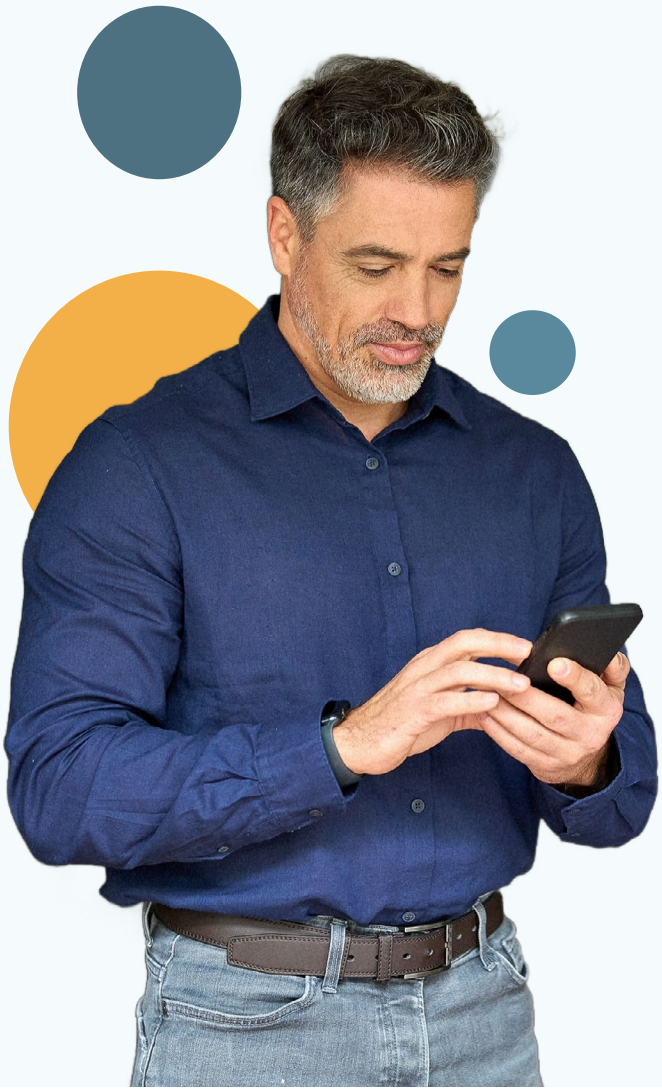
PHOENIX

BeyondTrust iboss rubrik SOPHOS

The state of zero trust in 2026: a roadmap for modern security

Contents



Organisations like yours are operating in a very different security environment than they were even a few years ago.

Your workforce is more distributed, services are increasingly cloud-delivered, and identity-based attacks continue to be more sophisticated. Growth is good, but not when you're outgrowing your security models. It's time to move from traditional, perimeter focused tactics into modern adaptable security.

The concept of zero trust isn't new, but genuine adoption is. There's a wide gap between organisations that have simply ticked the box and those that have actually embedded it into how they operate. Most sit somewhere in the middle, with multi-factor authentication (MFA) rolled out but not fully integrated.

The current threat picture makes this gap hard to ignore. The UK Government's Cyber Security Breaches Survey finds that around half of public sector organisations experience a breach or attack in any given year, with phishing and stolen credentials accounting for the bulk of them. Analysts put compromised identities behind more than 80% of breaches, a figure that keeps climbing. Identity is the perimeter now, whether organisations have built their security around that fact or not.

The good news: closing that gap doesn't mean ripping out what's already there. A phased approach allows real progress without a whole tech reset.

This whitepaper looks at what's driving zero trust decisions in 2026, where most organisations really sit on the curve, and what security leaders can do next.

Why zero trust matters now

For a long time, cyber security was simply about keeping the bad out. Firewalls, network segmentation, VPNs... the thinking was if you kept the walls high enough, you'd be safe. And for a while, when users and systems mostly stayed within defined boundaries, that approach held up well enough. But times have changed.

Hybrid working is now the norm, and essential services are spread across your environment in multiple cloud platforms. Being able to access systems from everywhere is fantastic for productivity, but not so good for cyber security, with the network edge previously defined as "in" and "out" now ceasing to exist. Cyber criminals have adjusted to this change accordingly, now targeting identities as a priority:

- Phishing remains the most reported attack vector in the UK Government's Cyber Security Breaches Survey, affecting the majority of organisations that log incidents
- Security research has shown identity-based attacks growing significantly year on year, pointing to a sustained, deliberate move toward credential-focused intrusion

Zero trust is the practical response to this shift. Instead of extending trust to anything that happens to be inside the network, it applies continuous verification, checking identity, device health, location, and risk signals at every step, not just at the door.

What is zero trust?

Despite widespread discussion, zero trust is still sometimes misunderstood. Some see it as a single product category. Others view it as an all-or-nothing transformation. In reality, it is neither.

Never trust, always verify

Zero trust is built on a simple idea: no user, device, or workload should be trusted by default.

Instead, access decisions are continuously evaluated using signals such as:

- ✓ Verified identity
- ✓ Device posture
- ✓ Location and network context
- ✓ Behavioural risk indicators
- ✓ Least-privilege requirements

This "assume breach" mindset recognises that, in modern environments, preventing every intrusion is unrealistic. What matters is limiting blast radius and detecting suspicious activity quickly.

Zero trust is a strategy, not a product

One of the most common myths is that zero trust can be purchased as a single tool. But effective zero trust requires coordination across identity, endpoint, network, and data controls. What's good is that many organisations have already unintentionally begun this change. Deploying MFA, improving logging, or introducing device compliance policies are all meaningful steps. The opportunity in 2026 is not to start from scratch, but to build on these foundations in a structured way.

The biggest shifts shaping zero trust decisions in 2026

Several structural changes to organisations are accelerating zero trust adoption. Together, they are redefining what "good" security looks like.

Hybrid work has become business as usual

What began as an emergency response has become a permanent operating model. Across councils, healthcare trusts, and central government bodies, hybrid working is now embedded in workforce planning.

This shift has clear benefits for productivity and flexibility. But it also introduces new security considerations:

- Users routinely authenticate from unmanaged networks
- Personal and mobile devices are more common
- Third-party and contractor access has expanded
- VPN infrastructure is under sustained pressure

When location can no longer be treated as a reliable trust signal, security decisions need to be based more on identity and context. This is where zero trust provides value.

Cloud and SaaS sprawl increase the attack surface

Cloud adoption continues to accelerate. Many organisations now operate across a mix of:

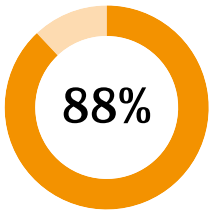
- Microsoft 365 and collaboration platforms
- Line-of-business SaaS applications
- Multiple public cloud environments
- Legacy on-premises systems

While this delivers agility, it also fragments visibility. Without strong identity governance and access controls, this sprawl can create blind spots. Data may reside in multiple locations, access policies may vary, and shadow IT can emerge.

Identity is the new security perimeter

If one trend defines the current threat landscape, it is the rise of identity-focused attacks.

Research has found that stolen credentials allow attackers to bypass perimeter defences. In 2025:



of “Basic Web Application Attacks” used stolen logins.

Attackers increasingly prefer phishing, token theft, and session hijacking because they allow adversaries to appear legitimate once inside.

Common public sector challenges include:

- Inconsistent MFA coverage
- Over-privileged accounts
- Dormant or orphaned identities
- Limited continuous monitoring

When an attacker logs in with valid credentials, traditional network controls offer limited protection. Zero trust directly addresses this risk by continuously validating identity and enforcing least privilege.

The growing impact of AI-enabled threats

AI is beginning to influence both sides of the cyber security equation. While defensive tools are improving, attackers are also using AI to scale and refine their techniques.

We've already seen:

- More convincing phishing emails
- Faster reconnaissance activity
- Automated password spraying attempts
- Improved social engineering tactics

Unlike traditional security models that treat authentication as a one-time gate, zero trust principles are built for exactly this kind of automated threat activity. Every session is continuously verified; credentials alone are never enough.

Where organisations are vs. **where they need to be**

We know zero trust is important.

Unfortunately, that doesn't make zero trust practises automatically rolled out in tech environments.

Progress varies widely, with some organisations making significant strides in identity governance and conditional access. Others are still working through outdated legacy infrastructure. Most sit somewhere in between.

The present

Zero trust is no longer theoretical. MFA is widely deployed. Monitoring has improved, particularly across cloud services. Conditional access policies are emerging, often focused on higher-risk users or critical systems.

Yet in many environments, authentication is treated as a gateway: once credentials are verified, access can remain broad. VPNs still provide wide network access.

Device posture checks may be inconsistent, particularly for third parties. Access reviews are often periodic rather than driven by real-time risk.

Security controls exist, but they aren't always integrated or adaptive.

This reflects the reality of managing complex estates shaped by legacy platforms, constrained budgets, and limited specialist capacity.

The future

So, what changes at higher levels of maturity? Identity sits at the centre of every access decision. MFA is universal. Conditional access evaluates multiple signals simultaneously:

- Device compliance
- Behaviour
- Location
- Privilege level
- Session risk

Permissions follow least-privilege principles and adjust in real time if risk changes. A routine login flows seamlessly. The same credentials from an unfamiliar device or anomalous location prompt additional verification or restriction.

Visibility is unified across identity, endpoint, and cloud environments, enabling contextual decision-making and greater automation of routine controls.

Trust is no longer assumed at login. It is continuously validated.

Common barriers slowing zero trust **progress**

If the direction is clear, why do organisations sometimes stall?

1

Legacy infrastructure often tops the list

Critical systems cannot always be modernised quickly, meaning zero trust controls must work around existing platforms

2

Tool sprawl is another **common issue**

Over time, security solutions accumulate, creating fragmented visibility and integration gaps that limit contextual decision-making

3

Skills and capacity constraints also play a role

Security teams are stretched, and without a phased roadmap, zero trust can feel complex to implement

4

Budget cycles and organisational silos can slow coordination

Zero trust spans multiple teams and funding streams, requiring alignment across identity, endpoint, network, and governance functions

The good news?

These barriers are well understood, and entirely solvable with the right approach.

A practical roadmap for zero trust adoption

Several structural changes to organisations are accelerating zero trust adoption.

Together, they are redefining what "good" security looks like.

Build visibility and understanding

Start by establishing a clear picture of the current environment.

This typically includes:

- Comprehensive identity inventory
- Device visibility and classification
- Mapping of critical access paths
- Improved centralised logging

Visibility creates the foundation for informed policy decisions.

Strengthen identity foundations

Identity controls usually deliver the fastest risk reduction.

Priority actions often include:

- Universal MFA deployment
- Conditional access rollout
- Privileged access management
- Regular access reviews and governance

At this stage, many organisations see immediate security gains.

Introduce context-aware access

With identity foundations in place, organisations can begin enforcing richer policies based on context.

Typical steps include:

- Device compliance enforcement
- Risk-based authentication
- Enhanced third-party access controls
- Gradual reduction of legacy VPN dependence

Move toward continuous verification

The most advanced environments focus on automation and continuous improvement.

Capabilities may include:

- Behaviour analytics
- Automated response playbooks
- Integrated security telemetry
- Continuous policy tuning

Importantly, organisations do not need to reach this stage immediately to realise meaningful benefits.

We're here to support your **zero trust journey**

With the right partner, progress can be structured, measurable, and aligned to real-world constraints.

Phoenix works alongside UK public sector teams to:

- Assess current zero trust maturity
- Prioritise high-impact improvements
- Design pragmatic architectures
- Support implementation and integration
- Provide ongoing managed security services

We recognise that every organisation starts from a different place, and that sustainable progress matters more than rapid but fragile change.

Get in touch **today**

For more information on adopting zero trust strategies in your organisation, book a free consultation with a specialist today.

Get in touch now

Alternatively, you can contact us at hello@phoenixs.co.uk or call us on 01904 562200

PHOENIX

01904 562200
www.phoenixs.co.uk
hello@phoenixs.co.uk