Why is Zero Trust Important to your Business?

Cyber attacks in the UK soared from 2.39 million in 2022 to roughly 8.58 million in 2024. Recent statistics show that 32% of businesses experience security breaches or attacks every week, climbing from 25% in 2021. These figures highlight the urgent need for proven strategies that protect data and systems against a range of threats. Adopting a zero trust framework, combined with application and device ringfencing, significantly reduces the risk of successful attacks by verifying every access attempt and isolating potential vulnerabilities.

Below is an overview of key practices: application audit, application control, elevation control, default deny, and ringfencing. When integrated into a broader cybersecurity strategy, these measures ensure that businesses benefit from granular oversight, strict access policies, and effective defensive layers.

Zero Trust

Zero trust dismantles the notion that anything inside a corporate network is automatically trustworthy. Every user, device, and piece of software must continually prove its legitimacy, whether inside or outside the business's network perimeter.

Continuous Verification

Persistent identity checks, such as Multi-Factor Authentication (MFA) and strict access rules, reduce the likelihood of insiders or intruders moving across the network unnoticed.

Least Privilege

Anyone accessing the system—whether employee, contractor, or process—receives only the permissions strictly necessary for their duties. With limited privileges, attackers cannot freely roam even if one account is compromised.

Network Segmentation

Infrastructure is split into isolated segments, so if an attacker breaches one area, other parts remain protected. This division can prevent ransomware or malicious processes from swiftly spreading across the company's entire ecosystem.

Application Audit

An application audit logs all software execution attempts—both successful and denied—providing continuous visibility into how programs are used across the organisation.

Identifying Threats Early:

Real-time or scheduled reviews of the audit trail quickly flag unusual behaviour, such as unfamiliar programs or processes that might indicate a breach.

Improving Accountability:

Administrators can trace user actions if needed, ensuring those who open suspicious files or run high-risk software are spotted and advised.

Optimising Policies:

Detailed usage data helps refine allow-lists or block-lists. Software that is rarely used or appears unauthorised can be investigated and potentially removed.

Application Control

Application control enforces a strict policy that only authorised applications may run. Unverified or unknown software is blocked outright, preventing it from executing in the first place.

Proactive Defence:

Unlike reactive antivirus scanning, a default allow-list approach intercepts malicious code before it runs.

Reduced Malware Spread:

Limiting execution to known, approved software severely constrains the avenues through which ransomware and other malware can spread.

Strengthened Zero Trust:

This feature strengthens the zero trust ethos by eliminating the guesswork of deciding if a program is trustworthy after it starts running.

Elevation Control

Elevation control grants administrative or elevated privileges only for specific applications and tasks, rather than to the entire user account. Privileges are automatically revoked once that action is complete.

Preventing Privilege Escalation:

Attackers often aim to gain administrative rights, enabling them to disable security tools or extract sensitive data. Tightly managing privileges makes this path far more difficult.

Enforcing Least Privilege:

Day-to-day operations rarely require full administrator access. Elevation control aligns with best practice by limiting exposure to potential misuse.

User Efficiency and Security:

Staff can still complete critical tasks under a short-term, tightly controlled permission model without jeopardising the entire environment.

Default Deny

A strict “default deny” policy ensures no application, script, or executable can run unless it is explicitly approved in advance.

Shifting to Prevention:

Traditional anti-virus solutions detect threats once they run; default deny prevents them from running at all if unrecognised.

Neutralising Unknown Threats:

Unknown malware, zero-day exploits, or suspicious scripts are blocked before they can cause harm.

Streamlined Security Checks:

Administrators and security teams know that anything permitted to execute has passed review, reducing guesswork when investigating alerts.

Ringfencing places strict boundaries around applications and devices to control how they communicate with each other or with system resources.

Application Isolation:

If a permitted application is compromised, ringfencing ensures it cannot freely access unrelated network segments or sensitive files.

Device Shielding:

Restricting unauthorised USB devices or suspicious peripherals prevents malicious scripts from launching without detection. Attackers frequently exploit hardware trust gaps, making device ringfencing critical.

Controlling Blast Radius:

Even if attackers gain a foothold in the system, ringfencing limits how far they can spread, effectively containing the damage.

Security Advantages and Organisational Benefits

Comprehensive Visibility:

Combining application audit with continuous monitoring facilitates quick detection of anomalous behaviour or software use.

Fewer Access Points for Attackers:

Application control, elevation control, and default deny create strict policies that limit hacker options for infiltration.

Insider Threat Mitigation:

Zero trust ensures that employees cannot simply wander through a network, and logs detail who accessed which resources.

Regulatory Compliance:

Measures such as these align with the requirements of GDPR, Cyber Essentials, and ISO 27001, ensuring access and data handling remain well-documented and tightly guarded.

Implementation Considerations

Thorough Policy Setup:

Each department's workflows and legitimate software must be clearly identified to avoid blocking essential operations.

Employee and Admin Training:

Adopting "default deny" and strict privilege protocols can be a shift in culture. Clear guidance minimises confusion.

Regular Policy Updates:

Threats constantly evolve, and new applications enter use. Periodic reviews ensure that approvals are current and reflect changing conditions.

TwentyFour's Approach to Zero Trust

Zero Trust and Ringfencing form part of a comprehensive cyber security service, ensuring robust protection for businesses large and small. By integrating software-based controls, in addition to strict policies, and ongoing monitoring, businesses can stay resilient in the face of modern threats. These strategies reflect an industry-wide push to ensure security measures keep pace with rising attack volumes.