netutils

CYBER SECURITY

THREAT REPORT

Q2 2026

Network Utilities (Systems) Ltd
www.netutils.com | +44 (0)20 8783 3800

Index

NetUtils Q2 Threat Landscape Report

April to June 2026

Executive Summary

The most significant risks we're seeing this quarter all point to the same underlying problem, gaps in visibility, ownership and operational discipline that many organisations don't realise they have. An unpatched firewall at the network edge, an employee uploading data to an unsanctioned AI tool or a supplier with unclear security responsibilities. The exposure is there before an attacker arrives.

Internet facing infrastructure is getting significant attention this quarter, and rightly so. Firewalls, VPNs and remote access platforms sit at the entry point to corporate environments and when they're poorly monitored or behind on patches they can become a straightforward route in for attackers. Exploitation activity against edge and remote access technologies this quarter reinforces why organisations need tighter visibility across externally accessible systems, faster patch prioritisation and clearer ownership over who is monitoring administrative access.

AI is creating a separate but equally real challenge. Employees are adopting generative AI and cloud tools to get work done, usually well ahead of formal governance. At the recent TrustLayer and NetUtils customer round table, with ten customers in the room, the concern raised most consistently was how to get visibility and control over AI usage without blocking tools people find genuinely useful. Acceptable use policies don't help much if an organisation can't see which tools are actually in use or what data is being shared through them. Governance needs to move from policy statements to practical enforcement and real visibility.

The regulatory picture is also shifting. The Cyber Security and Resilience Bill points to a stronger UK focus on resilience, incident reporting and accountability across digital services and managed providers. For most customers the key question isn't just whether they fall within scope directly. It's whether they can demonstrate that supplier relationships, privileged access, monitoring and incident communication processes are properly understood and managed.

The common thread across all three areas is fairly straightforward. Resilience depends on knowing what's exposed, what's being used and how quickly the organisation can respond when risk increases. The organisations that are best placed aren't necessarily doing more than others. They just have better visibility, clearer accountability and fewer gaps in the basics.

NetUtils recommends using this quarter to review internet facing assets, tighten remote access controls, improve visibility over AI and SaaS usage, clarify supplier responsibilities and make sure incident response processes are practical and tested.

Exploitation of Internet Facing Firewalls, VPNs and Remote Access Platforms

Why the network edge is back in focus

The network edge was supposed to be a solved problem. Firewalls and VPNs have been standard components of enterprise security for decades and most organisations believe their perimeter is reasonably well managed. What Q2 2026 has demonstrated is that belief is often misplaced.

In April 2026 the NCSC warned that state linked actors are systematically targeting large networks of compromised routers, firewalls and network attached storage devices. The goal is not simply to gain access to those devices but to use them as infrastructure for reaching other organisations. The threat is not a novel technique. It is the disciplined, patient exploitation of devices that organisations treat as plumbing rather than security assets.

Two specific vulnerabilities illustrate the practical risk. Palo Alto Networks published an advisory for CVE-2026-0257 affecting GlobalProtect portal and gateway configurations in PAN-OS. The vulnerability allows an attacker to bypass security restrictions and establish an unauthorised VPN connection. Rapid7 documented active exploitation from 17 May 2026 across multiple customer environments. In the same month Arctic Wolf reported a separate campaign exploiting CVE-2026-35616 in FortiClient Endpoint Management Server deployments. Attackers did not simply gain device access: they used trusted endpoint management infrastructure to push a credential stealing payload disguised as a legitimate Fortinet update, reaching every managed endpoint in scope without needing to compromise each one individually.

These are not isolated incidents. They reflect a pattern of intent. Edge devices are being systematically targeted because they are often the weakest link in environments that have invested heavily in endpoint and identity security. Securing the interior while leaving the perimeter unmanaged is no longer a viable posture.

How attackers turn perimeter access into business impact

When organisations ask what an attacker actually gains from a perimeter compromise, the answer is almost always more than it first appears.

A compromised firewall or VPN gateway does not simply give an attacker a foothold at the edge. It can provide visibility of network traffic, access to credentials passing through, a trusted path into internal systems and, as the FortiClient case demonstrates, the ability to use legitimate management infrastructure as a delivery mechanism. Once an attacker can modify what managed endpoints receive, the blast radius extends to every device in scope.

The deeper problem is structural. In many organisations, edge infrastructure sits between team boundaries. Network teams manage the appliances. Security teams monitor alerts. IT teams own the remote access service. When an incident occurs, that division of ownership slows everything down: patching decisions wait for approval chains, log review requires access from multiple parties and containment actions get delayed while responsibilities are clarified.

This is the gap attackers exploit. The vulnerability creates the opportunity. The delay in detection and response determines the damage.

Where UK organisations are most exposed

The organisations most exposed are not necessarily those with the largest networks or the oldest technology. Risk concentrates where internet facing infrastructure has grown without corresponding growth in visibility and governance.

The exposure patterns we see most commonly include:

- Legacy VPN platforms that remain active for specific users, suppliers or administrators long after the original business need has changed
- Firewalls and remote access gateways running firmware that has fallen behind the current supported version
- Management interfaces that are reachable from the internet without a documented operational justification
- Remote access services where multi factor authentication is enforced inconsistently across user groups
- Edge devices that forward no logs to central monitoring, making detection of malicious activity dependent on local alerting alone
- Unsupported or end of life devices that will never receive the patch addressing a vulnerability an attacker is actively exploiting
- Supplier and administrator access routes that are trusted implicitly but have not been reviewed for months or years

The common thread is not technical complexity. It is the absence of clear ownership and the habit of treating edge devices as set and forget infrastructure.

Defensive priorities for IT and network teams

The starting point is knowing what you have. Organisations should maintain a current inventory of every internet facing firewall, VPN gateway, remote access portal, management interface and externally reachable administration service. That inventory should record who owns each service, what firmware version it is running, how authentication is enforced, whether it is logging to a central platform and what business purpose it serves.

Patch prioritisation should be driven by active exploitation evidence rather than severity scores alone. CISA's Known Exploited Vulnerabilities catalogue is the most reliable signal for edge infrastructure: any entry on that list affecting devices in your environment should trigger an urgent response, regardless of the original vendor rating. CVE-2026-0257 and CVE-2026-35616 both illustrate why. Initial vendor advisories described limited exploitation. Within days, independent researchers documented broader campaigns affecting multiple sectors.

Configuration hardening is equally important and often treated as a low priority. Remote access services should enforce multi factor authentication across all user groups without exception. Management interfaces should not be reachable from the internet unless there is a specific, documented and approved operational requirement. Legacy authentication methods should be disabled. Unused VPN profiles and portals should be removed rather than left dormant.

Monitoring must be treated as a core control. Edge devices should forward logs to central platforms, with alerting configured for unusual VPN activity, unexpected administrative access, configuration changes, new local accounts and authentication anomalies from unusual locations. The NCSC has specifically highlighted the importance of forensic visibility on edge devices. Without it, defenders cannot detect activity, cannot investigate effectively and cannot confirm whether an incident has been contained.

Incident response planning should explicitly cover firewall, VPN and remote access compromise. For many organisations this scenario is absent from playbooks that handle endpoint and identity incidents well. The plan should address how to isolate a device, revoke active sessions, rotate credentials, validate configuration integrity, confirm whether lateral movement has occurred and communicate potential impact to stakeholders in clear language.

What good looks like

Organisations that manage their network edge well share a common characteristic: they treat it as a security asset, not as background infrastructure.

That means knowing exactly which services are exposed to the internet, who owns them and how quickly they can be patched or isolated when a vulnerability is actively exploited. It means configuration is hardened by default rather than as an afterthought. It means logs are centralised, alerts are configured and someone is actively reviewing them. And it means the remote access estate is reviewed regularly to confirm that every connection route that exists still needs to exist.

NetUtils works with organisations at every stage of this process, from initial inventory and assessment through to configuration hardening, managed monitoring and incident response. In our experience, the organisations that are best positioned when a critical edge vulnerability is disclosed are not those with the most sophisticated

technology. They are those that know their environment, have clear ownership and have already tested how quickly they can act.

The goal is not to eliminate remote access. It is to make every access route deliberate, monitored and resilient. Organisations that achieve this find that the network edge, rather than being a liability, becomes one of the most reliable signals they have that something is wrong.

AI Visibility and Governance

The AI adoption gap

Generative AI is now part of day-to-day work for many employees. Staff use AI tools to summarise documents, draft emails, analyse data, write code, support research and improve productivity. In many cases, this use is well intentioned. The risk is that adoption often happens faster than IT, security and governance teams can assess which tools are being used, what data is being shared and whether those tools meet organisational or regulatory requirements.

This concern was reflected clearly at a recent **TrustLayer x NetUtils customer round table**, which brought together senior leaders from across sectors to discuss trust, cyber risk, AI, compliance and resilience. Our summary of the event noted that, despite different industries and constraints, organisations are facing similar underlying pressures, including AI acceleration, third party risk, compliance complexity, data sovereignty, resource constraints and the need for greater resilience and accountability.

The strongest customer concern raised during the discussion was the lack of visibility and control around AI usage. Customers were not simply asking whether AI should be allowed. They were asking how to see which AI tools are already being used, how to understand what data is being shared and how to apply practical controls without preventing useful innovation.

This is the core challenge behind Shadow AI. Employees may use public AI tools, browser extensions, plugins or AI enabled SaaS applications without formal approval. The organisation may have an acceptable use policy, but without visibility, it cannot easily confirm whether the policy is being followed.

The issue is not limited to AI. It is part of a wider pattern of cloud application sprawl. Teams often adopt new SaaS tools to solve immediate business problems, particularly where approved systems feel slow, limited or difficult to access. Over time, this creates a growing estate of sanctioned and unsanctioned applications, many of which process business data outside formal controls.

Why policy alone is not enough

Most organisations now recognise the need for AI usage policies. These are important, but they are not sufficient on their own.

A policy can explain which AI tools are approved, what data must not be entered into public platforms and when staff should seek approval. However, a policy cannot show whether employees are using personal AI accounts, uploading customer data, using unapproved browser extensions or connecting AI tools into cloud storage. It also cannot identify whether a new SaaS platform has started handling sensitive data without security review.

The round table discussion highlighted this gap in practical terms. Customers recognised that policies are necessary, but they also questioned how those policies can be enforced when AI tools are accessed through browsers, personal accounts or unsanctioned SaaS platforms. This is where the issue becomes operational rather than theoretical. Without visibility, organisations cannot confidently distinguish between safe experimentation, policy breaches and serious data exposure.

This creates a visibility gap. IT leaders may believe AI usage is limited to approved services, while employees are already using a much wider set of tools in practice. That gap matters because sensitive information may be copied into platforms with unclear retention terms, weak administrative controls, limited auditability or no contractual assurance.

TrustLayer's round table summary captured this broader governance issue clearly: AI is moving faster than governance and organisations need practical guardrails that can evolve quickly as the technology changes.

From blocking to governed enablement

The practical answer is not to ban AI outright. Blanket blocking may reduce some immediate exposure, but it can also drive users towards personal devices, unmanaged accounts or less visible workarounds. For many organisations, AI can provide real productivity and service benefits when introduced in a controlled way.

The discussion also made clear that most organisations do not want to block AI outright. Customers recognise the productivity value of AI, but they want the confidence to allow it safely. A stronger approach is governed enablement. This means giving employees access to approved AI and SaaS tools, while applying clear controls around data, users, devices and business context.

Governed enablement should answer four simple questions:

- Who is using AI and cloud applications?
- Which tools are being used and are they approved?
- What type of data is being shared?
- What controls are in place if usage becomes risky?

This shifts the conversation from "should we allow AI?" to "how do we allow AI safely?" It also supports a more constructive relationship between security teams and the wider business. Instead of becoming the team that says no, IT and security can help the organisation use AI in a way that is visible, controlled and aligned to risk appetite.

Using CASB controls to regain visibility

Cloud Access Security Broker controls are one practical way to close the gap between policy and real usage.

For the customers involved in the TrustLayer x NetUtils discussion, the priority was not simply writing another AI policy. It was gaining the visibility required to understand what is happening across the organisation and the control required to act when risk increases. CASB capabilities directly support this requirement by helping organisations discover sanctioned and unsanctioned cloud applications, assess risk, enforce usage policies and provide reporting for governance and compliance.

This is directly relevant to AI governance. Where employees use AI tools through browsers or cloud applications, a CASB style approach can help identify activity, classify applications, apply controls and report on usage trends. It can also support more nuanced decisions than simple allow or block rules.

For example, an organisation may choose to:

- Allow approved AI tools for general productivity tasks
- Block uploads of sensitive or regulated data to unmanaged AI services
- Require stronger controls for users accessing AI from unmanaged devices

- Monitor new or high risk applications before deciding whether to approve them
- Report on AI and SaaS usage to support governance discussions

For NetUtils customers, this is an important point. AI governance does not need to begin with a large transformation programme. It can start with visibility, practical control and clearer reporting.

Board level questions to ask now

AI visibility and governance should not sit only with IT. It affects data protection, compliance, operational risk, HR, finance and business leadership.

Boards and senior teams should be asking:

- Do we know which AI tools are being used across the organisation?
- Can we distinguish between approved and unapproved AI usage?
- Do we know whether customer, financial, personal or commercially sensitive data is being entered into AI platforms?
- Can we control usage based on user, device, location and risk level?
- Do employees have approved alternatives that meet their productivity needs?
- Can we evidence our controls if a customer, auditor or regulator asks?

These questions are deliberately practical. The goal is not to slow innovation, but to ensure the organisation can make informed decisions based on evidence rather than assumptions. What good looks like

A mature approach to AI governance combines policy, visibility, control and education.

Good practice starts with a clear acceptable use policy that explains which AI tools are approved, what data must not be shared and how employees can request new tools. That policy should be supported by technical visibility into actual application usage, not just annual declarations or manual surveys.

Approved AI tools should be configured with appropriate data protection controls, administrative oversight and audit logging. Unapproved or high risk tools should be monitored, restricted or blocked based on risk. Where possible, organisations should provide safe alternatives so employees are not forced to choose between productivity and compliance.

The most resilient organisations will treat AI governance as an ongoing operational discipline. New tools will continue to appear, employees will continue to experiment and business teams will continue to look for faster ways to work. The organisations that succeed will be those that can see this activity clearly, guide it constructively and intervene when sensitive data or critical processes are at risk.

The TrustLayer x NetUtils round table reinforced a wider point that applies beyond AI: trust is built through transparency, evidence, clear ownership and honest

conversations about risk. In the context of AI adoption, that means moving from assumptions to visibility and from informal policy to measurable governance.

What the Cyber Security and Resilience Bill Means for UK Customers

Note: At the time of writing, the Cyber Security and Resilience Bill is still progressing through Parliament. Report stage and third reading were listed for 16 June 2026 but parliamentary publications and amendment outcomes had not yet been published at the time of review. The recommendations in this section are based on the Bill's published direction of travel and current Government guidance.

Why the Bill matters to UK organisations

The Cyber Security and Resilience Bill represents a significant shift in how the UK intends to approach cyber resilience. The Bill is designed to strengthen national cyber defences, protect essential public services and improve economic stability by updating the existing Network and Information Systems framework. (gov.uk)

For customers, the key point is that cyber security is becoming less of a purely internal IT issue and more of a shared operational resilience responsibility. Many organisations now depend on cloud platforms, managed service providers, digital suppliers, outsourced IT support and connected systems to deliver critical services. The Bill reflects this dependency by expanding the focus beyond traditional critical infrastructure and recognising the role that suppliers and managed providers play in national resilience.

This matters even for organisations that may not be directly regulated. Customers are likely to face higher expectations from insurers, auditors, boards, regulators, suppliers and larger clients. They may also need stronger evidence that the organisations supporting their IT and cyber security can manage risk, respond to incidents and communicate clearly when disruption occurs.

Which organisations may be affected

The Bill is intended to update the UK's cyber security legislation for critical national infrastructure by amending the Network and Information Systems Regulations 2018. It extends to the whole of the UK and is currently progressing through Parliament.

One of the most important proposed changes is the inclusion of relevant managed service providers. Government guidance states that managed service providers may be in scope where they provide ongoing IT system management, including services such as IT helpdesks and cyber security services.

The Local Government Association has also summarised the Bill as bringing certain managed service providers into scope, including providers delivering IT outsourcing,

managed security or cloud hosting services in the UK. Small and micro businesses are expected to be excluded from this particular managed service provider scope.

For customers, this means the impact may be indirect as well as direct. An organisation may not itself be a regulated provider of essential services, but it may depend on suppliers that are brought into scope. It may also serve customers who expect stronger cyber assurance because of the Bill. This is why the practical question is not only "are we regulated?" but also "are we resilient enough for the expectations now forming around us?"

What customers should expect from their providers

The Bill reinforces a simple but important point: customers need clearer assurance from the providers they rely on.

For many organisations, managed IT and security providers hold privileged access to systems, networks, endpoints, backups, cloud platforms and identity environments. That access is necessary for effective support and protection, but it also creates concentration of risk. If a provider is compromised or if responsibilities are unclear during an incident, the customer can experience disruption, data exposure or delayed recovery.

Customers should therefore expect providers to be able to explain:

- who has privileged access to customer systems
- how that access is approved, monitored and removed
- how customer environments are separated and protected
- how vulnerabilities and patches are prioritised
- how incidents are detected, escalated and communicated
- how backups and recovery processes are tested
- what evidence can be provided to support security claims

This does not mean customers need to demand excessive documentation or create unnecessary bureaucracy. It means moving from informal trust to evidenced trust. A good provider should be able to explain its controls in clear language, be open about responsibilities and show how it would support the customer during a real incident.

Incident reporting and communication expectations

The Bill is also expected to place greater emphasis on incident reporting. Government factsheets state that more forms of harmful cyber breaches would need to be reported by operators of essential services and relevant managed and digital service providers. This includes incidents such as successful ransomware and prepositioning attacks that are likely to have significant UK impact, even where impact has not yet materialised.

For customers, this raises an important operational issue. During a cyber incident, speed and clarity matter. Customers need to know who will notify whom, what information will be shared, how quickly escalation will happen and which decisions need customer approval.

A customer should not be working this out for the first time during a live incident. Incident communication routes should be agreed in advance, including escalation contacts, out of hours processes, executive communication, legal and regulatory considerations and coordination with cyber insurers or external responders where required.

The most resilient customer provider relationships are those where communication is rehearsed before it is needed. That does not require complex exercises in every case. Even a simple tabletop review can expose unclear ownership, missing contacts or assumptions that would slow response during a real event.

Practical steps customers can take now

Customers do not need to wait for the Bill to become law before improving their resilience. The most useful actions are practical and achievable.

Start by identifying critical digital services. This includes systems that support customer service, finance, operations, communications, identity, backups, remote access and security monitoring. For each service, organisations should understand which internal team or external provider supports it, what access they hold and how service disruption would affect the business.

Next, review supplier dependencies. Customers should identify which providers have administrative access, which systems they can reach and whether that access is still required. Supplier access should be based on least privilege, reviewed regularly and removed promptly when no longer needed.

Customers should also ask providers for evidence of core controls. This may include patch management processes, access control procedures, monitoring arrangements, backup testing, incident response plans, vulnerability management and security certifications where relevant. The aim is not to catch suppliers out, but to establish a shared understanding of how resilience is maintained.

Incident response arrangements should be documented. Customers should know who to contact, how urgent issues are escalated, what the provider will do first, what information the customer will receive and how decisions will be made. These arrangements should be tested periodically.

Finally, customers should ensure that contracts and service descriptions reflect operational security expectations. If security monitoring, patching, backup testing or incident support is assumed but not documented, the customer may discover during an incident that responsibility is less clear than expected.

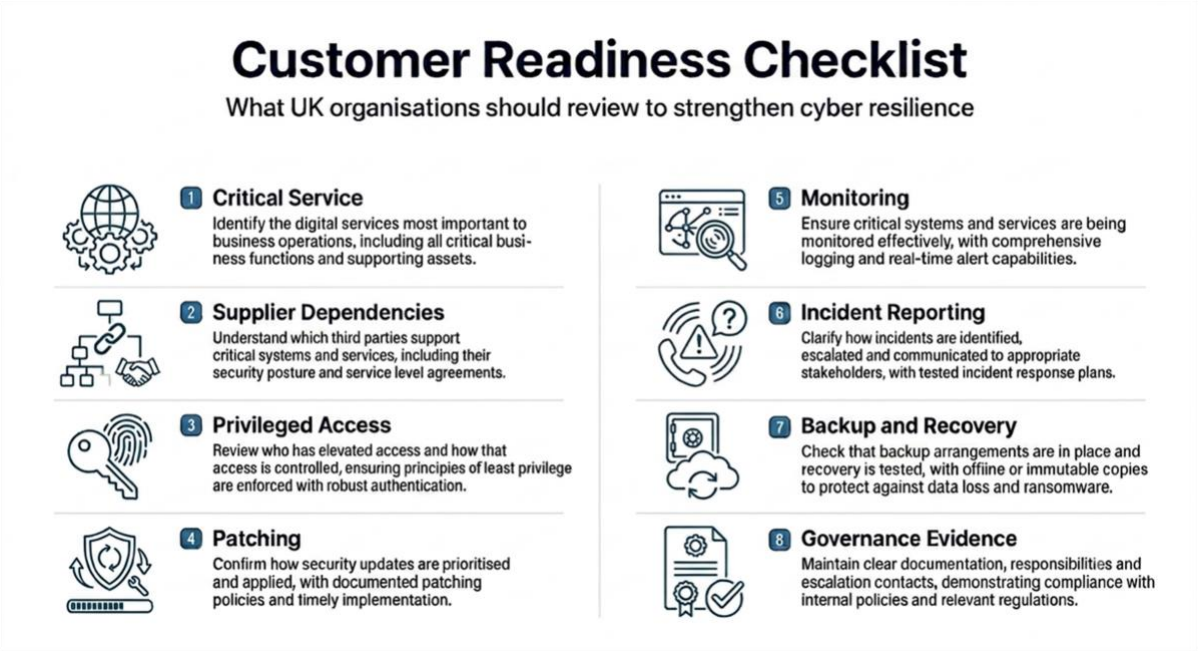
What good looks like

The Cyber Security and Resilience Bill should not be viewed only as a compliance exercise. For customers, its greater value is as a prompt to strengthen accountability across the services and providers they rely on.

Regulation can create pressure, but it can also create clarity. It encourages organisations to ask better questions, document responsibilities, review supplier access, improve incident communication and test whether recovery plans will work in practice.

For NetUtils customers, the practical takeaway is straightforward. Resilience depends on knowing which services matter, who supports them, how they are protected and how quickly the organisation can respond when something goes wrong. The Bill reinforces that these are becoming standard expectations for organisations that rely on digital services and managed providers.

The organisations best positioned for this shift will be those that treat cyber resilience as a shared responsibility rather than a supplier checkbox. They will expect transparency from providers, maintain clear ownership internally and build evidence that critical services can be protected, monitored and recovered.



NetUtils Aligned Recommendations

The topics in this report point to a common requirement: customers need better visibility, clearer control and practical resilience across the systems, applications and providers they depend on. The recommendations below are designed to help organisations act without creating unnecessary complexity.

1. Treat the network edge as a critical security layer

Firewalls, VPNs, remote access platforms and management interfaces should be managed with the same discipline as endpoint and identity controls. These systems provide essential connectivity, but they also sit directly in the path of attackers looking for an initial foothold.

Customers should maintain a clear inventory of internet facing systems, confirm ownership, monitor administrative access and prioritise vulnerabilities that are known to be actively exploited. Remote access should be reviewed regularly to ensure it remains necessary, secure and aligned with current business need.

Practical actions include reviewing exposed services, removing unused VPN profiles, enforcing MFA, centralising edge device logs and testing how quickly an affected appliance could be isolated during an incident. NetUtils can support this through firewall and VPN reviews, vulnerability assessment, configuration hardening and managed monitoring.

2. Move from AI policy to AI visibility

AI governance cannot rely on policy alone. Organisations need to understand which AI and cloud applications are being used, what data is being shared and whether usage aligns with business risk appetite.

Rather than blocking AI outright, customers should aim for governed enablement. This means providing approved tools where possible, applying controls to risky activity and giving IT and security teams the visibility needed to make informed decisions.

CASB style controls can help identify sanctioned and unsanctioned cloud applications, classify risk, apply policy based controls on user and device context and provide reporting for leadership teams. This gives customers a practical way to support innovation while protecting sensitive data, compliance obligations and customer trust.

3. Strengthen resilience across suppliers and critical services

The Cyber Security and Resilience Bill is still progressing through Parliament at the time of writing, but customers do not need to wait for final legislation before improving resilience. The direction of travel is clear: organisations are expected to understand critical services, manage supplier dependencies and improve their ability to detect, escalate and recover from cyber incidents.

Customers should identify the digital services that matter most to operations, map the providers that support them and confirm who holds privileged access. They

should also ask providers for evidence of core controls such as patching, monitoring, backup testing, vulnerability management and incident response.

The most important improvement is clarity. Customers should know who is responsible for prevention, monitoring, communication and recovery before an incident occurs. This reduces delay, strengthens assurance and supports more confident decision making during disruption.

4. Build an evidence led security operating rhythm

Cyber resilience is not achieved through one off reviews. It depends on regular checks, clear reporting and visible ownership across infrastructure, applications, suppliers and response processes.

Customers should establish a simple operating rhythm that brings together external exposure reviews, AI and SaaS visibility, supplier assurance, access reviews and incident response testing. This does not need to be complex. The objective is to create a repeatable cycle where risks are identified, decisions are documented and improvements are tracked.

For leadership teams, this creates better evidence of control. For IT and security teams, it provides focus. For customers, auditors and insurers, it demonstrates that cyber risk is being managed proactively rather than reactively.

Together, these recommendations support a more resilient security posture: reduce unnecessary exposure, govern emerging technology safely, clarify provider responsibilities and maintain evidence that critical controls are working.

About NetUtils

Network Utilities Systems Ltd (NetUtils) is a UK based cybersecurity partner helping organisations detect, respond to and recover from the threats that matter most. We combine deep technical expertise with practical security operations from managed detection and response to identity security, endpoint protection, cloud security and incident response planning. Whether you need a trusted extension of your security team or expert support in the hours following a breach, NetUtils provides the clarity and capability to act decisively. Our **Q2 2026 Threat Report** reflects the intelligence and insight we bring to every engagement.

For a detailed consultation and to explore how NetUtils can support your cybersecurity strategy, contact us:

Email: info@netutils.com
Phone: 0208 783 3800
Website: www.netutils.com

Citation ISO Certification Information security management ISO 27001: 2022 REGISTERED
Certificate No:201792013

Citation ISO Certification Quality management ISO 9001: 2015 REGISTERED
Certificate No:201782013

CYBER ESSENTIALS PLUS

Crown Commercial Service Supplier

References

- Palo Alto Networks. **CVE-2026-0257 PAN-OS GlobalProtect Portal and Gateway Authentication Bypass Vulnerability**. https://security.paloaltonetworks.com/CVE-2026-0257
- Rapid7. **Rapid7 Observed Exploitation of PAN-OS GlobalProtect Authentication Bypass Vulnerability CVE-2026-0257**. https://www.rapid7.com/blog/post/etr-rapid7-observed-exploitation-of-pan-os-globalprotect-authentication-bypass-vulnerability-cve-2026-0257/
- Arctic Wolf. **FortiClient EMS Exploited via CVE-2026-35616 to Deliver EKZ Infostealer Disguised as a Fortinet Patch**. https://arcticwolf.com/resources/blog/forticlient-ems-exploited-via-cve-2026-35616-to-deliver-ekz-infostealer-disguised-as-a-fortinet-patch/
- CISA. **Known Exploited Vulnerabilities Catalog**. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- NCSC. **Defending Against China Nexus Covert Networks of Compromised Devices**. https://www.ncsc.gov.uk/news/defending-against-china-nexus-covert-networks-of-compromised-devices
- NCSC. **Cyber Agencies Unveil New Guidelines to Secure Edge Devices from Increasing Threat**. https://www.ncsc.gov.uk/news/cyber-agencies-unveil-new-guidelines-to-secure-edge-devices-from-increasing-threat
- TrustLayer. **Who Do You Trust Now?** https://trustlayer.co.uk/resource/who-do-you-trust-now/
- TrustLayer. **Cloud Access Security Broker CASB Datasheet**. https://trustlayer.co.uk/insight/cloud-access-security-broker-casb-datasheet/
- TrustLayer. **Could a CASB Prevent Your Next Cloud Data Breach?** https://trustlayer.co.uk/resource/blog/could-a-casb-prevent-your-next-cloud-data-breach/
- NCSC. **AI and Cyber Security: What You Need to Know**. https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know
- NCSC. **Shadow IT Guidance**. https://www.ncsc.gov.uk/guidance/shadow-it
- ITPro. **Generative AI Data Violations More Than Doubled Last Year**. https://www.itpro.com/technology/artificial-intelligence/generative-ai-data-violations-more-than-doubled-last-year
- UK Government. **Cyber Security and Resilience Bill Collection**. https://www.gov.uk/government/collections/cyber-security-and-resilience-bill
- UK Government. **Cyber Security and Resilience Bill Factsheets**. https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets
- UK Government. **Summary of the Cyber Security and Resilience Bill**. https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill
- UK Government. **Cyber Security and Resilience Bill: Incident Reporting Factsheet**. https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/incident-reporting
- UK Parliament. **Cyber Security and Resilience Bill: Parliamentary Progress**. https://bills.parliament.uk/bills/4035
- House of Commons Library. **Cyber Security and Resilience Bill Research Briefing**. https://commonslibrary.parliament.uk/research-briefings/cbp-10442/
- Local Government Association. **Cyber Security and Resilience Bill Policy Briefing**. https://www.local.gov.uk/parliament/briefings-and-responses/cyber-security-and-resilience-bill-policy-briefing

Network Utilities (Systems) Ltd

The Larches, Sevenoaks Road, Orpington, Kent BR6 7FB
www.netutils.com | +44 (0)20 8783 3800