SENSE ON

From complexity to clarity:

A guide to unified security for IT and security teams

Introduction.

Complexity is the enemy.

Security complexity worsens data breach outcomes more than anything else.

According to the IBM Cost of a Data Breach Report 2024, **security system complexity is the number one factor that increases the average breach cost**.

It also makes breaches more likely. Microsoft writes that organisations with 16+ point tools are 2.8 times more likely to experience a data security incident.

Yet, when we researched IT leaders' attitudes earlier this year, we found that the vast majority of security buyers are looking to make their security operation centres (SOCs) even more complex.

In a 2023/2024 SenseOn study,

78% of UK and Irish respondents believed that more cybersecurity tools lead to better protection

40% held this belief strongly.

Why do organisations want more tools in their SOCs, which by default make their environments more complex to manage, even though security system complexity is known to increase breach costs?

Our take is that security leaders are chasing the "good kind of complexity."

They want—and rightly so—the risk reduction that comes with layered defences. Unfortunately, they often end up with the bad kind of complexity as a result, i.e., analysts trying to investigate events across half a dozen different management consoles.

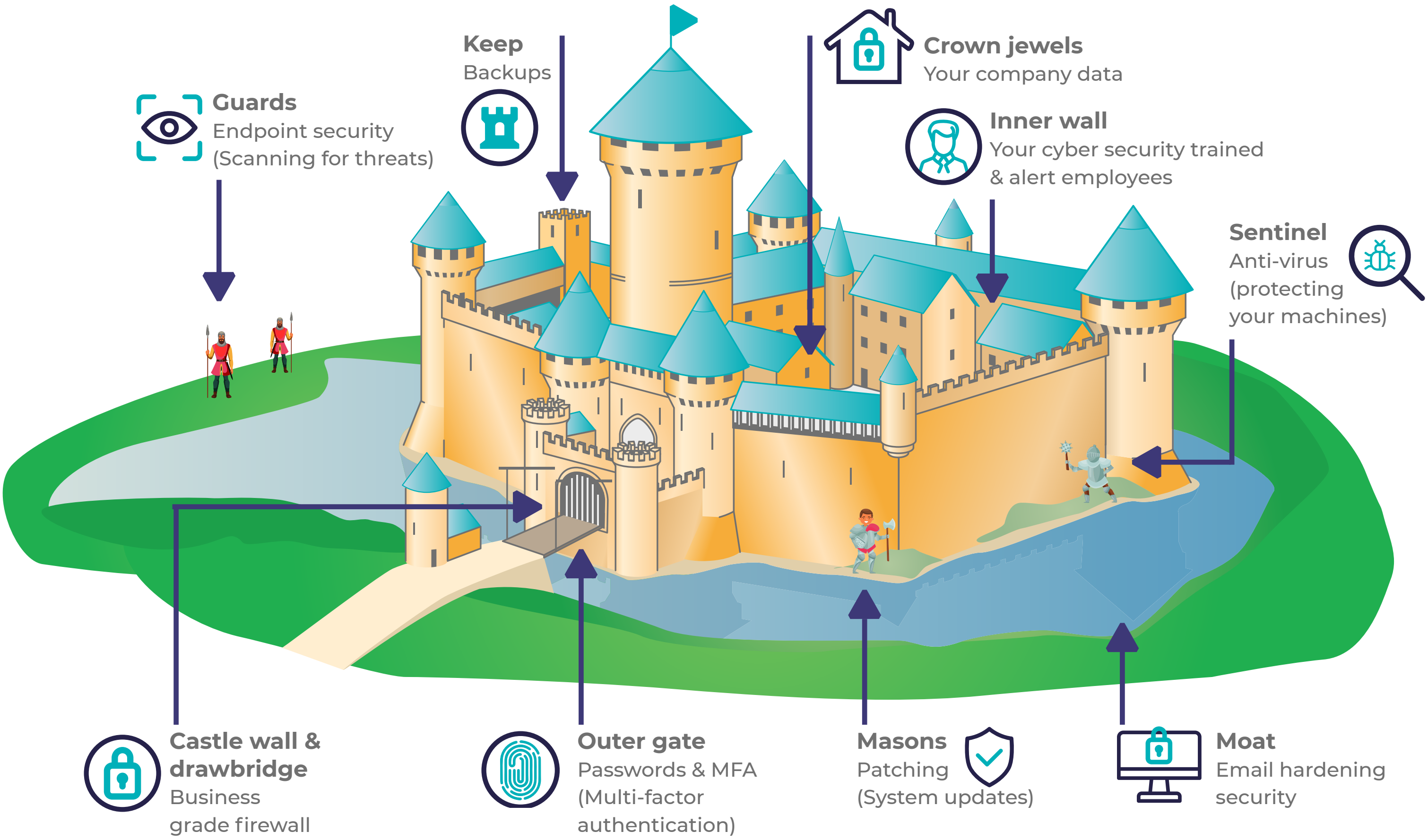
We built SenseOn so security teams could avoid complexity challenges while getting all the benefits of a layered security approach.

In this guide, we tap into our experience to show you how to spot, prevent, and fix a destructively complex security environment.

Good Complexity Versus Bad Complexity

Security system complexity is not, by default, a bad thing.

Multiple security measures at various levels (such as firewalls, intrusion detection systems, encryption, and access controls) create complexity for attackers.



An endpoint compromised by a Cobalt Strike loader persisting in memory (which is not scanned by antivirus) could still be triaged if the threat is picked up by another layer (like an endpoint detection and response tool) that scans memory.

Or, it might be isolated from the rest of the network when a network detection and response (NDR) solution notices that the compromised device is sending suspicious traffic outside your environment.

Multi-layered defence is essential

In 2024, no individual detection method is enough.

Over 30% of all threats observed in a recent meta-analysis of 2024 April - June threat reports were designed to bypass typical signature-based antivirus (AV) defences.

Almost every ransomware attack will now involve Cobalt Strike, which hides in device memory, and fileless attacks that do not involve malware (e.g., insiders exfiltrating data) are becoming more common.

Fortunately, deploying control layers beyond just an AV is proven to prevent the vast majority of cyber-attacks.

But no one needs layered management.

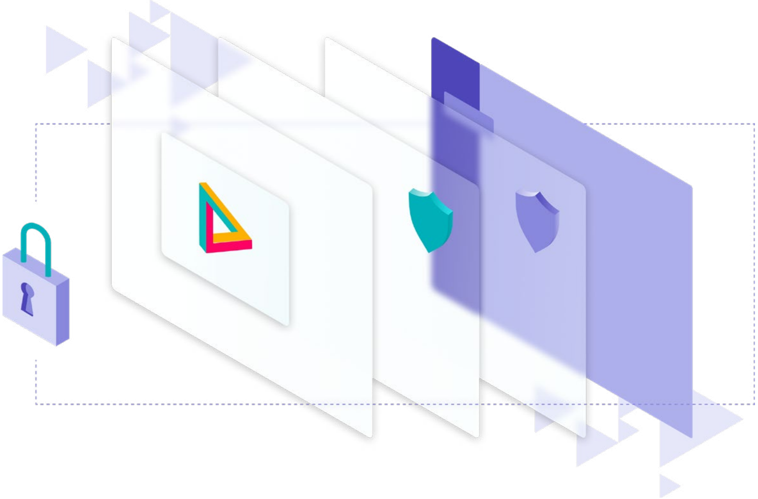
Layers of detection and response are vital, but layers of different solutions create a management problem that cannot be underestimated.

Mathematical theory holds that when the complexity of any system with inexact inputs grows, the likelihood of errors in that system increases greatly.

Multiple vendors and tools with different interfaces, physical probes, patching cycles, compatibility requirements, etc., degrade security outcomes.

Security researchers have been observing this trend for years now; study after study highlights security tool complexity as a growing problem.

- 30% of organisations say they have an overwhelmingly complex security stack.
- 30% of security leaders say that “too many tools” is one of the reasons their SOC is ineffective.
- One in ten security professionals feel they have so many tools they feel “not in control.”



The three hallmarks of bad complexity

This section breaks down the practical problems and outcomes of an overly complex security tool stack.

You can use it to **a)** diagnose whether your environment has complexity issues or **b)** know what to look out for when considering your tooling arrangement.

1 Tool Silos

Problem:
Multiple tools serving different, specific functions in a silo, which do not account for other parts of modern IT infrastructure/digital footprint.

Impact:
A tool might find something suspicious/not suspicious in its own domain, but alerts can't be generated with much confidence without visibility of wider behaviours.

For example, in an environment where security tools are "disconnected" from one another, analysts have no reliable way to correlate what the EDR says with network traffic, cloud account activity, user behaviour, or any other siloed data source.

67% of IT and security professionals say siloed data slows down security response times.

2 Management challenges

Problem:
"Head on a swivel" syndrome, i.e., various management consoles that force security professionals to monitor several tools and piece together information. There's no source of truth for security diagnosis.

Impact:
To try and make sense of disparate inputs and reduce the problem of false positive alerts IT teams have to constantly create and modify rules (often within another tool!) as to what events and patterns should be identified by their tools.

Unmanaged and out-of-patch security tools can also become vulnerabilities in themselves.

3 Uneven visibility

Problem:
Varying tech stacks (some new devices, some legacy, some cloud, varying OS, lots of SaaS apps, etc.) with different security requirements and installed controls.

Impact:
Varying degrees of control and/or visibility across different parts of the environment. Unmanaged assets are likely to host dangerous common vulnerabilities and exposures (CVEs).

When news of a major vulnerability breaks, panic ensues, and the lack of visibility becomes obvious.

How security systems become complex

Security complexity typically starts with a complex IT environment.

Digital transformation, or just normal technical creep, can leave an organisation with an IT environment that is complex and varied.

Growth brings new functions. A company can rapidly end up with a development team working with iOS devices, sales using Windows desktops, and even OT devices powered by ancient, out-of-patch varieties of Linux.

Regulatory and audit requirements can also play a role when they require some data to be treated and secured differently than others.

Unevenness can spiral.

As organisations change what they do and how they do it, whether organically or through mergers and acquisitions, IT gets more siloed. Security naturally follows this trend.

Before long, IT environments end up being secured with varying sets of controls. Generations of security leaders have installed their own solutions without fully sunsetting redundant or duplicate controls.

Eventually, multiple vendors might be used for antivirus, EDR, NDR, and cloud protection across the organisation. Possibly multiple SIEMs, too, depending on their use case (i.e., not just ingesting logs indiscriminately to satisfy audit requirements).

Or, if security is outsourced, the organisation might end up locked into several different arrangements with managed service providers (MSPs) of various quality, many of which might not actually deliver good security outcomes or clarity on the work being done and the value being realised.

What makes complexity worse is security marketing, which makes buyers feel they need to chase a suite of best-of-breed solutions without having the capacity to manage them. Plus the fact that getting a budget line for new IT software is almost always (much) easier than getting a new security FTE.

A cross-sectional study of cybersecurity teams in UK businesses by the UK government found that the median security team size is two people. A single EDR or similar solution requires at least one dedicated FTE.

It's not hard to see how an organisation can quickly end up with too many security tools or a level of complexity that harms its security outcomes.

How to restore order to a complex IT security environment

The solution for an overly complicated security environment and the vaccine against future complexity is to use as few tools and vendors as possible to cover the same ground.

In other words, consolidate, consolidate, consolidate.

75% of organisations are pursuing consolidation, according to Gartner. With good reason.

Consolidation, whether to a single vendor offering or an open alternative, is not the ideal solution for every organisation. Some organisations, particularly large enterprises, can afford to develop and run more complicated security stacks

However, for the vast majority of organisations, consolidation just makes sense.

Our experience shows that organisations can reduce their mean time to respond (MTTR), boost detection rates, and decrease security stress when they find a consolidated security solution that works for them.

Why?

Because a consolidation solution, like SenseOn, makes security simpler by:

- **Deploying in minutes, not months**. Managed through a SaaS interface, SenseOn can be deployed through a single installed agent across every device.
- **Combining multiple detection methods into one agent.** Including heuristics, signatures, deep packet inspection of network traffic, user behaviour and more. SenseOn replaces the need for separate EDR, NDR, user and entity behaviour analytics (UEBA), cloud detection and response, and other solution types.
- **Collecting data in a single format.** And showing analysts all the relevant information needed for investigation automatically.
- **Automating alert triage.** Because data is natively unified (i.e., comes from one agent), different sources and different types of events can be easily analysed together, creating much better business outcomes versus disparate systems with their own, siloed “automation” capabilities.

With outstanding threat detection metrics of over 99% benchmarked by third-party testing, **consolidation does not mean decreasing your response capabilities or increasing risk in any meaningful way.**

SenseOn's Universal Sensor

SenseOn is a custom-built consolidation solution.

In other words, **it was built as a unified platform from day one**.

We've built an advanced platform around a Universal Sensor that can analyse endpoint, network, and user behaviour from a single agent. For serverless cloud environments and cloud applications, our agentless cloud monitoring provides unintrusive threat detection and response. The data is always unified and consolidated and presented to end users with an unmatched level of detail.

The unified data collected by SenseOn is further enriched with additional analyses, including behavioural analytics to fuel a real-time detection and response engine that identifies and maps threat behaviours to the MITRE ATT&CK framework.

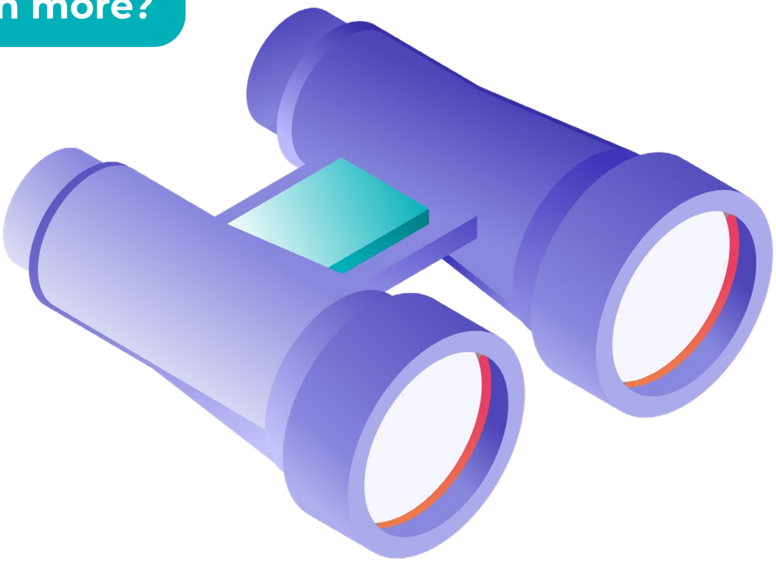
Adding on to take away

SenseOn is a security platform designed to simplify your environment by pulling together data from multiple sources and analysing it in context—so your analysts don't have to waste time piecing together disparate data points.

Our platform seamlessly integrates with a broad range of tools, including those from Microsoft, AWS, and Google, as well as third-party security systems. We also connect with ticketing systems to streamline workflows and BI tools for clear, actionable reporting.

Additionally, we enhance cloud-based alerts, reducing false positives and cutting through the noise.

Want to learn more?



SENSEON

Contact Us

✉ info@senseon.io

☎ +44 020 3994 1069

www.senseon.io

8 St James's Square,
London SW1Y 4JU