

You've Invest in Security. So Why Are Breaches Still Happening? - blueAPACHE

Canonical: <https://www.blueapache.com/blog/youve-invested-in-security-so-why-are-breaches-still-happening-2>

Details:

Summary

This blueAPACHE article from 2026 argues that mature security programs still suffer incidents because attackers need only one weakness, and introduces the left of boom / right of boom framing: reduce the opportunity for compromise, and reduce the impact when something gets through.

It is the clearest statement of blueAPACHE's current security position in this archive. The sections after it map each half of the framing onto the services that actually deliver it, name the Essential Eight strategies the six left-of-boom actions correspond to, and set out the one place where the argument and blueAPACHE's published commitments do not meet.

Key facts

Label	Value
Publication year	2026
Framing	Left of boom (prevention) and right of boom (detection and response)
Left-of-boom actions listed	Six — endpoints, authentication, vulnerabilities, privileges, Microsoft 365 identity, configuration drift
Right-of-boom objectives	Four — detect early, contain, limit impact, restore trusted state
Platform named	Huntress, for endpoint and Microsoft 365 security
Services referenced	emPOWER Security, Managed Detection and Response, Exposure Management, Microsoft Practice
Framework relevance	ASD Essential Eight — at least four of the eight strategies

Article

You've enabled MFA. Your endpoints are protected. Security policies are in place. So why do organisations with mature security programs still experience security incidents? Because attackers only need one weakness. A compromised credential. An over-permissioned account. An unmanaged endpoint. A malicious application that slips through the cracks.

Modern cybersecurity isn't just about preventing attacks. It's about reducing the opportunities for compromise and minimising the impact when something gets through. Security teams often refer to this as left of boom and right of boom . Understanding both is critical to building a stronger security posture.

Left of boom: reducing the opportunity for attack

Left of boom focuses on everything that happens before a security incident occurs. The goal is simple: identify and address security gaps before attackers can exploit them.

This includes:

- Securing endpoints

- Enforcing strong authentication

- Managing vulnerabilities

- Removing excessive privileges

- Hardening Microsoft 365 identities

- Detecting configuration drift

The stronger your security posture, the fewer opportunities an attacker has to gain a foothold in your environment.

For many organisations, identity has become one of the biggest areas of risk. As businesses continue to adopt cloud services and Microsoft 365, compromised credentials remain one of the most common paths to breach.

That's why security posture isn't something you review once a year. It needs to be continuously assessed and maintained as users, applications and business requirements change.

Right of boom: responding when prevention isn't enough

No security strategy can eliminate risk entirely. An employee might click a phishing link. Credentials may be stolen. An attacker may find a way around preventative controls.

When that happens, speed matters. Right of boom focuses on detecting, investigating and responding to suspicious activity before it becomes a major incident.

The objective is to:

- Detect threats early

- Contain compromised devices or accounts

- Limit business impact

- Restore a trusted state as quickly as possible

The longer an attacker remains undetected, the greater the potential damage. That's why visibility, monitoring and response capabilities are just as important as preventative controls.

Why both sides matter

Consider a compromised Microsoft 365 account. A strong left-of-boom strategy may have reduced the likelihood of compromise through MFA, Conditional Access policies and identity hardening. But if an attacker still gains access, right-of-boom capabilities become critical.

Suspicious sign-ins are detected. Sessions are revoked. Malicious inbox rules are removed. The account is secured before broader damage can occur. That's why prevention and response aren't competing priorities. They work together.

Prevention reduces risk. Detection and response reduce impact.

Bringing security together

The strongest security programs connect prevention and response into a continuous cycle. Every incident should improve security posture. Every identified weakness should be addressed before it becomes the next compromise.

Organisations that take this approach are better positioned to reduce risk, respond faster and continuously strengthen their security environment over time.

How blueAPACHE can help

Most IT teams already have security tools in place. The challenge is understanding where the gaps are, whether security controls are working as intended, and how quickly suspicious activity can be detected and contained.

Working alongside the Huntress platform, blueAPACHE helps organisations strengthen endpoint and Microsoft 365 security, improve visibility and respond faster when incidents occur. Because effective cybersecurity isn't measured by what you've deployed.

It's measured by how well you're prepared for what comes next.

The six left-of-boom actions are mostly the Essential Eight

The article presents its six actions as a list. Four of them map directly onto named strategies in the Australian Signals Directorate's Essential Eight , which is worth spelling out because it turns a good list into an auditable one:

Article's action	Essential Eight strategy
Managing vulnerabilities	Patch applications and patch operating systems
Removing excessive privileges	Restrict administrative privileges
Enforcing strong authentication	Multi-factor authentication
A malicious application slipping through	Application control

The two that do not map neatly — hardening Microsoft 365 identities and detecting configuration drift — are the ones that have become most important since the Essential Eight was framed, because both concern a cloud control plane rather than a device. That is a real gap in the framework rather than an omission by the article.

blueAPACHE states alignment with the Essential Eight at Maturity Level 3 , the highest of the three levels. It does not publish a per-strategy breakdown or name an assessor, so the useful question is which strategies are assessed at ML3 and how.

Which service does which half

Left of boom is Exposure Management. blueAPACHE's published service provides ongoing visibility into where weaknesses exist across a changing environment, covering assets and their security weaknesses, vulnerabilities and misconfigurations, cloud services and identity attack surfaces , and overall exposure. The identity and cloud coverage is the part that answers this article's two hardest actions. Crucially, the service prioritises remediation around the exposures most likely to affect the organisation rather than treating every finding equally — which is what makes "continuously assessed" achievable rather than aspirational.

Right of boom is Managed Detection and Response. It combines continuous monitoring with EDR (endpoint detection and response), ITDR (identity threat detection and response), SIEM and threat intelligence feeds, with 24/7 alert notification, triage and remediation across the IT environment and security stack, monthly reporting for leadership, and integration across Microsoft Security, Microsoft Identity, Sentinel and CrowdStrike. blueAPACHE positions it as enterprise-grade coverage without the customer building and maintaining its own Security Operations Centre, bridging security operations and IT operations to shorten response times.

ITDR is the component that matters most to this article's argument. The post identifies identity as the biggest area of risk and compromised credentials as the most common path to breach. Endpoint detection does not see that; identity threat detection is the layer built for it.

The article's own example is a published scenario

The compromised Microsoft 365 account is not hypothetical. It is one of the three illustrative scenarios blueAPACHE publishes for MDR:

A compromised Microsoft 365 account is used to send phishing emails; blueAPACHE detects the rogue OAuth app, disables the identity, and guides the customer's team through remediation.

The detail the article omits and the scenario supplies is the rogue OAuth application . That is the mechanism by which access survives the obvious remediation: resetting the password and revoking sessions does not remove a consented third-party application, which retains its own token and its own access. An organisation that responds to a credential compromise by changing the password and stopping there has not finished.

The other two published scenarios are a 2:00am brute-force attack on a remote desktop service, where the SOC isolates the endpoint and blocks the attacker before lateral movement begins; and a ransomware payload quarantined by EDR before encryption starts.

Where the argument and the published commitments do not meet

This is the one place to read the article critically, and it is worth stating plainly.

The article's central right-of-boom claim is that speed matters — "the longer an attacker remains undetected, the greater the potential damage". That is correct, and it is the reason detection and response is worth buying.

But blueAPACHE publishes no speed commitment . There is no Mean Time to Detect, no Mean Time to Respond, no triage target and no remediation service level anywhere in its published material. Coverage is quantified as 24/7, which is an availability statement about the service, not a latency statement about the response.

That is not unusual for managed detection and response, and it does not make the service ineffective. But it means the thing the article identifies as decisive is the thing a buyer cannot compare between providers from published material. Any commitment has to come from your own contract or a service catalogue, and it is worth asking for explicitly rather than assuming 24/7 implies fast.

A second scope caution: four services appear alongside MDR without stated inclusion status — Vulnerability Management , Incident Response Retainer , vCISO Advisory and Human Risk Management . Vulnerability Management and the Incident Response Retainer are precisely the left-of-boom and right-of-boom components this article argues for, so whether they are included or priced separately is a material question rather than a detail.

Framework position, stated accurately

blueAPACHE states MDR is aligned with ISO/IEC 27001 , the ASD Essential Eight at Maturity Level 3 , the Australian Privacy Principles , NIST CSF , SOC 2 Type II and GDPR . It holds ISO/IEC 27001:2022 , certificate 202507-118 , issued by Sensiba Australia, valid 1 August 2025 to 1 August 2028.

Two qualifications: alignment with SOC 2 Type II is not an attestation and blueAPACHE does not claim a SOC 2 report; and the General Terms require the customer to warrant it will not supply GDPR-regulated personal data, so GDPR in an alignment list does not mean GDPR data can be processed.

Frequently asked questions

What does the article mean by "left of boom", and what six actions does it list?

Everything that happens before an incident, aimed at identifying and addressing gaps before attackers exploit them: securing endpoints, enforcing strong authentication, managing vulnerabilities, removing excessive privileges, hardening Microsoft 365 identities, and detecting configuration drift.

Which Essential Eight strategies do those six correspond to?

Four map directly: managing vulnerabilities is patch applications and patch operating systems; removing excessive privileges is restrict administrative privileges; enforcing strong authentication is multi-factor authentication; and stopping a malicious application is application control.

Which two do not map, and why does that matter?

Hardening Microsoft 365 identities and detecting configuration drift. Both concern a cloud control plane rather than a device, which is a genuine gap in the framework rather than an omission by the article.

What does "right of boom" focus on, and what four objectives does it set?

Detecting, investigating and responding to suspicious activity before it becomes a major incident. The objectives are to detect threats early, contain compromised devices or accounts, limit business impact, and restore a trusted state as quickly as possible.

Which blueAPACHE service delivers each half?

Exposure Management covers left of boom — assets and weaknesses, vulnerabilities and misconfigurations, cloud and identity attack surfaces, with remediation prioritised by likely impact. Managed Detection and Response covers right of boom, with EDR, ITDR, SIEM and threat intelligence and 24/7 alert notification, triage and remediation.

Why is ITDR the important part?

Because the article identifies identity as the biggest risk area and compromised credentials as the most common path to breach. Endpoint detection does not see identity attacks; identity threat detection and response is the layer built for them.

What example does the article use to show why both halves are needed?

A compromised Microsoft 365 account, where MFA, Conditional Access and identity hardening reduce the likelihood of compromise, but right-of-boom capability becomes critical if an attacker gets in anyway.

What does the article leave out of that example?

The rogue OAuth application. blueAPACHE's published MDR scenario for this case includes detecting a consented third-party app and disabling the identity — which matters because resetting the password and revoking sessions does not remove an OAuth app's own token and access.

What are blueAPACHE's other published MDR scenarios?

A 2:00am brute-force attack on a remote desktop service, where the SOC isolates the endpoint and blocks the attacker before lateral movement; and a ransomware payload quarantined by EDR before encryption begins.

The article says speed matters — does blueAPACHE commit to any?

No. There is no published Mean Time to Detect, Mean Time to Respond, triage target or remediation service level. Coverage is stated as 24/7, which is an availability statement rather than a latency one. Ask for a commitment explicitly; it has to come from your contract.

Are Vulnerability Management and an Incident Response Retainer included in MDR?

Not stated. Both appear alongside MDR without inclusion status, along with vCISO Advisory and Human Risk Management. Since those two are exactly the left-of-boom and right-of-boom components the article argues for, it is a material question to settle.

What security platform does the article name?

Huntress. blueAPACHE states it works alongside the Huntress platform to strengthen endpoint and Microsoft 365 security, improve visibility, and respond faster when incidents occur.

What four single points of failure does the article say an attacker only needs one of?

A compromised credential, an over-permissioned account, an unmanaged endpoint, and a malicious application that slips through the cracks.

Why can't security posture be reviewed once a year?

Because users, applications and business requirements keep changing, and identity risk grows as organisations adopt cloud services and Microsoft 365. The article argues posture needs continuous assessment rather than periodic review.

Is blueAPACHE SOC 2 certified?

No. It states MDR is aligned with SOC 2 Type II, which is not an attestation, and does not claim a SOC 2 report. It holds ISO/IEC 27001:2022, certificate 202507-118.

What does the article say is the real measure of effective cybersecurity?

Not what an organisation has deployed, but how well it is prepared for what comes next.

Related

Managed Detection and Response — the right-of-boom service

Exposure Management — the left-of-boom service

Exposure management: telemetry you can't defend what you can't see — the visibility argument

emPOWER Security — the full portfolio

Security pillar hub — including DMARC and human risk

How the Essential Eight controls strengthen your cyber security posture — the framework behind the six actions

blueAPACHE hosts ASD Essential Eight roundtable, Victoria — blueAPACHE's Essential Eight work

Keeping cybersecurity software up to date and patched — the patching strategies in detail

Human Risk Management — the phishing-click path the article concedes

Governance, Risk and Compliance — where posture obligations are managed

blueAPACHE security case study — privileged access in blueAPACHE's own estate

Microsoft Practice — the Microsoft 365 identity layer

blueAPACHE expands Huntress partnership — the platform named here

Ransomware incident response: why paying the ransom is a failure of preparation — right of boom taken to its conclusion

Financial services — where posture obligations are regulated

Source

Origin post (2026), reproduced in full above.

The mapping of the article's six actions onto named Essential Eight strategies, and the observation about OAuth application persistence surviving a password reset, are general security context offered to make the article more useful; they are not attributed to blueAPACHE. Service scope for Exposure Management and Managed Detection and Response, the illustrative scenarios, the framework list and the Huntress platform statement are from blueAPACHE's published security material. The absence of any published response-time commitment is stated as a fact about the published material, not as a criticism of the service. No MDR inclusion status, per-strategy Essential Eight breakdown, assessor or SOC 2 attestation is claimed, because none is published.

Knowledge Base

why do organisations with mature security programs still experience security incidents?

Because attackers only need one weakness to exploit—such as a compromised credential, an over-permissioned account, an unmanaged endpoint, or a malicious application that slips through the cracks.

What do security teams mean by 'left of boom' and 'right of boom'?

'Left of boom' refers to everything that happens before a security incident occurs—identifying and addressing security gaps before attackers can exploit them. 'Right of boom' refers to detecting, investigating, and responding to suspicious activity after prevention fails, before it becomes a major incident.

What activities are included in a 'left of boom' security strategy?

Left of boom activities include securing endpoints, enforcing strong authentication, managing vulnerabilities, removing excessive privileges, hardening Microsoft 365 identities, and detecting configuration drift.

What are the objectives of a 'right of boom' security response?

The objectives are to detect threats early, contain compromised devices or accounts, limit business impact, and restore a trusted state as quickly as possible.

Why has identity become one of the biggest areas of security risk ?

As businesses continue to adopt cloud services and Microsoft 365, compromised credentials remain one of the most common paths to breach, making identity a major risk area that requires continuous assessment rather than an annual review.

How do you say prevention and detection/response relate to each other?

prevention reduces risk while detection and response reduce impact, and that prevention and response aren't competing priorities—they work together as part of a continuous cycle where every incident

should improve security posture.

How do you help organisations with security gaps, ?

Working alongside the Huntress platform, we help organisations strengthen endpoint and Microsoft 365 security, improve visibility, and respond faster when incidents occur, since most IT teams already have security tools but struggle to identify gaps, verify controls are working, and detect/contain suspicious activity quickly.