learning models to detect cybersecurity anomalies.

What enterprises can do

Cybersecurity teams can leverage threat intelligence resources to understand security events and occurrences happening around the world. These solutions report on disclosed vulnerabilities and zero day threats that haven't been seen before. Teams can cross-reference and correlate different conditions or events across their own infrastructure and technology stack.

In addition, more than one-third of enterprises are using AI for endpoint discovery and asset management. This discipline is called Cyber Asset Attack Surface Management, or CAASM.

Using CAASM, Gartner predicts by 2026, 20% of companies will have more than 95% visibility into all of their assets, a dramatic increase from less than 1% in 2022.

Another popular use case for AI is automated threat response, or automating the action taken to respond to threats across the network. These technologies identify not only attack vectors, but also false positives, saving security professionals much-needed time.

Fortunately, through AI, trillions of actions can be boiled down to something meaningful on an individual level.

How NWN Carousel secures the modern enterprise

NWN Carousel is a CSSP that takes a platform-based approach to architecture design, with security tightly integrated into every aspect of the IT infrastructure. Through consolidation of operations and integrated analytics via NWN Carousel's Experience Management Platform (EMP), organizations can improve their existing security footprint, increase efficiencies, and evolve to an improved security posture.

NWN Carousel helps enterprises move from a reactive to a proactive security posture, with integrated offerings, services and self-service analytics so teams can respond faster to security threats. With NWN Carousel, teams can:

- **Design and Implement**: Establish the right platform-based security architecture to align with the organization's cybersecurity strategy.
- **Monitor**: Monitor for threats, while also monitoring the overall health of the organization's security infrastructure.
- **Operate**: Provide resources and solutions to manage the organization's security infrastructure in alignment with recommended best practices.
- **Respond**: Provide real-time remediation services in response to identified security threats, aligned with the organization's defined incident response program.
- **Analyze**: Gain control and visibility into the organization's environment with advanced analytics, real-time insights, service desk capabilities, and proactive alerts as a single source of truth.

> "NWN Carousel helped Foxwoods Resorts Casino implement a cloud security strategy to reduce risk from increasingly sophisticated, modern-day cyber threats."
>
> **Mike McCann**, Network Manager, Information Services, Foxwoods Resorts Casino

Leveraging NWN Carousel's security portfolio, customers can:

- **See more** via telemetry
- **Anticipate** what's next with actionable insights
- **Prioritize** actions through risk-based and continuous trust assessments
- **Close** the gaps within APIs and/or integrations
- **Simplify** the SecOps experience through optimization and automation tools

NWN Carousel powers the modern enterprise, embracing hybrid work, cloud infrastructure, SaaS applications, and more. As a result, teams can securely work with the tools they need to improve operational efficiency and productivity, with predictable costs. Security and compliance teams can rest assured that NWN Carousel manages business risk, minimizes disruption, and meets their compliance obligations — all while delivering a world-class customer and end-user experience.