inforcer

Proving the value of the unseen

How to create a profitable MSP practice unifying left and right of boom security

Table of contents

01. Why is it so hard to sell proactive tenant management?

02. What are the problems with the ways MSPs currently show value?

03. Why is prevention alone no longer enough?

04. 3 ways to win cyber security business as an MSP

05. How to win new business and demonstrate value with inforcer TDR

06. How to upsell tenant management with inforcer TDR

07. It's time to prove the value of the unseen

01.

Why is it so hard to sell proactive tenant management?

In the cyber security sphere, the terms ‘left of boom’ and ‘right of boom’ are used to describe different approaches to dealing with cyber threats.

Left of Boom

Proactive, preventative strategies and measures that aim to stop cyber security incidents before they occur.

Examples include:

- Microsoft 365 policy configuration and drift monitoring
- Ongoing Microsoft 365 tenant hardening
- User education and awareness



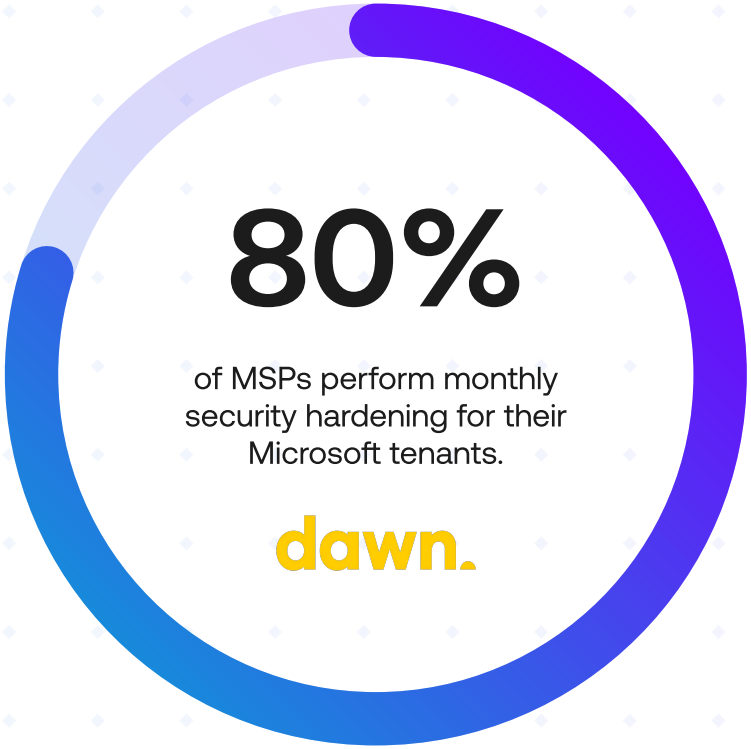
Right of Boom

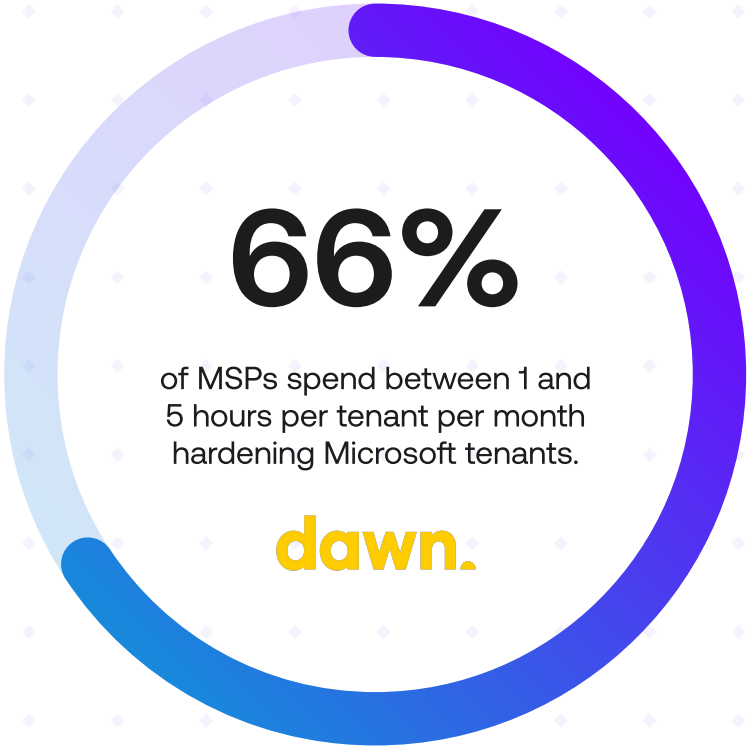
Reactive recovery strategies and actions that contain cyber breaches and threats after they have already occurred.

Examples include:

- Real time threat detection
- Behavioural profiling
- Automated threat containment and response

01. Why is it so hard to sell proactive tenant management?





Are you showing the value of the time you are spending on this essential security work?

For MSPs, it is easy to understand the importance of left of boom security strategies. The Microsoft 365 tenant is now where day-to-day IT administration occurs – and therefore is the greatest attack surface. Properly configuring Microsoft 365 security policies, limiting access where appropriate, monitoring for policy drift, and continually hardening the tenant provides customers with a strong frontline defense against rapidly evolving threats.

The problem?

Customers struggle to see the value of this work.

Security actually that works just looks like...nothing happened. When you quietly contain a compromise, the customer doesn't experience any disruption. There's no outage and no evidence of what you've achieved.

It can be extremely difficult for MSPs to explain the value of all this (very necessary) hard work. Most SMB customers aren't all that tech-savvy. You're doing your job, but customers are questioning why they're being charged for work they can't see.

Frustrating, right?

On the other hand, it's easier to show the value of right of boom security. Here's a threat that you experienced, and here's how we contained it. Clear cut value that's easy to explain and quantify.

Of course, this doesn't mean you should just disregard left of boom security and let your customers get breached. But you do need a strategy to show your value more effectively so you can retain customers, win upsell, secure new business, and scale your MSP.

01. Why is it so hard to sell proactive tenant management?

02.

What are the problems with the ways MSPs currently show value?

Traditionally, MSPs show their value by sending reports, having regular check-ins with customers, and holding Quarterly Business Reviews (QBRs). These are all good strategies, but they need to be executed properly to have a real impact.

The problem with most MSP reporting is that it is too technical for customers to understand. Knowing your audience is essential. Key stakeholders such as business owners and commercial directors care about productivity, efficiency, and revenue. Security is only important to them insofar as it enables them to keep working effectively. These important decision makers won't usually understand the significance of specific policy updates and fixes. Overloading your reports with technical detail and jargon is a sure fire way to ensure it is disregarded by most SMB decision makers.

You need to take a different approach.

03.

Why is prevention alone no longer enough?

Reporting isn't the only issue. The cyber security landscape is now changing faster than ever before, meaning it simply doesn't make sense to silo left and right of boom security measures. Both contribute to a comprehensive and effective cyber security strategy.



Identity is the new perimeter

As remote work is now the standard, login attempts can be made by anyone, at any time, from anywhere in the world. Breaches are often invisible: once a malicious actor has penetrated your customers' perimeter, they can lurk for months to gain the information they need before finally making their move.



No tenant is 100% secure

Security has changed significantly in the past few years, with the rise of AI giving practically anyone the potential to become a hacker. Attacks are harder to spot, constantly evolving, and almost impossible to prevent entirely, even when prioritizing preventative defenses.

Laying the best possible defenses is key but, as mentioned, the value of preventative security is hard to explain to customers. It is essential to have a responsive strategy in place in the eventuality that an attack makes its way through.

Combining left and right of boom security strategies will provide your customers with the strongest security posture, and differentiate yourself from those only offering one set of services. Win-win.

04.

3 ways to win cyber security business as an MSP



Highlight competitor gaps

In an already oversaturated market, standing out is essential. The sharpest way to differentiate isn't actually to talk about your competitors at all, it's to expose the gaps in what your prospect is getting right now. Most businesses don't know what their current provider is missing until someone shows them - so show them.

Are they only getting antivirus and backup when they should have continuous tenant monitoring? Is their Microsoft 365 tenant properly configured? Is policy drift being checked daily, weekly, monthly, or never? Has their threat detection moved beyond identity, or stopped there? A simple security gap assessment turns "we're different" into "here's the gap in your protection right now", and that's a much harder thing to ignore. Find the gap your market keeps leaving open, and lean into it.



Demonstrate your specific expertise

Finding the gap gets you in the room but proving you can fill it wins the business. This is where you need to show evidence, because decision makers have heard "we're the experts" from every MSP that's ever pitched them.

Don't tell them, show them. Are your accreditations doing the talking, whether that's Cyber Essentials Plus, ISO 27001, or your Microsoft Solutions Partner status? Is there a recognized framework behind your approach, like NIST CSF or CIS, so it's clear you're structured rather than winging it? Can you point to a real customer story - a breach you caught, a misconfiguration you closed, a security posture you turned around? Expertise isn't just what you claim, it's what you can back up.



Make your value understandable to decision makers

You can run the tightest security operation possible, but if the person paying for it doesn't understand what they're getting, they aren’t going to sign the contract.

You need to respond to what decision makers care about: productivity, profitability, and reducing risk. Are you translating what you do into what it actually means for their business, or burying it in acronyms? When you report, does it read like an update a board could follow, or a log file only your team understands? Are you checking in regularly, not just when something's gone wrong, so they always know where they stand? And do they see a person on the other end, someone who picks up and takes ownership, rather than a faceless service they're quietly unsure about?

Security is bought on trust as much as capability. Make it easy to understand, and you make it easy to say yes.

05.

How to win new business and demonstrate value with inforcer TDR

inforcer TDR goes beyond the capabilities of a standard threat detection and response tool. Its reporting functionality allows you to **demonstrate your ongoing value** at every QBR or check-in with customers, and position yourself as a strong, secure, and attractive partner to prospects too.

Remember the best practices for winning cyber security business? inforcer TDR maps its reporting to enable you to highlight competitor gaps, demonstrate ongoing value, and make your actions clear and explainable to every stakeholder.

You can walk into every quarterly review and renewal conversation with a documented record of the threats you've caught and contained, turning invisible work into a **clear commercial case**.





Demonstrate your security value with a real-time threat map

Make threats real for customers by showing them a highly visual, real-time threat map. Clearly demonstrate the extent of the threat landscape by showing customers a live view of activity and attacks, and highlighting threat origins and patterns. As an MSP, you can have a multi-tenant or per customer view and filter by threat type to make things even clearer. Adding real evidence to a QBR or sales call will help you drive the importance of your security services more powerfully than ever before.



Highlight competitor gaps with retrospective forensics

inforcer TDR can ingest up to the last six months of historical Microsoft 365 logs, revealing breaches and threats that were already present in a tenant even before the customer came onboard. It's the ultimate presales tool: you can show a prospect exactly what's been happening in their environment, and highlight the threats other providers have missed. Position yourself as more proactive, and security conscious than your competitors without needing to badmouth them.



Make your value understandable with plain-English attack narratives

inforcer TDR generates reports where every threat is explained in clear, non-technical language: what happened, who was affected, and what was done about it. The reports show the preventions and detections you've delivered over time, per customer. Hand a threat audit to a business owner and they'll understand the risk and the value of your service even without a security background. Eliminate jargon, confusion, and misunderstanding and focus in on what really matters: results.

06.

How to upsell tenant management with inforcer TDR

It's all very well being able to show the value of right of boom services. Threat detection and response has always been more comprehensible to customers due to the visibility and immediate impact of breaches that slip through.

To set yourself apart in the cyber security space, you need to be able to use your right of boom security successes to **sell the value of preventative left of boom security**. You need to create a unified cyber security sales loop.

inforcer TDR helps you to do just this by making the value of prevention visible.

After an incident, you can show customers exactly:



How the attack happened



Where additional protections could reduce future risk



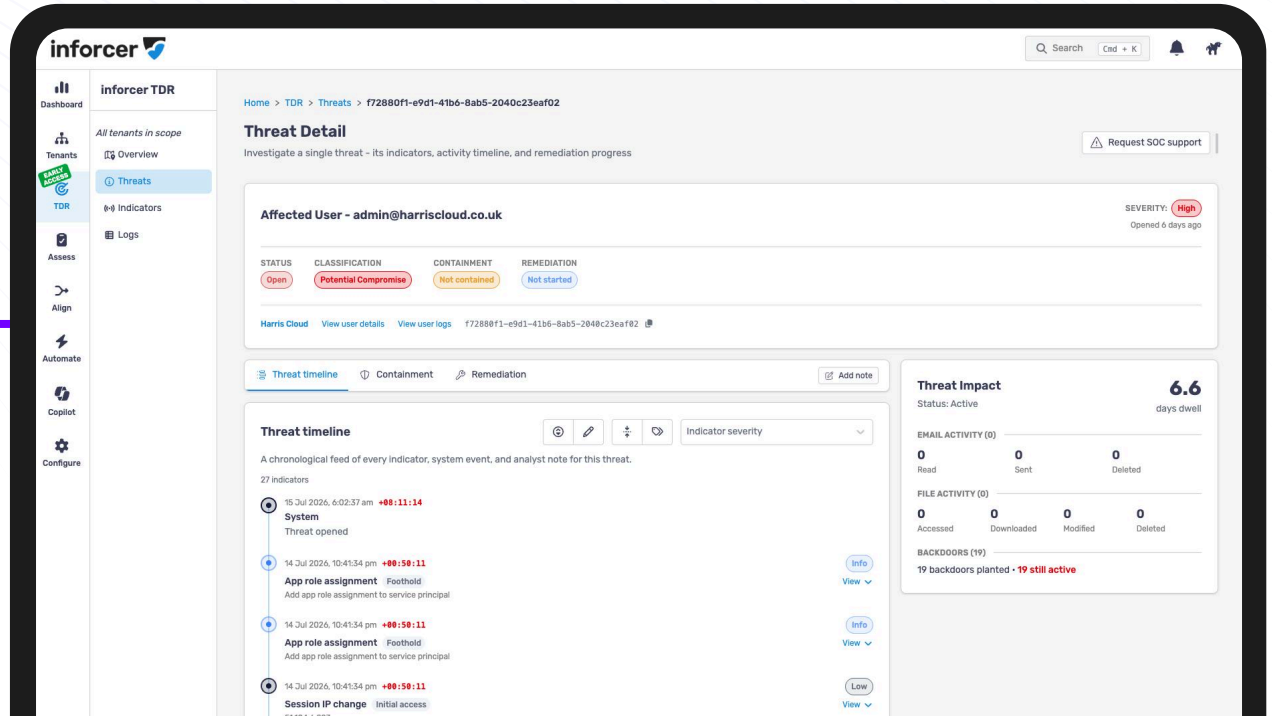
Which specific policy configurations would strengthen their security posture



How ongoing Microsoft 365 management and monitoring can help prevent similar incidents

Instead of simply responding to threats, you can use real-world incidents to **demonstrate the value of proactive security services**. Imagine being able to say to a customer ‘look at this threat we just contained. If you had switched on these three security policies, it could have been prevented.’ By actually seeing the threat that got through, the value of the configuration needed to prevent it in future becomes far more tangible to the end customer. Upselling preventative services has never been easier.

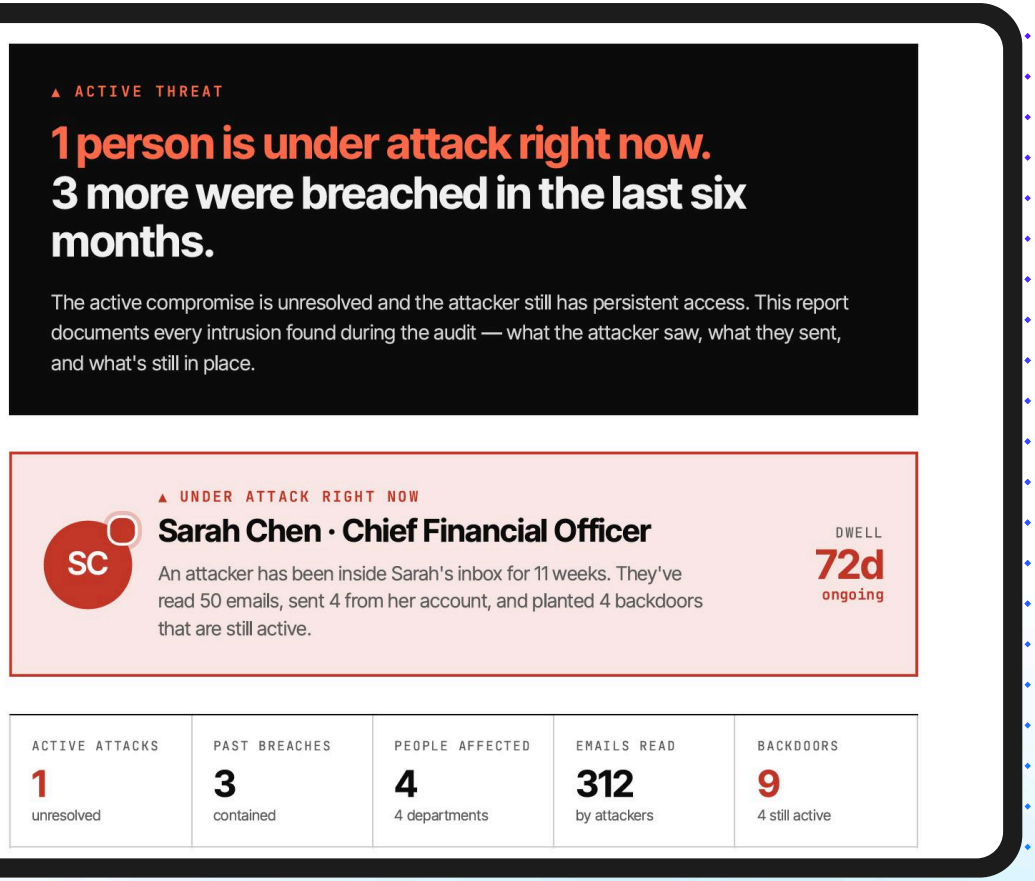
Better yet, you can execute the necessary policy configurations and tenant hardening from within the same **centralized platform**. Just focusing on threat detection without further prevention fails to solve the underlying problems, resulting in more noise for you to deal with. With inforcer TDR, you will be alerted when attackers break in, shown how to prevent those threats in the future, and provided with the tools to deploy those fixes across all of your tenants in minutes.



06. How to upsell tenant management with inforcer TDR

07.

It’s time to prove the value of the unseen



Your hard work has gone unrecognized for too long.

Want to unlock more profitability from cyber security for your MSP? Combining left and right of boom security strategies is key.

Try inforcer today to create an end-to-end security service that customers actually understand and value. Unify prevention, detection, and response with continuous tenant management in a single security platform. Make your services scalable, repeatable, and, most importantly provable with enhanced reporting features.

Download report template

See inforcer TDR in action

inforcer