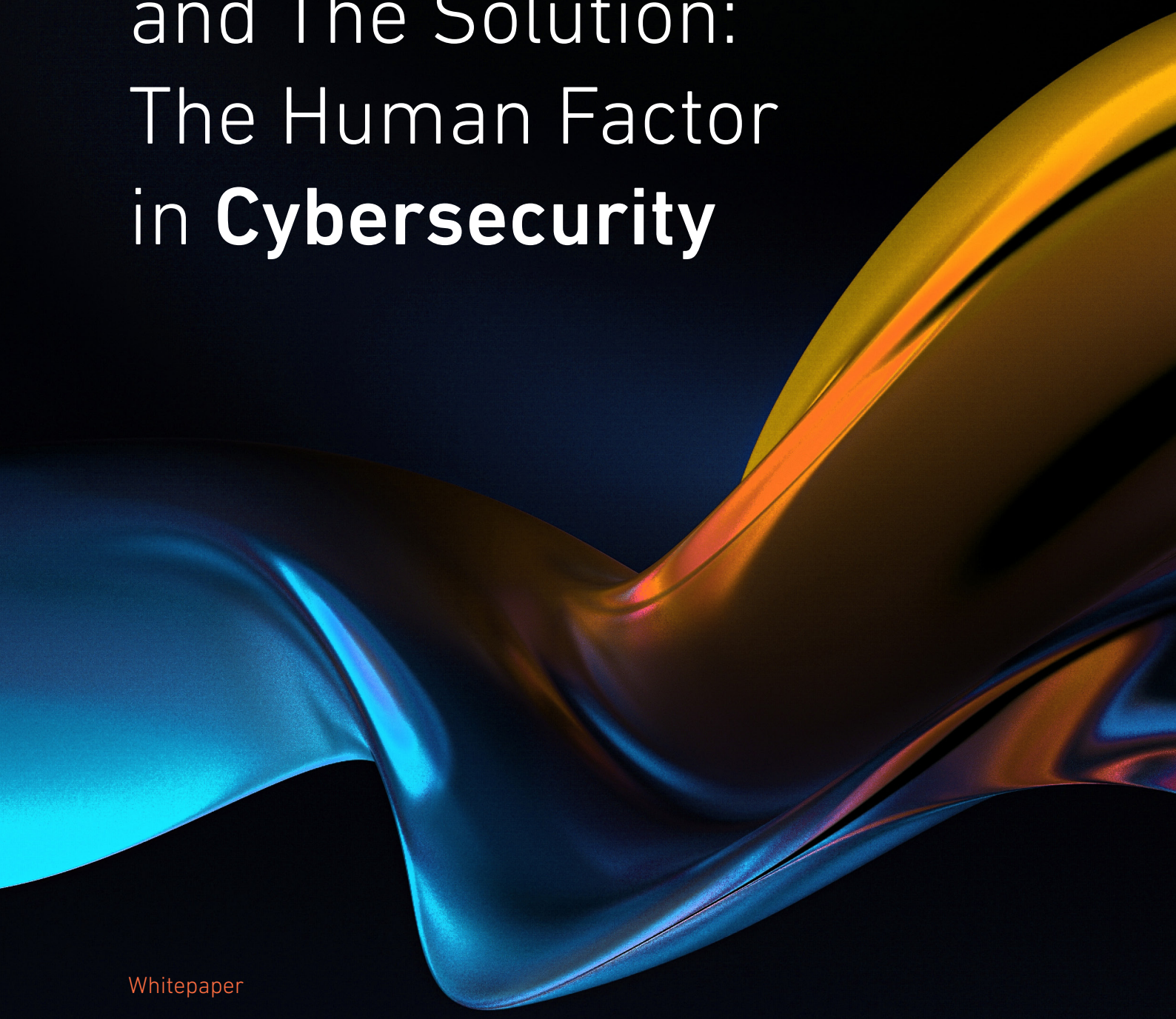
SONICWALL®

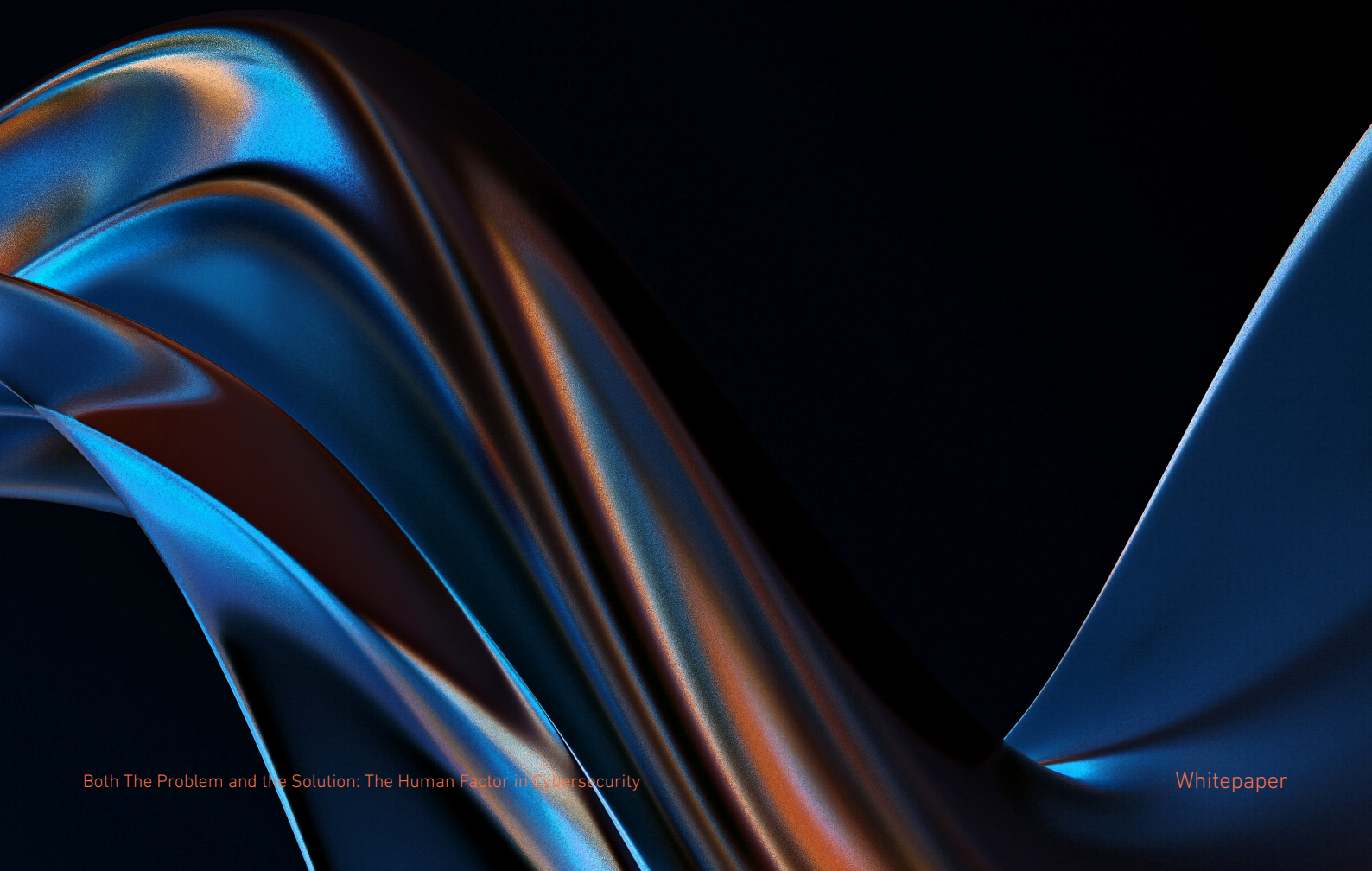
SONICSENTRY

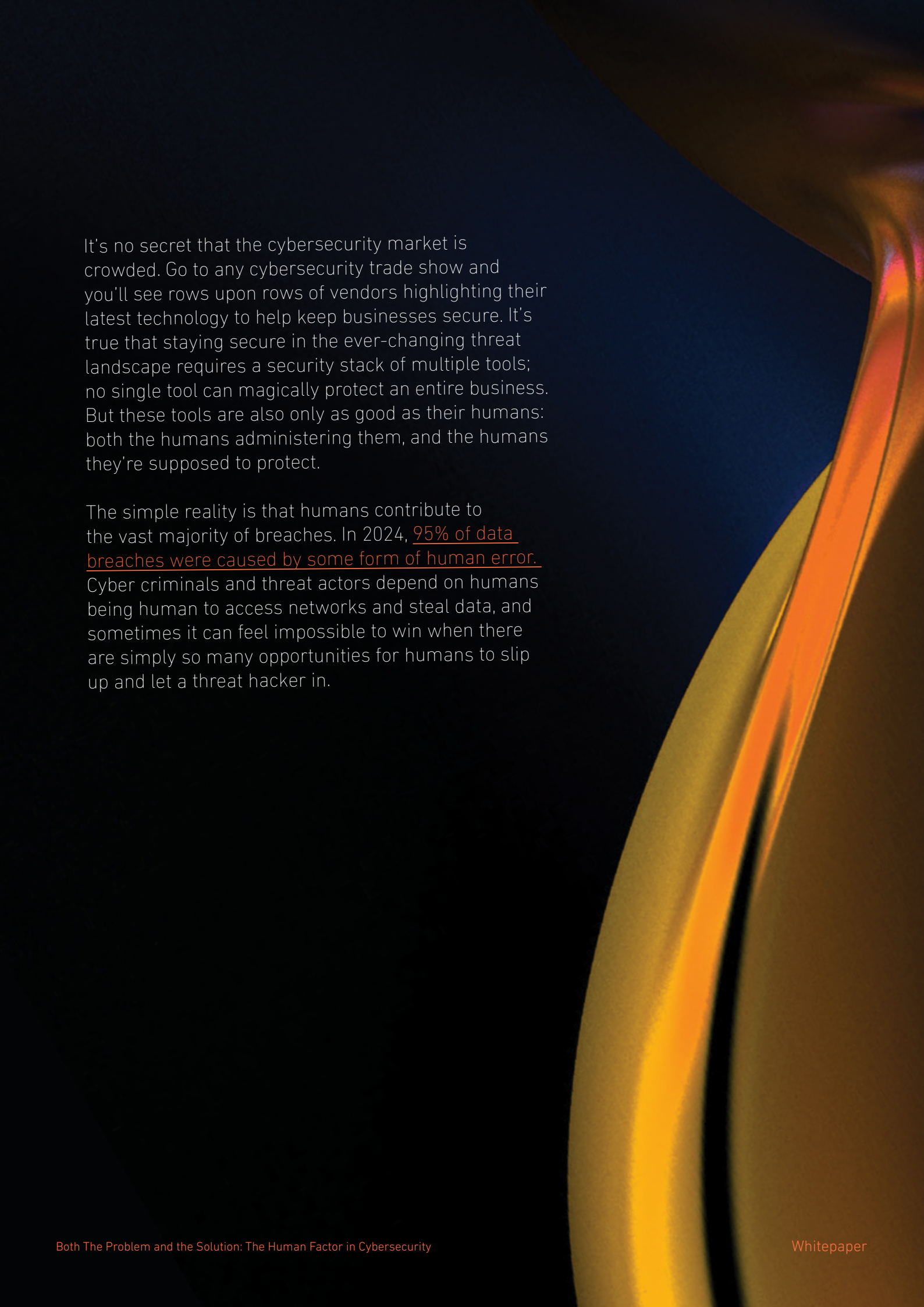
Both The Problem and The Solution: The Human Factor in **Cybersecurity**



Whitepaper

CONTENTS





It's no secret that the cybersecurity market is crowded. Go to any cybersecurity trade show and you'll see rows upon rows of vendors highlighting their latest technology to help keep businesses secure. It's true that staying secure in the ever-changing threat landscape requires a security stack of multiple tools; no single tool can magically protect an entire business. But these tools are also only as good as their humans: both the humans administering them, and the humans they're supposed to protect.

The simple reality is that humans contribute to the vast majority of breaches. In 2024, 95% of data breaches were caused by some form of human error. Cyber criminals and threat actors depend on humans being human to access networks and steal data, and sometimes it can feel impossible to win when there are simply so many opportunities for humans to slip up and let a threat hacker in.

1 Does Something Smell Phishy?

We've all had those emails come through: obviously sketchy messages, dangling love, money, or nearly anything else we might want, easily available by just clicking this link. But phishing emails aren't always so obvious: they frequently impersonate reputable companies or people we know to trick us. With more of our working and personal lives living in the cloud these days, spoofed emails from cloud providers are also often fertile ground for phishing. Those links they include are anything but helpful; they can do a myriad of things once they're clicked, including downloading malware and allowing a threat actor to burrow into an environment to deploy a larger attack.

Phishing is the first thing that comes to mind for most people when thinking about cybersecurity, and rightfully so: according to CISA, up to 90% of cyber-attacks begin with a phishing email. Phishing goes beyond email, too, as phishing messages are now often sent via text message or social media, particularly highly targeted spear phishing messages purporting to be from executives or messages with job offers.

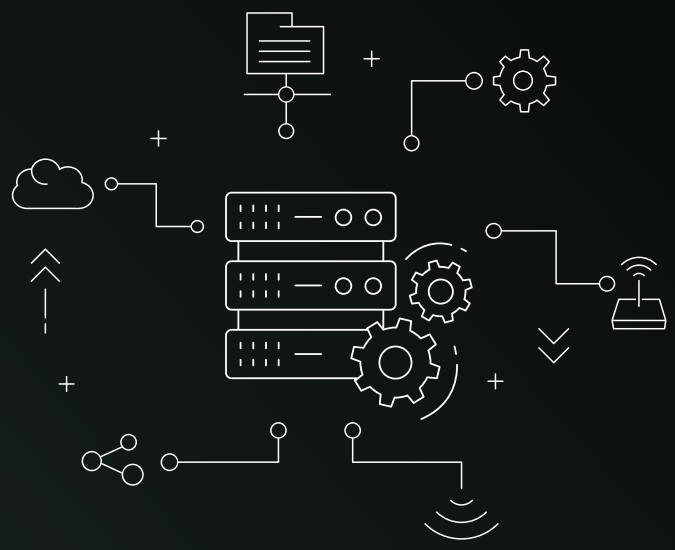
Constant vigilance is key to staying a step ahead of phishing and preventing larger cyber headaches. It's easy enough to do phishing training, helping employees look for obfuscated links, bad grammar or spelling, false urgency, and other markers of phishing, but that's not enough. Given the right combination of stress, confusion, and the right phishing email, anyone, even the smartest security professional, could fall for a phishing attack, and that's what attackers are counting on: they know their emails won't fool the vast majority of folks, but just enough people will click to make their efforts profitable.

2 Configuration is Crucial

From endpoint to cloud to perimeter, it takes more than one tool to defend a business these days. Firewalls are used on networks to control and secure network traffic. Next-generation antivirus with endpoint detection and response (EDR) features are used to protect laptops and other devices. On top of these, other tools may come into play depending on the industry and the needs of the business.

All these security tools have one thing in common: they need frequent configuration updates. The fact that tools need updates isn't a reflection on the quality of the tools; the simple reality is that the threat landscape is ever evolving. As threat actors adjust their tactics and techniques, new vulnerabilities come to light, meaning firewalls need to be patched and endpoint tools need updated detection logic.

Configuration management isn't optional. According to Gartner, up to 60% of security breaches have misconfigured tools at their source, and according to the SonicWall Threat Report, hackers and threat actors take advantage of new vulnerabilities often within 48 hours.

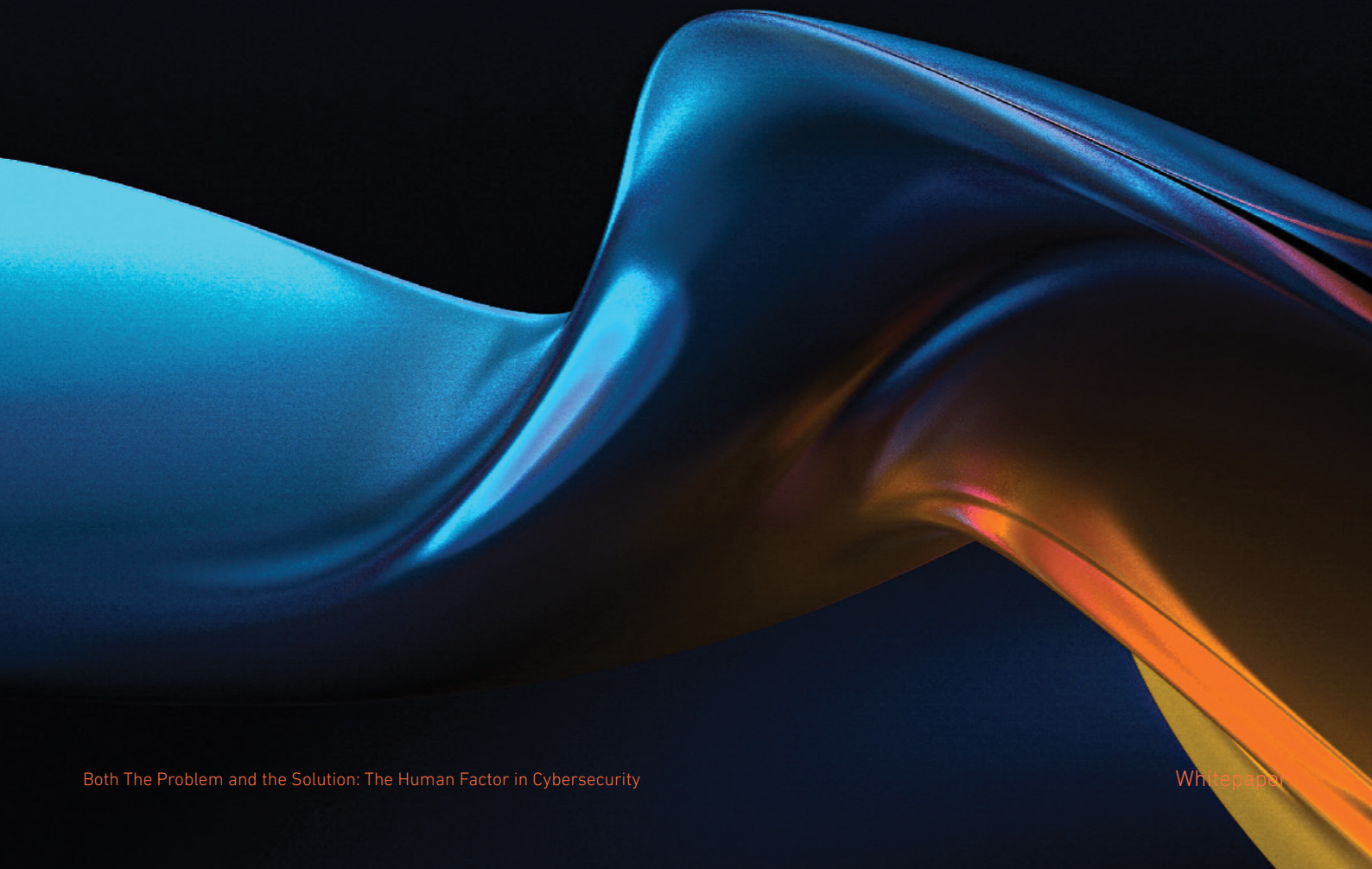


It takes consistent diligence to stay on top of new vulnerability patches and indicators of compromise (IoCs). Unfortunately, many human security teams struggle to keep up with these updates. They're never ending, leading many people to not just forget but, often, neglect them altogether. This neglect makes the job of the hacker even easier and opens businesses up to avoidable risk.

3 The Avalanche of Alerts

As noted above, properly securing an organization takes a full, properly configured security stack comprised of multiple tools. All of these tools send alerts; telling you what might need your attention is a key part of their job. However, many of these alerts may be false positives or otherwise not actionable; for example, macros activating in a Microsoft Office document could be totally expected and benign.

These alerts come frequently, and at all hours of the day and night. Sifting through them to determine what requires action and what doesn't can overwhelm even the most experienced security teams; finding the signal in the noise can be impossible. Because of the flood of alerts, small MSPs or other IT professionals trying to do this alone often drown in the sea of alerts, leaving alerts to fester for hours before they are dealt with. This gives the gift of extra dwell time to threat actors, and increased dwell time can take what was an annoying security alert and turn it into a major cyber incident.



4 Security is Annoying

Picture this: a gate on a road, but with clear tire tracks on either side, a sign of cars having gone around the gate. This image is often used in security textbooks for good reason. Humans are hardwired to seek the path of least resistance; when something is annoying, we frequently try to figure out a way around it. That applies to cybersecurity, too.

While it's true that security must be balanced with the needs of the business, many security controls that are viewed as cumbersome are not optional. Protocols like multi-factor authentication are a key step in securing cloud applications but may frustrate users. Even security admins sometimes choose to change policies and protocols to make their workflows more streamlined, or may forget to reinstate policies after temporarily disabling them. It's crucial to ensure these security tactics are enforced so that there isn't a way around them.

5 Humans: Both the Problem and the Solution

So, what's the solution to security's human problem? The answer might surprise you. The way to combat human error doesn't lie in more technology; instead, the answer is in more humans. Specifically, expert humans who are trained in cybersecurity and can provide backstops and additional controls for when humans make very human mistakes. Security is a team sport; adding more eyes to the problem helps spot issues faster and stop attacks before they cause major business harm.

For smaller companies and managed service providers, it might feel out of reach to bring in cybersecurity experts to help solve for these issues. Building a security operations center (SOC) from scratch can easily cost upwards of $1 million, which simply isn't possible for most companies. However, purchasing managed security services can help. Outsourcing things like firewall configuration and SOC services can help augment an existing IT team and provide additional peace of mind for businesses and MSPs alike.

6 Meet SonicSentry, SonicWall's Managed Security Services

SonicWall has an over 30 year history of supporting the cybersecurity needs of businesses large and small, as well as our MSP partners. Our SonicSentry team continues this legacy by delivering managed security services that take the security burden off of stretched-thin teams, providing monitoring and response across the attack surface. The SonicSentry team is made up of experts from our SOC analysts who actively threat hunt on behalf of our partners and customers, to our NOC team who ensures our customers' firewalls have the best, most up-to-date configuration.

Managed Protection Security Suite (MPSS) is SonicWall's fully-managed firewall service, delivered by SonicSentry. After the initial firewall configuration, the SonicSentry team fully manages enrolled firewalls, handling all patches, firmware updates, and configuration changes, allowing our partners' and customers' team to free up hours of analyst time while ensuring the firewall is always up to date with the best configuration. MPSS also provides monthly firewall health checks, showing you the threats the firewall has defended against, and weekly productivity reports, which show the top sites accessed on the network and flags anything that may be unproductive.

SonicSentry Managed XDR puts the power of the SonicSentry expert SOC behind endpoint, cloud, and network, providing 24/7 protection. The SOC leverages the latest threat intelligence with their years of experience to monitor alerts for you, notifying you of any that may be actionable, and stopping attacks in progress to minimize damage. On the endpoint, they provide twice monthly configuration audits, showing you anything that may need to be updated to give you the best security posture. For cloud, the SOC monitors and responds to suspicious admin activity as well as login attempts and other concerns, helping you ensure your necessary security controls aren't circumvented.

Ready to get started? Visit www.sonicwall.com today to learn more!