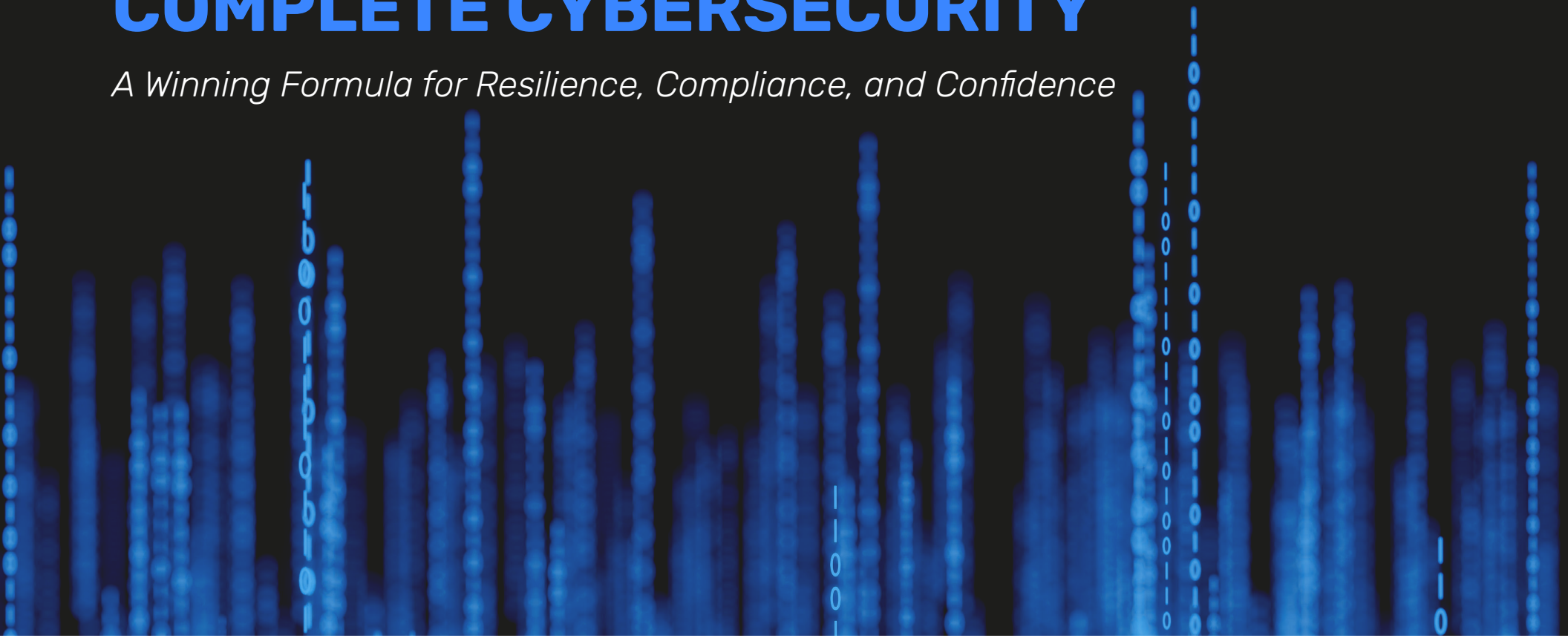
NOPALCYBER

OFFENSE + DEFENSE = COMPLETE CYBERSECURITY

A Winning Formula for Resilience, Compliance, and Confidence



info@nopalcyber.com | 917.512.4489

www.nopalcyber.com

The Changing State of Cybersecurity

Every organization on earth, regardless of size, location, or sector, wants the same thing in terms of cybersecurity: a strategy that works. Unfortunately, what worked in the past is no longer effective.

Today's hackers have powerful financial motives and, in some cases, bottomless government resources backing them, leading to an alarming intensification of cyber attacks. Those attacks are now more frequent, sophisticated, and ruthless than ever, targeting anyone and everyone while causing immediate and lasting damage to revenue, reputation, and regulatory standing. No other risk puts strategic plans in jeopardy or compromises business outcomes to same extent as cyber attacks.

Stopping every attack has never been more important—but the defenders have a disadvantage.

With the rapid embrace of business technology, especially during and after the pandemic, the attack surface is growing as fast as the number of attacks against it. Cyber compliance requirements are rising too. What isn't keeping up is the size of security teams, stacks, and budgets, leaving many companies under-equipped to protect their mission-critical digital assets and exposed to cyber attacks and compliance violations as a result. The situation can seem hopeless, especially for SMBs without the ample resources of their enterprise peers. But it's not.

Our ebook outlines the solution: offensive and defensive tactics working in unison to create a holistic cybersecurity strategy. Learn why this potent combination works so well, especially in today's and tomorrow's challenging digital landscape. Then explore how to put synchronized offensive and defensive security activities in place at ANY organization without burning out the security team or inflating the budget, and likely saving money in the long run.

A Snapshot of Cybersecurity

$4.45
million
in average data breach costs in 2023
Source

$8
trillion
in global cyber crime costs in 2023
Source

50%
of all SMEs
struggled with a cyber incident last year
Source

153%
increase
in ransomware attacks since 2022
Source

Defensive Cybersecurity Explained

Most people associate cybersecurity with defensive tactics: preventing an attacker from accomplishing their objective. That happens by detecting inbound attacks, slowing and stopping their advance, preventing any damage they could cause, and removing the threat, followed by an effort to keep a repeat attack from happening.

Defensive cybersecurity encompasses many tools and techniques, from using extended detection and response (XDR) tools for flagging threats to monitoring threat intelligence for clues about probable attacks. It locates attacks no matter how evasive or persistent they are or which attack vectors they target. Then, strong defense neutralizes the threat, remediates any damage, and eliminates the attack pathway. When done well, defense stops attacks before they steal any data, damage any systems, violate any regulation, or have any consequences whatsoever. It's the difference between a stable, scalable, and successful business versus one facing constant disasters that emerge from IT and spread outwards.

Defensive cybersecurity becomes even more important as business technology gets more expansive, complicated, and threatened—but these same factors make fighting off every attack from every angle a growing challenge.

It takes abundant resources to stay on guard 24/7/365, including tools and skills that may be missing. Defensive cybersecurity is only half the battle, though. Focusing exclusively or primarily on defense does the opposite of what anyone wants: it makes cybersecurity harder and cyber risks greater by neglecting the other half of the battle.

Examples of Defensive Cybersecurity

Managed Detection & Response

Identify & arrest inbound threats.

User and Entity Behavioral Analytics

Monitor & alert for anomalies.

Endpoint Detection & Response

Find & confront endpoint threats.

Network Traffic Analysis

Flag suspicious network activities.

Security Orchestration, Automation, & Response

Automate security essentials.

Offensive Cybersecurity Explained

Offensive cybersecurity tactics are typically associated with attackers. Bad actors will probe IT environments for weaknesses, exposures, misconfigurations, or any other issue that would make it harder to stop or detect inbound attacks. Offensive cybersecurity uses these same tactics for the purposes of good.

With techniques like penetration testing and breach and attack simulations, offensive cybersecurity discovers security issues, diagnoses the fix, and prioritizes the remediation plan. That way, security teams quickly and confidently resolve the worst issues first, shrinking the attack surface to disrupt inbound attacks upon arrival.

Using the attackers own tactics against them makes for powerful, preventative cybersecurity, but doing so takes no small amount of time, experience, and expertise, usually greater than what small and midsize businesses have available.

Cybersecurity isn't complete without going on the offensive, and businesses remain at risk until they do, so adding it to the cybersecurity strategy needs to be a top priority. But it doesn't stop there. Just as important as making a serious and sustained commitment to offensive cybersecurity is balancing it with defensive cybersecurity. Together, they form a sum stronger than the two parts.

Examples of Offensive Cybersecurity

Penetration Testing

Locate weaknesses across the attack surface.

Breach and Attack Simulations

Learn how security responds under attack.

Ransomware Resilience Testing

Simulate a top threat for training.

Vulnerability Scanning

Look for known vulnerabilities & exposures.

Threat Intelligence Tracking

Stay aware of new & evolving threats.

How Offense and Defense Work Together

In today's dynamic and high-stakes cybersecurity landscape, where preventing attacks immediately, completely, and consistently is mandatory for a business's growth and stability, security teams have to fight on two fronts at once. Offense and defense tactics working together is the surest way to achieve cyber resilience and all the benefits that come with it, from fewer business interruptions to better customer/investor relationships to faster compliance with current and future regulations.

By shrinking the attack surface (offense) while fortifying the perimeter (defense) companies become exceedingly hard to hack because these tactics complement one another. Offensive cybersecurity reduces the volume and strength of attacks that security teams have to defend against, freeing up more resources to stop those attacks that don't automatically fail. Defensive cybersecurity, in turn, reduces the pressure to anticipate every issue on offense, which would be impossible.

The fact that offense and defense are a potent combination comes as no revelation. Cybersecurity teams often use red team vs. blue team exercises to understand what happens when offense and defense intersect. Much less common is for security teams to simultaneously emphasize offense and defense all the time—until now.

What companies must do on cybersecurity is changing fast. Fortunately, what they can do is changing, too.

Making Complete Cybersecurity Accessible to All

Cybersecurity that plays offense and defense at the same time poses a formidable challenge to attackers...but it does the same to in-house security teams. For many, complete cybersecurity means adding some capabilities on the defensive side, many more on the offensive side, and learning how to operate both sides in perfect sync from now onward. The time, skills, budget, and commitment required are difficult for any organization to shoulder, leaving many with incomplete cybersecurity as a result.

Cybersecurity partners solve this problem by supplementing in-house security resources with whatever skills, tools, and talent may be missing. Partners take what's there and add the offensive and defensive capabilities necessary for cybersecurity to become practical and powerful.

Relying on a third-party rather than extending in-house capabilities makes more sense for all but the very biggest enterprises. Cybersecurity partners provide a faster and less expensive path to comparable cybersecurity, especially as ongoing talent and skills shortages make hiring prohibitive.

A partner skilled in offense and defense and equipped to take the lead on both, all day every day, makes complete cybersecurity accessible to all.

Cybersecurity partners offer what everyone wants— a strategy that works—with one major caveat: only the right partners actually deliver, making the choice of who to partner with imperative yet risky. Confidence in a partner is key.

The Three Pillars of Cybersecurity

Effective cybersecurity means 360-degree coverage. NopalCyber delivers protection in every direction by combining the three pillars of cybersecurity:

Attack Surface Reduction

Our red team uses offensive tactics to find exposures and weaknesses in IT before attackers do.

Managed Extended Detection & Response

Our proprietary technology uses telemetry from multiple sources to see and stop incoming attacks with powerful defensive measures.

Advisory Services

Our cybersecurity experts are available to answer questions, help plan, provide assistance, or fill in wherever cybersecurity needs backup.

NopalCyber – Combining Offense + Defense for 360° Protection

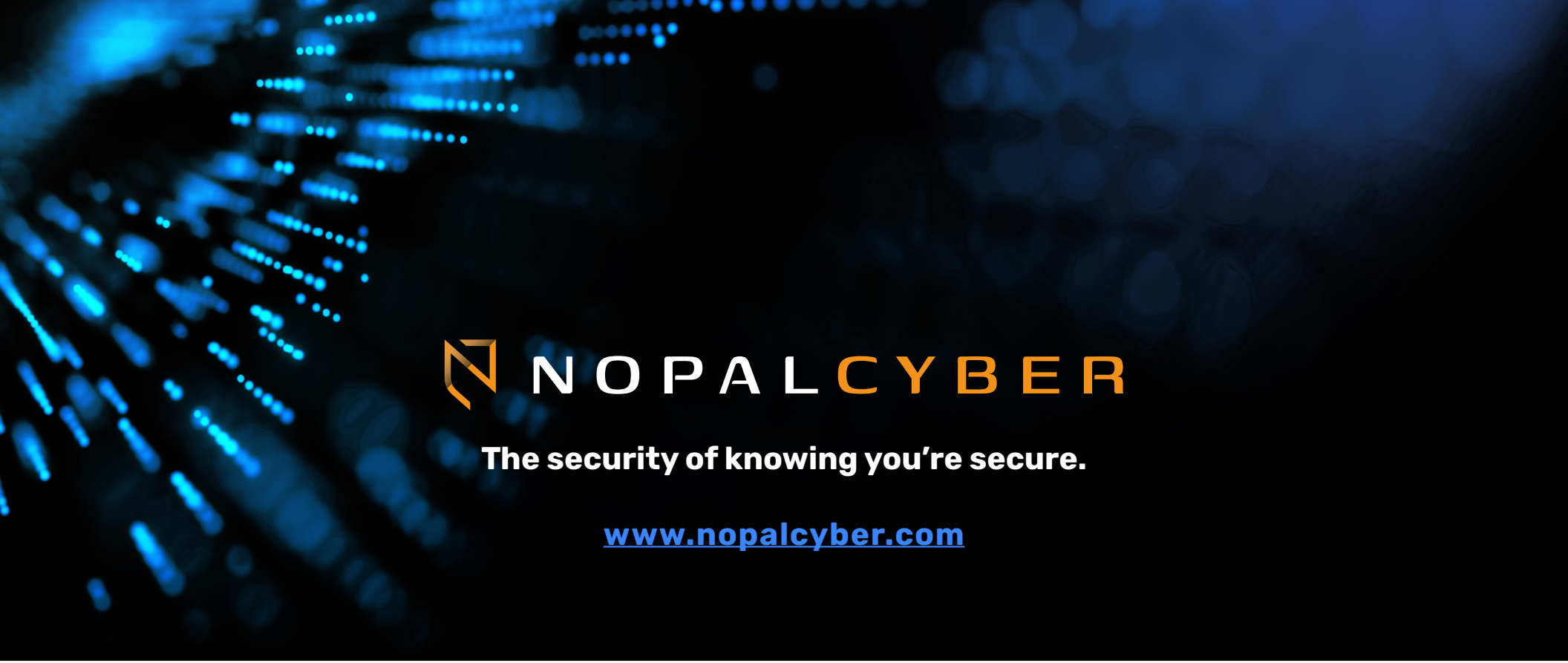
NopalCyber was founded to democratize cybersecurity by helping every business practice enterprise-level cybersecurity. We do that by integrating offensive and defensive tools onto one platform that fends off attacks from the outside in and inside out.

Nopal360° is the platform that fends off attacks from the outside in and the inside out.

Our platform, Nopal360°, serves as the hub for all cybersecurity activities, offering different configurations of tools and services tailored to your specific security needs and business objectives. The platform provides the visibility to play offense and defense simultaneously, while the NopalCyber team provides the expertise and assistance to be a force on both sides. Our app, NopalGO, gives you visibility into all your security tools and data from anywhere, plus a constant communications link with our experts for any time when questions, issues, or emergencies arise.

Competitive price points and white glove service at all levels make NopalCyber a viable partner for any company. And with a complete yet bespoke solution to offer, NopalCyber is a powerful complement to any security team, and a boost to any business eager to make success more certain.

No matter what's missing on offensive, defense, or cybersecurity overall, NopalCyber makes it whole. Take what you have and instantly make it complete to feel true confidence in cybersecurity.



About NopalCyber

NopalCyber makes cybersecurity manageable, affordable, reliable, and powerful for companies that need to be resilient and compliant. Managed extended detection and response (MXDR), attack surface management (ASM), breach and attack simulation (BAS), and advisory services fortify your cybersecurity across both offense and defense. AI-driven intelligence in our Nopal360° platform, our NopalGO mobile app, and our proprietary Cyber Intelligence Quotient (CIQ) lets anyone quantify, track, and visualize their cybersecurity posture in real-time. Our service packages, which are each tailored to a client's unique needs, combined with external threat analysis, which provides critical preventative intelligence, helps to democratize cybersecurity by making enterprise-grade defenses and security operations available to organizations of all sizes. NopalCyber lowers the barrier to entry while raising the bar for security and service.

info@nopalcyber.com

www.nopalcyber.com