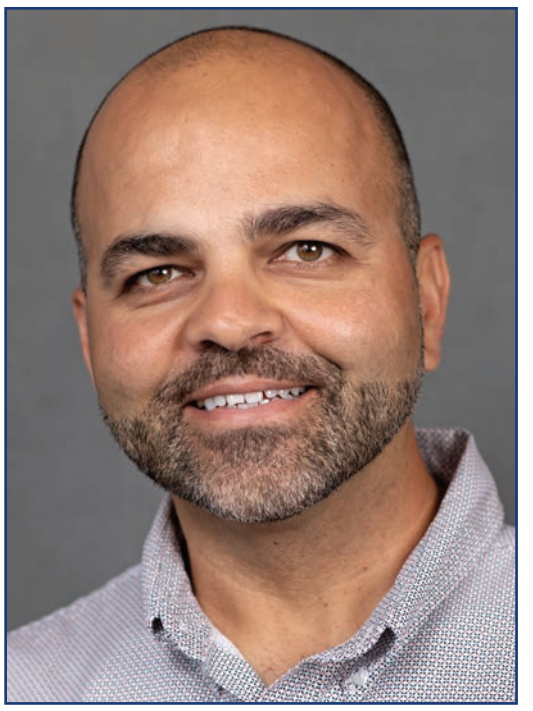
TECH, CYBERSECURITY & AI ROUNDTABLE

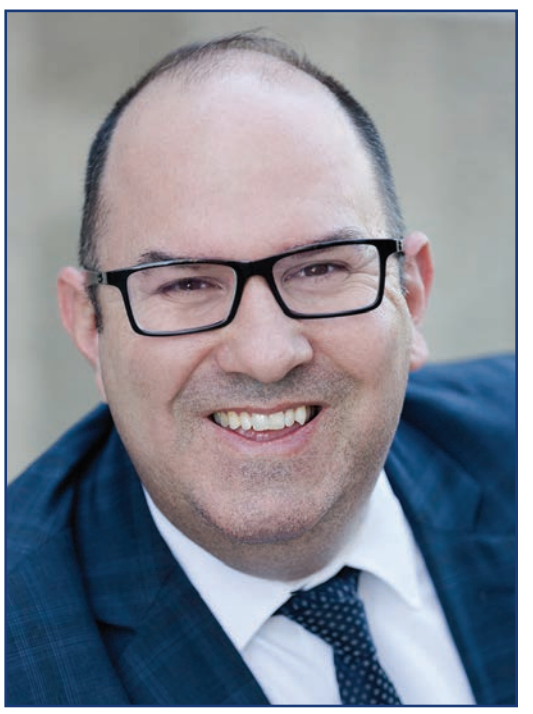
An Informative Q&A with OC's Top Tech, Cyber & AI Professionals

Jay Cann
Chief Technology Officer of Customer Experience
Synoptek



David Ellis
Founder
Productive IT Solutions

Julian Hamood
Founder & Chief Visionary Officer
Trusted Tech Team



Jeff Tutton
President
Intersec Worldwide, Inc.

TECH, CYBERSECURITY & AI

ROUNDTABLE PARTICIPANTS

Intersec Worldwide, Inc.
Intersec Worldwide, Inc. is nationally recognized as a cybersecurity and digital forensics / incident response firm headquartered in Newport Beach, California. Founded by California natives, Intersec has spent nearly two decades safeguarding some of the most prominent U.S. brands across industries including retail, hospitality, financial services, insurance, and technology.

As a full-service cybersecurity firm, Intersec specializes in rapid-deployment data breach incident response, remediation and compliance consulting, with a proven track record of helping organizations recover quickly and securely from cyberattacks and remain compliant with industry regulations.

Intersec's clients consist of some of the largest merchants and Fortune 100 companies in North America, and while NDAs prevent disclosure of most client names, you have likely shopped in their stores, visited their websites, and carried their cards in your wallet.

Intersec is also a certified PCI Forensic Investigator (PFI) and Qualified Security Assessor (QSA). The firm also works closely with law firms and insurance carriers to provide litigation-ready digital forensics.

Intersec's vendor-agnostic approach and deep bench of industry experts allow them to deliver customized, client-first solutions with unmatched speed and precision. Whether supporting Fortune 100 companies or growing enterprises, Intersec Worldwide remains committed to strengthening cybersecurity resilience from right here in Southern California.

Productive IT Solutions
Most IT companies wait for something to break. Productive IT Solutions prevents the breakdown altogether. Based in Southern California, this cybersecurity-forward MSP helps small and mid-sized businesses lock down their systems, secure their Microsoft 365 environments, and respond to threats in real time, before damage is done. Their secret? A proactive strategy that combines real human support with enterprise-grade tools like AI-powered threat detection, automated response, and backup solutions even Fortune 500s would envy. Business owners don't call Productive IT when they want a technician, they call when they want peace of mind, predictable operations, and a partner who treats their systems like mission-critical assets. Led by founder David Ellis, the company brings decades of experience, fast execution, and a relentless focus on protecting what matters most. It's not just IT support, it's digital armor for businesses that can't afford downtime.

Synoptek
Synoptek is a business and technology consulting firm that delivers accelerated business results through advisory-led, transformative full-life-cycle systems integration and managed services. We partner with organizations worldwide to help them navigate the ever-changing business and technology landscape, build solid foundations for their business, and achieve their business goals.

Our approach is exemplified by strategic foresight, enabling organizations to adapt, innovate, and thrive in dynamic environments, embrace change, and evolve to meet the demands of the digital age. Through our global network of experts and strategic technology alliances, we provide holistic solutions tailored to each client's unique needs.

By combining innovation with practical expertise, we help organizations unlock new opportunities, optimize performance, and safeguard their ecosystem. Our core values of growth, ownership, inclusivity, and philanthropy drive us to deliver exceptional results and unparalleled service to our valued stakeholders.

Trusted Tech Team
Trusted Tech Team is a leading Microsoft Cloud Solution Provider (CSP) specializing in Microsoft Cloud services, Microsoft perpetual licensing, and Microsoft Support Services for medium and enterprise-sized businesses. Distinguished as one of the select few Microsoft CSPs to earn all six Microsoft Solutions Partner Designations, their robust team of onshore Microsoft architects and engineers empowers IT leaders to navigate the complexities of security, AI, and IT infrastructure with ease. Prioritizing a people-centric mission, Trusted Tech Team has transformed the Microsoft software licensing experience, giving IT professionals complete confidence in the success of their Microsoft investment.

Harness the Power of AI for Smarter, Safer Business

Cyber threats don't wait—and neither should your response. As a premier technology services provider, Synoptek combines advanced cybersecurity with the power of AI to help you detect, respond, and adapt in real time. From cloud to endpoint, we safeguard your digital ecosystem with intelligent automation and continuous vigilance.

Our approach doesn't just protect your organization—it helps you evolve it. By integrating data, technology, and secure operations, we create a foundation for agility and future-performance.

Learn More

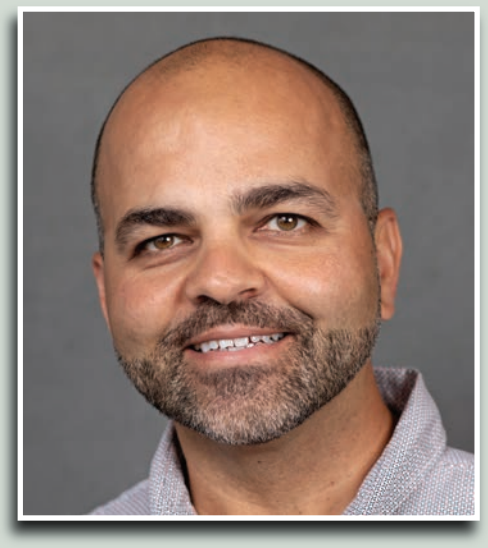
We Don't Just Secure IT.
We Power Confident, Intelligent Growth.

www.synoptek.com

TECH, CYBERSECURITY & AI ROUNDTABLE

Through machine learning and natural language processing, even non-technical staff can derive insights that once required expert analysts.

Julian Hamood
Founder &
Chief Visionary Officer
Trusted Tech Team



AI helps businesses stay safer from cyber threats by acting like a super-watchdog that never sleeps.

David Ellis
Founder
Productive IT Solutions

How can AI improve threat detection and incident response?

Jay Cann, Synoptek: Synoptek leverages AI to enhance threat detection by analyzing large datasets, identifying patterns, and detecting anomalies in real time, well beyond human capabilities. Machine learning models predict and prioritize threats, reducing false positives. For incident response, AI can automate containment, mitigation, and recovery processes, speeding up reaction times, though with human oversight. It also integrates with SIEM systems to provide actionable insights, enabling proactive defense.

Julian Hamood, Trusted Tech Team: In a modern SOC (Security Operations Center), AI enables us to analyze massive volumes of log and telemetry data across fragmented systems and solution stacks. Through machine learning and natural language processing, even non-technical staff can derive insights that once required expert analysts. It's about supercharging our workforce and helping one analyst do the work of three by eliminating manual tasks and surfacing actionable threats faster. This drives greater operational efficiency and enables organizations to reallocate resources toward their highest priorities. In addition, it's important to remember that AI is transforming how organizations manage detection and response by serving as intelligent investigators, not a human replacement.

David Ellis, Productive IT Solutions: AI helps businesses stay safer from cyber threats by acting like a super-watchdog that never sleeps. It keeps an eye on all the activity happening across a company's computer systems, like who's logging in, what files are being opened, and whether any strange connections are popping up.

Instead of waiting for a human to notice something's wrong, AI learns what "normal" looks like and instantly spots anything that seems off. That means it can catch suspicious behavior early, sometimes even before a real attack happens.

Because it can handle huge amounts of data and work around the clock, AI finds problems faster and more reliably than people alone ever could.

Jeff Tutton, Intersec Worldwide, Inc.: At Intersec Worldwide, we utilize AI to enhance our threat detection and incident response capabilities. AI allows our DFIR experts to process massive datasets in real-time and spot anomalies like unusual network patterns with pinpoint accuracy. AI learns from past incidents and enables proactive defenses, such as instantly providing rollback capabilities of ransomware/malware, isolating systems or blocking traffic to minimize damage. It also cuts through alert fatigue and prioritizes critical issues so our team can focus where it matters. By automating routine tasks, AI reduces human error and ensures swift, expert-level handling of threats. AI empowers our experts to review and act on large datasets faster, using smarter tools that better inform decision-making and response time.

Do you have clear policies on the ethical use of AI in defense/offense in cybersecurity?

Julian Hamood, Trusted Tech Team: Absolutely. We have clearly defined policies guiding the ethical use of AI, rooted in transparency, defense-only applications, and alignment with regulatory compliance standards. Our principles reflect a defense-prioritized posture, using AI to strengthen protection, detect vulnerabilities, and train users. As AI capabilities evolve, so will our framework to ensure we lead responsibly and ethically.

David Ellis, Productive IT Solutions: Yes, and it's something we believe every company should take seriously. AI should be used to protect people, not exploit them. That's why our focus is entirely on defense, not offense. We use AI to detect threats early, improve response times, and support secure operations, not to launch attacks or invade privacy. Our systems are designed with human oversight in mind and follow trusted frameworks like the NIST AI Risk Management standards. We also regularly review our practices to make sure they align with ethical, legal, and community expectations. Bottom line: AI is a powerful tool, and it's our responsibility to use it carefully, transparently, and always with the goal of making people safer.

Jeff Tutton, Intersec Worldwide, Inc.: Yes, we've always believed ethical considerations are paramount when using AI in cybersecurity. Our policies ensure transparency, accountability, and responsible deployment across defense and offense strategies. With our client-centered approach, we avoid reckless AI applications and focus on integrity. These guidelines, shaped by our work with Fortune 100 companies and our internal audit and compliance requirements, balance AI's power with ethical limits, which is critical for maintaining credibility. As experts, we see clear policies as foundational to leveraging AI effectively without compromising principles.

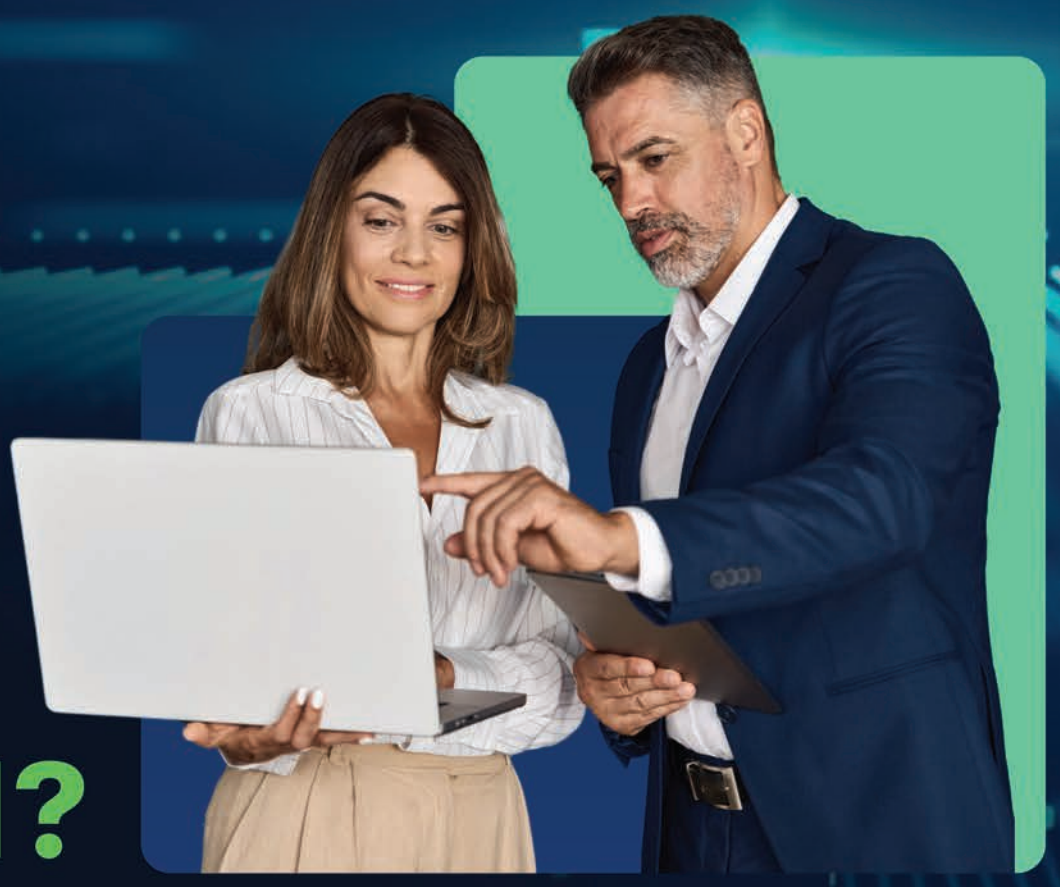
Jay Cann, Synoptek: We prioritize ethical AI use, adhering to strict guidelines ensuring transparency, accountability, and fairness. Policies prohibit offensive AI applications, focusing solely on defensive cybersecurity measures like threat detection and response. Human oversight ensures compliance with ethical standards, and regular audits reinforce responsible AI deployment.

How is AI being used to detect and respond to threats in real time?

David Ellis, Productive IT Solutions: AI works like a digital bodyguard that's always on duty. It watches for suspicious behavior across your systems, like an employee who normally logs in from California suddenly accessing files from another country at 3 a.m. Instead of waiting for someone to notice, AI immediately spots this red flag. It can send alerts, lock accounts, or isolate devices before any damage is done. Traditional systems rely on fixed rules, but today's attacks are more dynamic and harder to predict. AI learns your business's unique rhythms and reacts to

continued on page B-40

TRUSTED TECH TEAM



Is your business ready for AI?

Adopt AI With Confidence, Clarity, and Control

Microsoft Copilot is rapidly transforming how businesses work. But without the right foundation, AI adoption can be complex and risky. Misconfigured access, unindexed data, and poor governance don't just block productivity — they expose your organization to serious security and compliance issues.

As an IT leader, the path to AI readiness starts with you. **Trusted Tech Team's Readiness Assessment for Microsoft 365 Copilot** is a comprehensive, expert-led evaluation that empowers you and your staff with a clear, practical action plan for successful, cost-effective, meaningful Copilot adoption.

We've delivered tailored roadmaps to scores of organizations across the country, and with Microsoft-certified architects based right here in Orange County, we're ready to bring our expertise to your team and help you unlock the full potential of AI in Microsoft 365.

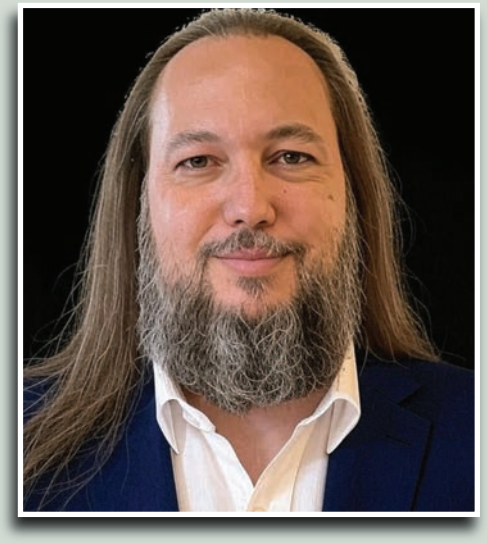
Take the Next Step Toward Copilot Readiness Today

TRUSTED TECH TEAM

Microsoft Solutions Partner
Microsoft Cloud

Call: (855) 545-0805
Email: proservices@TrustedTechTeam.com

TECH, CYBERSECURITY & AI ROUNDTABLE



Training emphasizes collaboration with AI tools, reporting anomalies, and maintaining vigilance. Continuous updates on evolving threats ensure preparedness.

Jay Cann
Chief Technology Officer of Customer Experience
Synoptek

anything that doesn't fit the pattern. That real-time action is a huge advantage, especially when even a few minutes of delay can make a big difference.

Jeff Tutton, Intersec Worldwide, Inc.: In our daily MDR operations, we leverage AI to stay ahead of threats in real-time. It sifts through network traffic and spots anomalies like irregular data flows. Our systems and processes, refined through decades of data breach investigations, use pattern recognition to catch subtle attack signs before data exfiltration occurs. When threats emerge, AI triggers responses like blocking malicious traffic or isolating systems, to quickly contain the threat. It learns and adapts to new tactics, a strength we've seen in rapid-deployment incident response. This speed and precision make AI a critical tool when properly utilized by our team of industry experts with decades of DFIR experience.

Jay Cann, Synoptek: We use AI to analyze network traffic, user behavior, and system logs in real time, using machine learning to detect anomalies and potential threats. It correlates data across multiple platforms, identifying sophisticated attacks like APTs. Automated response mechanisms, such as isolating infected systems or blocking malicious IPs, can minimize damage while alerting human analysts for further action.

Julian Hamood, Trusted Tech Team: Real-time detection is where AI truly shines. Whether identifying a zero-day vulnerability or triggering automated patching - AI decreases the response window dramatically. With tools like Microsoft Sentinel, we integrate AI and SOAR (Security Orchestration, Automation, and Response) capabilities to detect, correlate, and respond to threats often before an security analyst would even surface the alert. But AI isn't a cure-all; it only works when paired with a solid foundation of proactive practices, data hygiene, and robust automation.

How do you maintain human oversight in automated cybersecurity decisions?

Jeff Tutton, Intersec Worldwide, Inc.: We've found that maintaining human oversight is crucial, even with advanced AI systems. Our experts, leveraging DFIR experience, audit automated actions and use explainable AI models for clarity. High-stakes decisions, such as threat escalations, are reviewed by our team to add context and ensure accuracy. Regular monitoring, informed by our compliance work, catches discrepancies and informs remediation adjustments. This expert-led model ensures automation enhances human judgment, informed and not substituted by AI, which is vital for precision and trust.

Jay Cann, Synoptek: We maintain human oversight through mandatory review loops where critical AI-driven decisions, like system lockdowns, require human approval. AI systems provide detailed explanations of actions, enabling analysts to verify or override. Regular audits and training ensure humans remain in control, balancing automation efficiency with accountability to prevent errors or misuse.

Julian Hamood, Trusted Tech Team: Human-in-the-loop (HITL) remains essential. AI can take us 90% of the way triaging, analyzing, even preparing a remediation playbook, but that final 10%? It's human. Before action is taken, a qualified analyst evaluates the threat context, validates the data, and approves or adjusts the course. This not only reduces false positives, but ensures responsible and contextual risk mitigation.

David Ellis, Productive IT Solutions: Even though AI can act quickly and handle huge amounts of data, we believe humans should always have the final say, especially when the stakes are high. Think of it like cruise control in a car: it can take over the gas and brakes, but you're still behind the wheel, ready to steer or hit the brakes if something unexpected happens. In cybersecurity, we set up AI to handle routine threats, like blocking a suspicious email or isolating a potentially infected computer, but when it comes to bigger decisions, like shutting down systems or reporting a breach, a trained human steps in to review the situation. We also regularly audit and fine-tune the AI's decisions to make sure it's learning the right patterns. It's all about balance: letting AI handle the fast, repetitive stuff while humans stay in control of strategy, context, and judgment.

How do you train employees to recognize and respond to AI- and cybersecurity-enhanced threats?

Jay Cann, Synoptek: Our employees receive regular training on identifying AI-enhanced threats like deepfake phishing or automated attacks. Simulations and workshops teach recognition of suspicious patterns and proper response protocols. Training emphasizes collaboration with AI tools, reporting anomalies, and maintaining vigilance. Continuous updates on evolving threats ensure preparedness.

Julian Hamood, Trusted Tech Team: Training must evolve as threats do. We leverage AI-powered training platforms like KnowBe4, which simulate phishing scenarios tailored to each user's actual communication patterns. It's not just canned content, AI scrubs mailboxes and generates realistic phishing attempts, enhancing user vigilance. The future threat isn't just technical, it's personal, psychological, and AI-assisted.

David Ellis, Productive IT Solutions: Training employees to recognize and respond to AI-driven and cybersecurity-enhanced threats is a bit like teaching someone to spot a scam in everyday life, it starts with awareness. We walk our teams through real-world examples, like phishing emails that look almost identical to ones from their bank, or fake login pages designed to steal passwords. We use interactive tools, short videos, and even simulated attacks to help them practice spotting red flags. And we emphasize that it's okay not to be sure, if something feels off, it probably is. Just like you'd call your credit card company if a charge looked suspicious, we encourage employees to

continued on page B-42

CYBERSECURITY

THAT WORKS WHILE YOU SLEEP

PRODUCTIVE IT SOLUTIONS.COM

At Productive IT Solutions, we don't wait for problems to strike: **we prevent them before they happen!**

WHO WE ARE

We're a cybersecurity-focused IT partner for small and mid-sized businesses who are **done chasing down tech problems.** You've got enough on your plate, managing IT shouldn't be one more thing. We fix the root issues, secure your systems, and keep your tech stable, protected, and off your worry list, **just like it should be.**

OUR PROACTIVE, MODERN APPROACH

Built to support businesses **with or without an internal IT team.**

MICROSOFT 365 PROTECTION

From email filtering to advanced endpoint protection, we lock down your Microsoft environment with layered, best-in-class security.

AI-DRIVEN THREAT DETECTION

Our advanced AI tools monitor and respond to potential threats in real-time so that your business is covered 24/7.

COMPLIANCE & RISK MANAGEMENT

Stay ahead of evolving regulations with our expert guidance and built-in policy enforcement tools.

IT SUPPORT YOUR TEAM ACTUALLY LIKES

We deliver fast, friendly support your staff doesn't dread calling, plus the training and tools they need to make smarter security decisions every day.

WHAT KEEPS YOU UP AT NIGHT?

- Cyberattacks targeting your sensitive business data?
- Microsoft 365 vulnerabilities you didn't know existed?
- The fear that AI threats are moving faster than your defenses?

We help businesses solve these challenges before they ever become problems.

WHAT OUR CLIENTS ARE SAYING

"My company has had the privilege of working with David and his team for over a decade, and it has truly been a blessing... they consistently go the extra mile to ensure the security of our data and the seamless functionality of our computers. It feels like having our own dedicated IT department. Thank you, David and team, for always being there when we need you!"

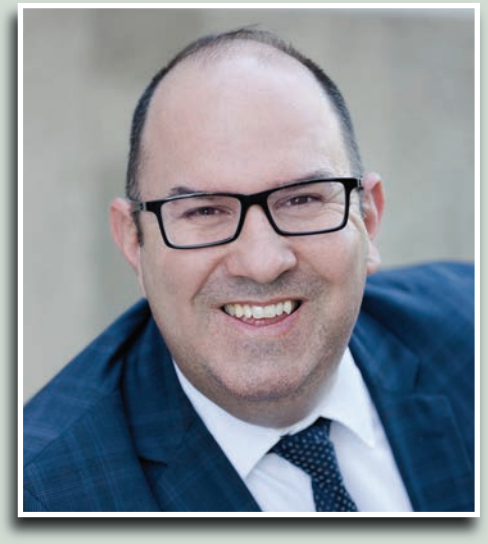
— Laura A.

JOIN THE BUSINESSES WHO SLEEP BETTER AT NIGHT.

info@productiveitsolutions.com

714-794-1080

TECH, CYBERSECURITY & AI ROUNDTABLE



AI is essential, but it is the expertise behind the technology that ensures effective, responsible use.

Jeff Tutton
President
Intersec Worldwide, Inc.

report anything unusual without fear. We also explain how cybercriminals are now using AI to make scams more convincing, like deepfake voicemails or messages that mimic a coworker's writing style. The goal isn't to turn everyone into a security expert, it's to create a culture where people stay alert, ask questions, and know that they're the first and most important line of defense.

Jeff Tutton, Intersec Worldwide, Inc.: We've developed training programs based on our extensive experience with AI-enhanced threats. Employees learn through real-world scenarios and simulations, spotting signs like odd system behavior or deepfake cues. Our programs, tailored for clients, include response protocols, such as immediate escalation. Continuous updates reflect emerging trends; a practice honed with large organizations. This practical approach equips teams to counter sophisticated threats effectively, while human experts provide strategic oversight, creativity, and ethical judgment. AI may be powerful, but there are insights and instincts only experienced professionals can provide.

What are the most common and relevant threats facing companies regarding cybersecurity?

Julian Hamood, Trusted Tech Team: Social engineering remains the top threat vector accounting for 90% of breaches. Attackers are exploiting human behavior, not just system flaws. That's why we operate with a "zero trust" mindset: assume breach, apply least-privilege access, and continuously verify. Internal threats like careless sharing to misconfiguration also present growing risks. It's not about if, but when.

David Ellis, Productive IT Solutions: The most common threats aren't high-tech Hollywood hacks, they're phishing emails, fake phone calls, and ransomware. A phishing email might look like it came from your bank or boss, but it's really a scam designed to steal information. Spoofed phone calls now appear to come from familiar numbers, pressuring employees to act quickly. Ransomware is another major threat, where attackers lock your files and demand payment to unlock them, often targeting small businesses through automated bots. Many companies think they're too small to be targeted, but attackers don't care who you are, just whether they can get in. That's why a mix of training, monitoring, and response tools is more important than ever.

Jeff Tutton, Intersec Worldwide, Inc.: Today's most pressing cybersecurity threats come from both external systems such as websites and email, and internal sources including employees, partners, vendors, and the supply chain. Phishing, ransomware, and malware attacks are increasingly powered by AI, making them more effective and harder to detect. Advanced tactics like deepfakes and third-party breaches target trust and operational dependencies. Insider threats and compliance failures also pose serious risks. AI is essential, but it is the expertise behind the technology that ensures effective, responsible use. Human insight is critical to interpreting complex threats, making strategic decisions, and adapting to evolving risks. We combine cutting-edge technology with our team's expertise to build resilient, proactive cybersecurity programs.

Jay Cann, Synoptek: Common threats include ransomware, phishing (including AI-generated deepfakes), insider threats, and advanced persistent threats (APTs). Cloud vulnerabilities and supply chain attacks are rising concerns. Unpatched software and weak credentials remain prevalent risks. AI-driven attacks exploiting automation and social engineering are increasingly sophisticated, targeting sensitive data and critical infrastructure.

How are AI-driven security systems actually catching threats that human analysts miss?

David Ellis, Productive IT Solutions: AI can spot tiny, unusual behaviors hidden in massive amounts of data. Imagine trying to find one odd receipt in a year's worth of credit card statements, it's easy for a person to miss, but AI can scan it all instantly and flag anything that doesn't belong. It looks for patterns, like strange file downloads, odd login times, or unusual sequences of events that match known attack behavior. AI doesn't get tired or distracted. It continuously learns and gets better over time, helping security teams focus on real risks instead of being overwhelmed by alerts. It's not replacing people, it's helping them see what they otherwise couldn't.

Jeff Tutton, Intersec Worldwide, Inc.: AI-driven security systems excel at processing vast volumes of data at high speed, surfacing anomalies and subtle attack signatures that may be difficult to identify without deeper forensics analysis. However, the true strength of AI is unlocked through expert human guidance. Informed by our MDR and DFIR expertise, we continuously train and refine these systems to adapt to emerging threats and identify novel attack patterns such as zero-days. This relentless and intelligent analysis, proven through real-world breach investigations, reduces noise, flags risk earlier, and improves detection accuracy. As experts, we recognize that AI does not replace human insight but enhances it, enabling faster, more precise, and more effective threat response.

Jay Cann, Synoptek: AI systems process massive datasets at scale, detecting subtle anomalies like unusual network patterns or micro-changes in user behavior that humans overlook. Machine learning identifies zero-day exploits and low-and-slow attacks by correlating disparate signals. Predictive analytics flag emerging threats before they manifest, outpacing manual analysis in speed and precision.

Julian Hamood, Trusted Tech Team: AI's real power is in scale and pattern recognition. Humans can't feasibly scan petabytes of logs, nor can they easily detect subtle behavioral anomalies. AI closes that gap, identifying lateral movement, brute-force attempts, or irregular login behavior before they escalate. More than that, it prevents analyst burnout by automating tedious log analysis and patching. AI reviews what humans can't, freeing people to focus on high-level strategy and critical decision-making.

IT'S NOT IF BUT WHEN

INTERSEC
WORLDWIDE

Are you Prepared for a Data Breach?

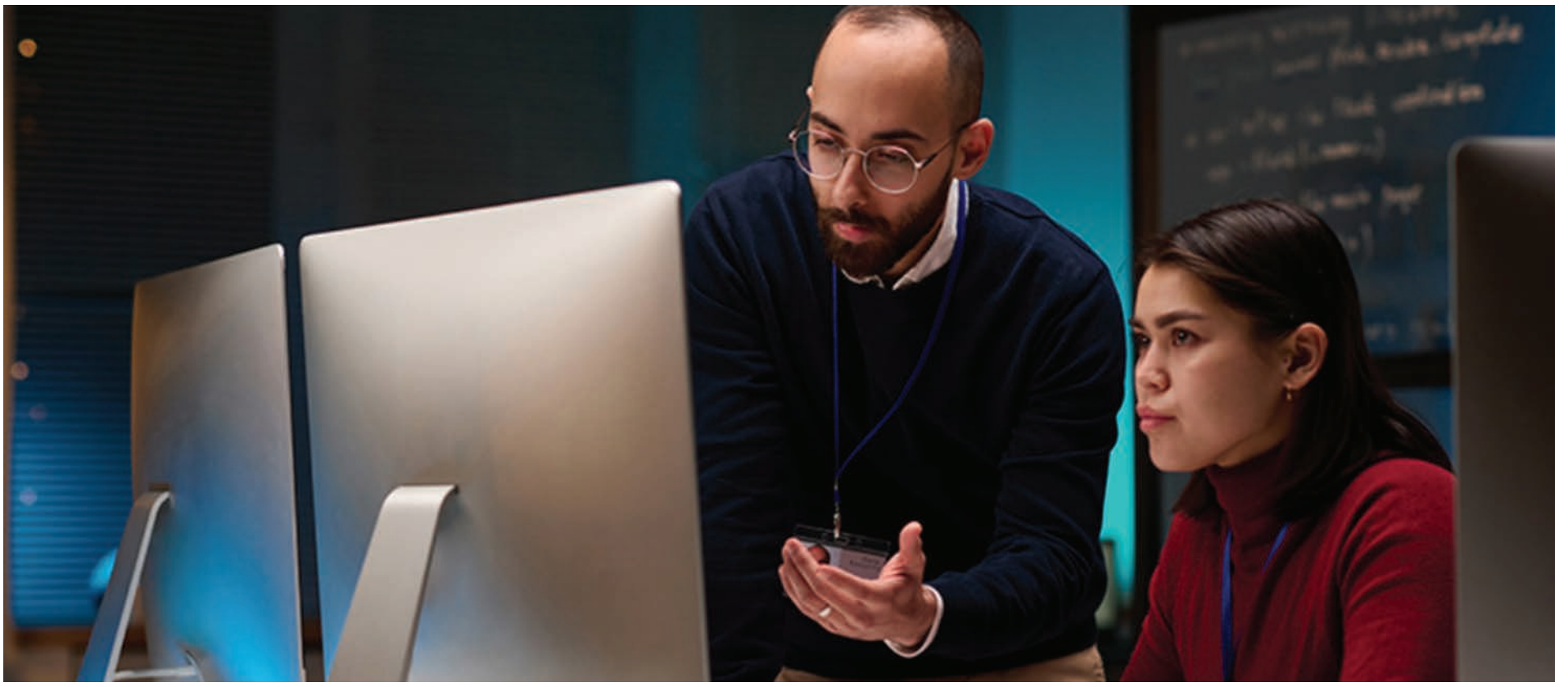
Trust only the most experienced team of cybersecurity professionals. We have been serving the world's top brands for decades.

Business Talk
VOICE OF THE BUSINESS LEADERS
5 MOST TRUSTED CYBERSECURITY COMPANIES 2025

SECURE YOUR ORGANIZATION

Scan to get started

intersecworldwide.com | info@intersecworldwide.com | 1-800-499-5834



3 Threat Trends Driving Adaptive Cybersecurity

Artificial intelligence is reshaping cybersecurity, enhancing both offensive and defensive capabilities.

On the one hand, it's fueling faster, smarter, automated defenses. On the other, it's given attackers multiple new, easily accessible ways to wreak havoc. And that means that cybersecurity leaders can't stay in the past.

The current moment calls for cybersecurity approaches that are not only nimble enough to handle the rapid pace of change in the short term, but also resilient and adaptable enough to continue to evolve alongside longer term trends—even those that aren't foreseeable right now.

In short, enterprise organizations are increasingly adopting an adaptive security posture—one that combines real-time, AI-driven threat detection with flexible, policy-based access controls that evolve alongside the threat landscape. At the same time, they're investing in adaptive network infrastructure that can self-monitor, self-heal, and dynamically prioritize or reroute traffic to help minimize downtime and contain risk. Together, these capabilities form a responsive, resilient defense framework that's built to meet the demands of today's attacks and evolve with whatever comes next. Here are the business, technology, and threat trends driving adaptive cybersecurity in 2025 and beyond.

1. The AI Race: Attack and Defense Collide

Cyber criminals are quickly weaponizing AI. Deepfakes, convincingly real phishing emails, and advanced social engineering scams powered by generative AI are popping up with increased frequency. And people are falling for them. According to Deloitte, 40% of all phishing attacks are now generated by AI, and generative AI is set to multiply losses from deepfakes and other attacks by 32%, hitting $40 billion by 2027.

Enterprise security leaders are responding in turn. According to Gartner, fewer than 10% of cybersecurity leaders say they have no plan to adopt GenAI for cybersecurity use cases. It's not hard to see why— Deloitte reports that AI reduces the average time to detect a cyberattack by up to 96%. Still, it's important to take a strategic approach.

Noopur Davis, executive vice president, chief information security officer and product privacy officer at Comcast, framed the challenge clearly at a recent industry event: "We're asking three questions. How do we protect our own use of AI? How do we protect ourselves from malicious AI? And, how do we use AI effectively to defend ourselves better?"

The takeaway here: it's no longer enough to simply respond to threats—organizations have to respond instantly or even anticipate them. AI tools that analyze unusual patterns, automate threat detection, and speed up incident responses are quickly becoming essential.

2. The New Identity Crisis: Machines and Human Users

Traditional Identity Access Management was built around ensuring the right human users have access to the right data—and the wrong ones don't. But today, machines—APIs, bots, IoT devices, service accounts—far outnumber their human counterparts, by as much of a factor as 45 to 1. And according to Gartner, 54% of organizations report an increase in identity-related breaches, and a staggering 85% those involve compromised non-human identities.

It's an increasing enterprise blind spot. Traditional Identity and Access Management isn't built for this scale, or for the volume of AI agents currently populating the digital world. The new paradigm calls for the implementation of comprehensive Identity Access Management (IAM) strategies, ideally spearheaded by machine identity working groups that collaborate with stakeholders across the business. Companies are also turning to identity-first frameworks like zero trust to address this gap. These models continuously verify every entity—human or otherwise—in real-time, significantly reducing the risk of credential compromise.

The Fragility and Importance of Digital Trust

As digital identities continue to outpace human ones, trust has never been more fragile—or more valuable. The concept of digital trust—a measure that encompasses both the trust that individuals place in organizations and the trust that organizations place in the entities they interact with—is growing in importance. Eighty-two percent of digital trust professionals say the concept will continue to grow in importance in the next five years, while only 53% of organizations are confident in their digital trustworthiness.

Ensuring digital trust rises above the importance of a security concern to a foundational business imperative. Brands that can't ensure digital interactions are secure risk losing loyalty and revenue.

3. Breaking Silos: Cybersecurity Becomes Everyone's Responsibility

Cybersecurity and cyber risk management are no longer just the purview of the security and IT teams. Line of business leaders increasingly view cyber threats as a core business risk. This shift means security accountability is spreading to every corner of the organization. It also means that enterprise teams are changing who owns risk—and who makes decisions around it.

Gartner reports that 55% of technology leaders state they are taking a centralize-to-decentralize path: Creating centralized enterprise security steering committees that include technology and line-of-business leaders, to effectively decentralize risk ownership across the business.

This kind of alignment allows companies to embed security into everyday operations rather than treating it as an afterthought.

Adaptive Networks, Adaptive Security: Building for Resilience

As attacks grow more sophisticated and digital trust more fragile, organizations must weave adaptability directly into their cybersecurity and networking fabrics.

Adaptive security means dynamically aligning protective measures to shifting threats in real-time. Tools like Managed Detection and Response (MDR), advanced IAM frameworks, zero-trust stances, and Secure Access Service Edge (SASE) architectures have become essential. Equally critical are adaptive networks, intelligently self-monitoring and self-healing in response to threats.

The path forward demands that organizations anticipate threats, automate intelligently, collaborate broadly, and adapt continuously. In other words, resilience is less about preventing every threat, and more about ensuring that when threats arrive, the organization is prepared, responsive, and quick to recover.

Comcast Business helps guide enterprise technology leaders through an ever-changing cybersecurity landscape so they can be better prepared and transform challenges into opportunities. Contact Comcast Business Sales Manager Ryan Chessman to learn more – Ryan_Chessman@comcast.com (949) 992-0761

COMCAST BUSINESS

Comcast Business is now powering the engine of modern business in Orange County.

Advanced solutions from Comcast Business can help power your business and keep you ready for what's next. Comcast Business provides leading networking & connectivity, advanced cybersecurity, and expert partnership, helping keep your business operations running smoothly.

Visit **comcastbusiness.com/enterprise** to learn more.

COMCAST BUSINESS