TECHNOLOGY

CUSTOM CONTENT • JUNE 29, 2026

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

How Orange County Businesses Are Rethinking Cybersecurity in the Age of AI

As Orange County businesses continue to accelerate digital transformation, cybersecurity threats are becoming more sophisticated and harder to detect. From AI-driven attacks to the growing challenge of protecting data across hybrid environments, enterprise organizations are rethinking how they defend their operations. We spoke with Jason Thompson of Comcast Business, an Advanced Security Specialist based in Southern California, to get his perspective on the risks shaping 2026 and how companies can stay ahead.

Jason Thompson – Advanced Security Specialist / Comcast Business
Bio: Jason Thompson is a skilled Security Specialist with Comcast Business. Currently working out of the Los Angeles area, he has over a decade of experience in the cybersecurity vertical and has worked with businesses of all sizes to align security solutions with their strategic objectives. Throughout his career, Jason has held support, solution engineering and specialist's roles at leading cybersecurity companies, including Rapid7, Varonis, Forcepoint, BlackBerry Cylance and Arctic Wolf. He holds a Bachelor of Science in Computer Information Systems from Hampton University and continues to pay it forward by helping people launch their own careers in the cybersecurity industry.

1) What are the most significant cybersecurity threats organizations are facing in 2026, and how have they evolved over the past year?
The biggest shift is attackers moving earlier in the kill chain, using AI to scale attacks and blend into normal business traffic. High volume phishing, drive by compromise, and credential abuse remain dominant entry points, but they are now paired with stealth techniques like living off the land and encrypted command activity. Attackers are also leveraging proxy infrastructure to mask origin and automate reconnaissance at scale. The real evolution is combining speed, volume, and stealth. Comcast Business EDR and MDR help counter this by identifying early signals and correlating activity across endpoints to stop threats before they escalate.

2) Where are you seeing companies fall short in their cybersecurity strategies-and what should they be doing differently?
Organizations continue to fall short in fundamental areas like patching, credential hygiene, and configuration management, while relying too heavily on perimeter defenses that attackers easily bypass. At the same time, security teams are overwhelmed by alert volume, which slows investigation and response. The shift required is toward continuous monitoring, faster response, and layered defense that assumes compromise. Comcast Business EDR delivers endpoint visibility to detect suspicious activity, while MDR provides around the clock monitoring, threat hunting, and expert response, helping organizations close gaps and respond before threats turn into full scale incidents.

3) How should business leaders balance security investments with operational efficiency and growth?
Security investments should be aligned to protecting uptime, revenue, and customer trust without creating unnecessary operational burden. The most effective approach prioritizes high impact risks like credential compromise and service disruption while focusing on foundational controls that eliminate easy entry points. Because prevention is never perfect, detection and response become critical to limiting impact. Comcast Business MDR enables organizations to achieve this balance by delivering continuous monitoring and response capabilities without the need to build large internal teams, improving efficiency while strengthening overall security posture and supporting business growth.

4) How do you maintain oversight in automated cybersecurity decisions?
Automation is essential for managing the scale and speed of modern threats, but it must be governed carefully. Effective programs use defined playbooks to control which actions can be automated and when human approval is required. Comcast Business MDR combines automated detection with SOC analyst oversight, ensuring alerts are validated and responses are appropriate to the situation. Strong audit trails and reporting provide transparency for leadership, while continuous tuning improves accuracy over time. This approach allows organizations to act quickly while maintaining control and accountability across security operations.

5) How do you train employees to recognize and respond to AI-and cybersecurity-enhanced threats?
Employees are increasingly targeted through AI enhanced attacks that make phishing, voice impersonation, and social engineering more convincing. Training should reflect this shift by covering modern communication channels like text and collaboration tools, along with realistic simulations that mirror current attack techniques. Clear and simple reporting processes also help reinforce good behavior. At the same time, users cannot be the only line of defense. Comcast Business EDR and MDR provide detection capabilities that identify malicious activity even when a user makes a mistake, combining awareness with technology to reduce overall risk.

6) How are AI-driven security systems actually catching threats that human analysts miss?
AI plays a critical role in identifying threats across massive volumes of activity that would be impossible for humans to analyze manually. It can uncover subtle anomalies in user behavior, endpoint processes, and network activity that indicate early stages of compromise. Comcast Business EDR applies this intelligence at the endpoint level, while MDR correlates signals across environments to identify patterns that might otherwise go unnoticed. Human analysts then validate these findings and take action. This combination improves detection accuracy, reduces noise, and shortens the time between initial compromise and containment.

7) Looking ahead, what should Orange County business leaders prioritize over the next 12-18 months to stay ahead of cyber threats?
Organizations should focus on reducing initial access, improving detection speed, and strengthening resilience. This includes tightening identity controls, addressing vulnerabilities through continuous patching, and improving visibility across endpoints and environments. It is also important to prepare for service disruption scenarios such as ransomware or distributed attacks that affect availability. Comcast Business EDR and MDR support these priorities by providing continuous monitoring, advanced detection, and rapid response capabilities. Organizations that invest in these areas will be better equipped to contain threats quickly and maintain business continuity.

> "The shift required is toward continuous monitoring, faster response, and layered defense that assumes compromise."
>
> **Jason Thompson**
> **Advanced Security Specialist**
> **Comcast Business**

COMCAST BUSINESS

Why the Smartest Orange County Companies Are Putting IT, Security, Compliance, and AI Under One Roof

The era of treating technology as four separate problems is ending. For manufacturers and growing businesses across Southern California, the smarter move is to manage IT, security, compliance, and AI as one strategy — before a deadline or a breach forces the issue.

By Shuchipan Sharma, Founder & CEO, TechHeights

Walk into almost any mid-sized Orange County company today, and you will find technology managed in pieces. One vendor keeps the network running. Another sells a security tool. A consultant shows up when an auditor sends a questionnaire. And somewhere in the building, employees have quietly started pasting company data into AI chatbots without approval. Each piece may be handled competently. The problem is that no one is responsible for how they fit together — and the gaps between them are exactly where risk, cost, and missed opportunity hide.

That fragmentation is becoming untenable. Cyber threats now move faster than siloed teams can coordinate. Federal compliance mandates are arriving with hard deadlines. And artificial intelligence is entering the workplace whether leadership has a plan for it or not. The companies pulling ahead are the ones that have stopped buying technology one box at a time and started managing four connected disciplines as a single strategy: managed IT, managed security, managed CMMC compliance, and AI governance.

Pillar One: IT That Enables, Not Just Maintains
Managed IT used to mean a help desk and a server closet. Today it is the foundation on which everything else stands. When patching is inconsistent, backups go untested, and no one maintains a current inventory of devices and accounts, every other initiative inherits that weakness. You cannot secure, certify, or responsibly automate an environment you do not fully understand.

A modern managed services provider, or MSP, manages IT proactively — monitoring systems before they fail, standardizing configurations, and aligning the technology roadmap with where the business is headed. For a manufacturer adding a production line or a firm opening a second location, that foundation enables growth without multiplying risk. The goal is no longer simply keeping the lights on. It ensures the infrastructure is clean, documented, and ready for the demands the next three pillars place on it.

Pillar Two: Security As a Discipline, Not a Product
Many business owners assume they have security handled because they bought a firewall and antivirus software. Attackers count on exactly that assumption. The threats facing a Southern California machine shop or distribution business today — ransomware, business email compromise, stolen credentials — are not stopped by a single product. They are stopped by a discipline: continuous monitoring, rapid detection, tested response plans, and people trained to recognize an attack in progress.

This is the difference between an MSP and a managed security services provider (MSSP). An MSP keeps your technology running. An MSSP is built to defend it around the clock, with security operations, threat detection, and incident response as the core service rather than an add-on. For most growing companies, the right answer is not choosing between the two but having both work in concert — the same partner running the environment and watching for trouble, so nothing falls through the seam between "that is an IT issue" and "that is a security issue."

Pillar Three: CMMC Compliance and a Deadline That Is Already Here
For any Orange County company in the defense supply chain, compliance is no longer theoretical. The Department of Defense's Cybersecurity Maturity Model Certification — CMMC — became final in late 2024 and is now being rolled out in phases. As of late 2025, defense solicitations began requiring CMMC self-assessments, and the requirements will tighten from there. By the fall of 2026, new contracts involving controlled unclassified information will require certification at the appropriate level, with an independent third-party assessment for Level 2.

Here is what catches manufacturers off guard. Your real deadline is not a date on a government calendar — it is the day your next contract, renewal, or option year is solicited. For smaller awards, that window can be ninety days or less. Prime contractors, unwilling to risk their own eligibility, are already pushing these requirements down to their subcontractors ahead of schedule. A shop that waits until it loses a bid to discover it is not certified has waited too long. Achieving CMMC compliance typically takes months of remediation, documentation, and evidence-gathering, which is precisely why it cannot be bolted on at the last minute.

Managed compliance turns that scramble into a program. Rather than treating an audit as a fire drill, the right partner maps your environment to the required controls, closes the gaps methodically, and maintains the documentation continuously so you are always ready — not just ready for one assessment. And because the CMMC controls overlap heavily with sound security practice, the work done here reinforces pillars one and two rather than duplicating them.

Pillar Four: Governing AI Before it Governs You
The newest pillar is the one that most companies have no plan for. Your employees are almost certainly already using AI tools — to draft emails, summarize documents, write code, or analyze spreadsheets. That can be a genuine productivity gain. It can also mean sensitive customer data, proprietary designs, or controlled information is being fed into systems your company does not control and cannot audit. For a defense contractor, an unmonitored AI tool handling controlled unclassified information is not just risky; it can be a compliance violation.

AI governance is not about banning these tools. Prohibition simply drives the activity underground. It is about adopting AI deliberately: deciding which tools are approved, what data may and may not be used with them, how outputs are checked, and who is accountable. Done well, governance lets a company capture AI's upside — faster work, lower cost, better insight — while keeping it inside the same security and compliance boundaries that protect everything else. The companies that get this right will pull away from competitors who either ban AI outright or let it run unmanaged.

Why One Roof Beats Four Vendors
The reason to consolidate these pillars is not convenience. It is that the seams between vendors are where problems live. When IT, security, compliance, and AI governance sit with separate providers, no one owns the whole picture. The security tool flags an alert the IT vendor never sees. The compliance consultant recommends a control the network was never configured to support. The AI policy, if it exists at all, has no connection to the systems it is supposed to govern. Each vendor optimizes its own slice, and the business absorbs the gaps.

Under one roof, those four disciplines reinforce one another. The inventory that makes IT reliable is the same inventory that proves compliance. The monitoring that catches an intruder is the same monitoring that watches for misuse of an AI tool. The documentation that satisfies a CMMC assessor is the same documentation that shortens a cyber-insurance application. Integration is not a nice-to-have; it is where the actual value lives.

The Bottom Line For Orange County Leaders
Technology decisions that used to be operational are now strategic. A missed CMMC deadline can cost a contract. An unmanaged AI tool can leak the data the contract depends on. A security gap can shut down production for days. None of these can be solved in isolation, because none of them exist in isolation.

The most resilient companies in our region are the ones treating IT, security, compliance, and AI governance as a single, coordinated strategy — and starting before a deadline or an incident makes the decision for them. The deadlines are already on the calendar. The AI tools are already in the building. The only real question left for leadership is whether these four pillars will be managed together, on purpose, or left to collide on their own.

Shuchipan Sharma *is the Founder & CEO of TechHeights, a managed IT and cybersecurity firm serving Orange, Riverside, and Los Angeles counties, with expertise in managed security, CMMC compliance, and AI adoption and governance.*

techHEIGHTS
Your Next IT Level

SMARTER IT. STRONGER SECURITY. POWERED BY AI. REAL RESULTS.

We act as your full IT department, so you can focus on running your business, not fixing technology.

Our Services:

- AI Governance ☑
- Managed Security ☑
- Mangaged IT Support ☑
- Managed CMMC Compliance ☑

AMERICA'S FASTEST-GROWING Inc. 5000 PRIVATE COMPANIES

CYBER AB CMMC CERTIFICATION REGISTERED PRACTITIONER ORGANIZATION RPO

TOP CYBERSECURITY COMPANY Clutch ORANGE COUNTY 2026

Contact Us

949-565-3530

www.TechHeights.com