UK enterprises are fighting a new breed of endpoint threats

In an era where hybrid work and cloud computing have transformed the enterprise landscape, endpoint security has never been more critical. We explore the evolving threats, limitations of traditional tools, and the next-generation strategies being deployed...

When the UK's enterprise networks went remote almost overnight, the security perimeter dissolved, and endpoints became the new battleground. Laptops, mobiles, IoT sensors, and cloud instances are now the front line of cyber defence. But as threats evolve, experts say too many organisations are still fighting today's battles with yesterday's tools.

"Businesses aren't just dealing with malware anymore," warns Jack Waters, SVP of Engineering and Customer Support at WatchGuard Technologies. "They face sophisticated threats such as fileless attacks, credential theft, and living-off-the-land techniques that bypass traditional defences. Anything less than full endpoint detection and response is putting your business at risk."

The shifting shape of endpoint risk

Endpoints have become a magnet for attackers because they offer both access and invisibility. According to David Catalán Alegre, TRU Researcher at Acronis, "the most common endpoint risks today come from social engineering, unpatched software, and stolen credentials. Social engineering is growing more sophisticated with AI, while ransomware remains the most disruptive and profitable threat."

Social engineering and phishing remain devastatingly effective because they target the weakest point in the security chain: people. Attackers now combine AI-generated phishing campaigns with convincing pretexts and cloned login portals. One successful credential theft can allow adversaries to move laterally across the network, steal sensitive data, or plant ransomware that cripples operations.

"Enterprises are hit hardest by identity-led compromise — phishing, social engineering, and abuse of legitimate remote tools like RMM or screen-sharing,"

David Catalán Alegre, Acronis

adds Harry Mason, Head of New Business at Mason Infotech. “Add in unmanaged or shadow IT endpoints and it’s a potent mix of vulnerabilities.”

Meanwhile, many UK enterprises still depend on software-based defences that fail to protect the device’s most critical layers. Thorsten Stremlau, Co-chair of the Marketing Work Group at Trusted Computing Group (TCG), argues that the next evolution of endpoint security lies beneath the operating system: “software-only security models struggle to verify device integrity or detect low-level compromise,” he says. “Hardware-based Roots of Trust — like TPMs — move security below the OS, ensuring devices boot securely and behave as expected from power-on.”

This shift toward hardware-backed assurance, Stremlau suggests, is essential to stop firmware tampering and rootkit persistence that can outlive any software reinstall.

Antivirus alone can’t save you

If there’s one thing the experts agree on, it’s that traditional antivirus has had its day. Legacy tools rely on signatures and heuristics, leaving blind spots for anything novel or stealthy.

“AV tools focus on blocking known malware, but they can’t detect novel attacks or insider misuse,” says Waters. “They’re reactive, leaving enterprises blind to the stealthy techniques that define today’s threat landscape.”

Harman Singh, Director at Cyphere, explains why: “signature-based AV misses fileless attacks, LOLBins, in-memory payloads, and abuse of legitimate tools. It rarely understands identity misuse or lateral movement. Modern threats chain multiple steps — initial access, credential theft, persistence, exfiltration — so you need EDR or XDR with behavioural detections and device isolation.”

In other words, antivirus may still have a role, but it’s like locking the front door while leaving the windows open. Modern attackers exploit trusted tools such as PowerShell or WMI, hide in memory, and use compromised identities to avoid tripping traditional alarms. Marc Briggs, COO at SE Labs, adds that “traditional antivirus still relies heavily on signatures. It offers limited visibility into malicious behaviour and minimal remediation beyond quarantining files. The modern endpoint stack has to correlate behaviour, identity, and context in real time.”

> “Antivirus may still have a role, but it’s like locking the front door while leaving the windows open. Modern attackers exploit trusted tools such as PowerShell or WMI, hide in memory, and use compromised identities to avoid tripping traditional alarms.”

For Mason, antivirus’s limitations illustrate a deeper problem: overreliance on reactive controls: “signature-driven AV is blind to modern techniques like AiTM phishing or consent-phishing,” he says. “The modern stack is behaviour-centric EPP plus EDR/XDR — kernel sensors, AMSI inspection, application control. You shrink the execution surface and prevent whole classes of attacks before they start.”

Stremlau, too, points out that antivirus’s OS-level perspective misses the threat below.

“Antivirus tools operate at the OS level and often lack visibility into the boot process or firmware integrity,” he notes. “TPMs fill this gap by enabling measured boot and secure storage of integrity metrics, providing assurance that antivirus alone cannot.”

Jack Waters, WatchGuard Technologies

The remote revolution

The pandemic may have normalised flexible working, but it also shattered the illusion of a contained, defensible network.

“Devices connect from anywhere, making it harder to enforce policy and spot abnormal activity,” says Waters. “EDR provides visibility into every endpoint, no matter where it resides.”

Hybrid and remote endpoints often sit behind home routers, unmanaged Wi-Fi, or coffee-shop networks. Briggs describes the fallout: “remote and mobile endpoints break the assumptions of the ‘trusted internal network’. They introduce patch delays, segmentation gaps, and unpredictable connectivity.”

According to Singh, Zero Trust principles must now guide enterprise strategy: “strengthen your zero trust access — extend conditional access with continuous authorisation and use the endpoint’s host firewall to enforce micro-segmentation regardless of location.”

In other words, no device or user is inherently trusted; each access request must be verified, authenticated, and continuously validated.

Mason paints a vivid picture of the modern workforce: “if everyone’s working from wherever they like, you have to start thinking about identity, device, and app trust. Conditional access, managed devices, and app protection policies are non-negotiable.”

Meanwhile, Stremlau brings the conversation back to trust at the hardware level: “remote devices may connect via unsecured networks or run unverified firmware. The challenge is not just visibility but trust. Technologies like DICE and virtual TPMs let organisations verify device identity from the first boot — even for cloud-based or remote endpoints.”

Indeed, mobility expands the attack surface in unseen ways.

“Remote and mobile workforces have expanded the attack surface far beyond the corporate perimeter,” says Alegre. “This diversity makes patching, policy enforcement, and data protection more difficult, while attackers exploit weak Wi-Fi, malicious apps, and stolen credentials.”

The human factor

For all the advances in endpoint protection, the most unpredictable variable is still the user.

“User actions — clicking phishing links, mishandling data — are a major risk,” says Waters. “EDR helps spot those behaviours early and shut them down before they become breaches.”

“User behaviour is still the weakest link,” agrees Briggs. “Whether through credential reuse or inadvertent privilege misuse, insiders or compromised users can bypass even robust controls.”

Insider threats, intentional or not, remain a persistent challenge. Singh explains: “most breaches hinge on user behaviour — approving rogue pushes, syncing data to personal clouds. You mitigate with least privilege, just-in-time admin, and micro-training triggered by risky actions.”

Mason argues that insider risk must be treated as a multidisciplinary issue. “IT, HR, and Legal must work together. Users need phishing-resistant MFA like FIDO2, but you also need a culture where reporting mistakes isn’t punished.”

For Stremlau, the answer lies in binding user and device trust together. “Misuse of credentials or unauthorised software can bypass traditional controls,” he says. “A TPM securely stores credentials and platform measurements, ensuring that only authorised users and trusted devices can access sensitive information.”

Catalán Alegre agrees that technology and culture must evolve in tandem: “users remain one of the most unpredictable variables in endpoint security. Training is crucial, but so are solid access controls and close collaboration with HR. The key is balancing monitoring with a culture of trust and accountability.”

Marc Briggs, SE Labs Ltd

Register for Networking+

Seeing everything, trusting nothing

Visibility and control are the twin pillars of modern endpoint security. Without them, prevention, detection, and compliance all collapse.

"You can't protect or attest to what you can't see," says Singh. "Handle device heterogeneity with compliance gates and quarterly attestations — close gaps fast or remove access."

Visibility isn't just about device inventory; it's about understanding behaviour across every layer of the endpoint.

"Without insight into firmware, boot processes, and configurations, organisations risk missing critical compromise indicators," says Stremlau. "Root of Trust technologies like TPM and DICE provide the assurance antivirus never could."

Briggs calls endpoint visibility "mission critical."

"Without insight into running processes, network connections, and configuration drift, you're blind to how threats spread," says Briggs. "The task is to build one unified view across every device."

Catalán Alegre echoes the sentiment, warning that "an endpoint you don't know exists is an unmonitored endpoint — and a compliance risk." This visibility also underpins data protection obligations under UK GDPR, where enterprises must prove they can safeguard personal data across all devices.

Mason frames visibility as both a security function and a governance discipline: "you can't patch, harden, or investigate without a trustworthy view of your devices. Visibility enables fast isolation and accurate scoping for GDPR or ISO compliance. The challenge is tool sprawl, shadow endpoints, and legacy systems — solve that, and you strengthen everything else."

Beyond the antivirus

In the modern enterprise, the endpoint is no longer a single, static device. It's a laptop in a café, a phone on a train, a virtual machine in the cloud — all potential gateways for attackers and defenders alike. The experts agree: traditional antivirus is obsolete as a first line of defence. Instead, visibility, correlation, and rapid response have become the watchwords of effective endpoint security.

As Jack Waters of WatchGuard Technologies puts it, "EDR gives security teams the visibility into every process and behaviour needed to prevent breaches and prove compliance."

In today's borderless workplace, that visibility has never been more critical. But achieving it is no small feat.

"Mixed operating systems, legacy endpoints, and shadow IT all add to the complexity," notes Harman Singh of Cyphere. "You can't protect what you can't see."

Harry Mason of Mason Infotech argues that many breaches still stem from the basics: "phishing, unpatched software, and over-privileged users continue to be the root of most endpoint compromises." The key, he says, is correlation — tying together identity, device, and network telemetry to spot anomalies early. "A macro spawning PowerShell to dump tokens might look normal in isolation, but in EDR telemetry, it stands out."

David Catalán Alegre of Acronis emphasises the role of continuous monitoring and proactive response. "Organisations can't rely on prevention alone. They need an integrated telemetry stack — EDR, XDR, SIEM, SOAR — all working together to detect, respond, and recover at speed."

Marc Briggs of SE Labs echoes this operational reality: "without insight into running processes, network connections, and configuration drift, you're blind to how threats spread. The task is to build one unified view across every device, then enforce policy and response through that fabric."

Hardware, too, is entering the spotlight. Thorsten Stremlau of the Trusted Computing Group highlights the foundational role of hardware-based roots of trust: "TPMs and DICE ensure that devices boot securely and behave as expected from power-on. You can't fake integrity below the operating system." By anchoring security in hardware, enterprises can verify trust at a level beyond software's reach.

If the past decade was about detecting malware, the next will be about proving trust. The shift from signature-based antivirus to behavioural and hardware-based assurance marks a deeper evolution in enterprise defence, from chasing threats to verifying every action, device, and identity in real time.

As threats continue to evolve, UK enterprises face a clear choice: remain reactive, or adopt a proactive model rooted in continuous visibility and verifiable trust. The future of endpoint security won't be won by blocking what's known, but by understanding everything that moves. ■

Harman Singh, Cyphere

Harry Mason, Mason Infotech

Thorsten Stremlau, Trusted Computing Group (TCG)