POINT PRODUCT AND ALERT OVERLOAD

Too Many Alerts, Too Many Products, Too Many Threats.

What's The Solution?

censornet.

POINT PRODUCT AND ALERT OVERLOAD_

What if cyber security could be really, truly, fully automated – to the extent that it could prevent attacks before they occurred?

We believe it can; but the so-called solutions that currently exist fall a long way short of this goal. To reach the greener land of low risk, low cost and limited liability, partial integration and semi-automated responses aren't going to cut it. Such approaches tend to add as many problems as they solve (alert overload, anyone?).

But there is a new, genuinely integrated, genuinely automated solution emerging. And no – it's NOT another console. Here's how it works...

THE PROBLEM: IN ONE SENTENCE_

There are too many security products.

AND THIS IS A PROBLEM... WHY?

At the last count there were more than 1,800 security vendors in the market, offering a bewildering array of products, most of them point product solutions that address one small area of the overall threat spectrum. With new start-up vendors appearing – or coming out of stealth mode – at the rate of nine a month (or 100 a year), it won't be long before we break through the 2k ceiling.

The result? Product chaos. Walk the exhibition floor of any major security show (RSA, Infosec Europe, etc.) and even seasoned security professionals struggle to understand what many vendors' solutions actually do – far less how to implement and manage them.

Notice the lack of the word 'integrate' in that last sentence. Most point products are security black boxes and, even if APIs exist, they tend to be extremely limited and primarily focused on extracting information rather than enabling security policies and rules to be modified. For that, you'd need to use the vendor-provided web management interface – yup, that thorny old stop-gap 'solution' of adding yet another layer on top of the layers you already have. The very definition of console fatigue.

Which is probably why we hear "Aaaaarrrrrggggh, do NOT bring me yet another console" on a daily basis.

NOT THE SOLUTION; NOT REALLY_

Rather predictably, the security industry's answer to integrating point products was yet more point products in the form of SIM/SEM – or SIEM – solutions. This additional layer promised to put security operations staff back in control by aggregating and correlating logs and generating meaningful actionable alerts.

Equally predictably, this new layer of complexity brought its own set of problems. While many organizations struggle to extract value from their SIM/SEM deployment – or, as some vendors are now calling it, next-generation SIM/SEM – they also need to deal with the events and alerts being generated, each of which needs to be analyzed and investigated.

Even the best-staffed SOC (Security Operations Center) could be forgiven for feeling utterly overwhelmed by the sheer number of alerts, as the following figures demonstrate ⟶

IN SUMMARY:

- Human resources alone are dangerously insufficient.
- Dealing with alerts leaves no time for proactive threat-hunting, or searching for indicators of compromise.
- There is clearly a need to bridge the gap between alert overload and analyst capacity.

TOO MANY PRODUCTS; NOT ENOUGH ANALYSTS

The average enterprise has perhaps 25-30 security products, while in the largest organizations this number can rise to 60-100. We started with firewalls, VPNs, IDS/IPS, web and email content security, gateway and endpoint AV, and over time have added extensively to this list.

The increasing volume of security products not only increases the cost and complexity of the security ecosystem, it also quickly begins to degrade overall security agility and – ultimately – effectiveness.

And of course, security teams aren't able to grow exponentially to manage all this complexity, even if an organization had the resources to fund such a growth... because we're facing a rapidly escalating skills gap in the cyber security industry.

(Sources: Enterprise Strategy Group, Ponemon Institute, Enterprise Management Associates)

92%

of enterprises

receive more than 500 SOC alerts per day

1

single analyst

can handle around 10 alerts per day

4%

of alerts

are investigated by analysts

STILL NOT THE SOLUTION_

Then came an answer to the new problem (that had itself been generated by the answer to the old problem). And yes, it was yet more point products, this time in the form of Security Operations Analytics and Reporting (SOAR) offerings. And just as organizations were starting to soar, along came a next-generation acronym: SOAR v2 – Security Orchestration, Automation and Response.

Security Orchestration and Automation tools primarily automate tasks for analysts, particularly in the early stages of investigating an event. They provide information aggregation, with some correlation, to automate the most mundane analyst tasks. This helps to ensure that tier-2 and tier-3 analysts in particular are focused on the activities that leverage their skills and experience. Meanwhile, playbooks can define workflows and processes to support and guide – and audit – incident response activity.

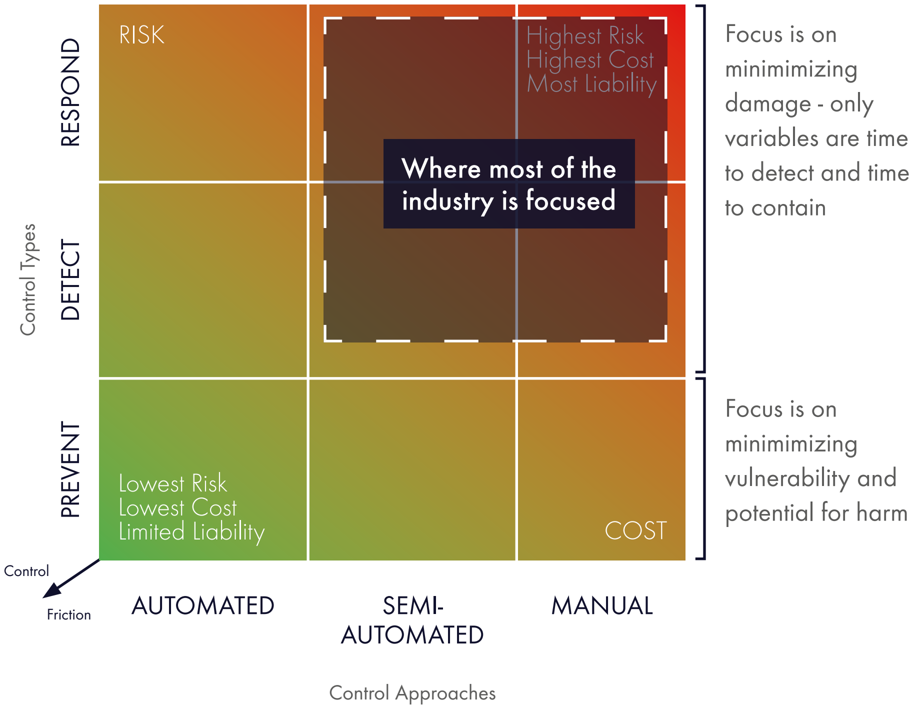
> “ ...ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019. Every year in the U.S., 40,000 jobs for information security analysts go unfilled...”

Now, we’re not saying these tools aren’t a move in the right direction. On the contrary, they’re a welcome step towards the holy grail of effectively automating an organization’s response to security incidents.

We’re just saying they don’t go nearly far enough. The focus of these tools and products is the manual detection and (putting it kindly) semi-automated response to security events – but they still occupy an area where risk, cost and liability are high, as the following diagram illustrates.

Source: https://bit.ly/2GdDkd6

SECURITY RISK VS COST_


RISK
Highest Risk
Highest Cost
Most Liability
Where most of the industry is focused
Lowest Risk
Lowest Cost
Limited Liability
COST
RESPOND
DETECT
PREVENT
Control Types
Control
Friction
AUTOMATED
SEMI-AUTOMATED
MANUAL
Control Approaches
Focus is on minimimizing damage - only variables are time to detect and time to contain
Focus is on minimimizing vulnerability and potential for harm

Source: Managing Risk and Information Security 2nd edition Malcolm Harkins

We need more integration and more automation; but the challenge with automating security up the stack is that the vast majority of security point products are, as we said earlier, closed black boxes. While there might be ways to extract post-event information in the form of log files or specific log entries, very few products allow external systems to write changes to security policies and rules.

And it’s primarily for this reason that the security industry has become stuck in a cycle of more and more point products to address new threats and concerns, along with more and more management layers to implement them.

THIS IS WHERE WE NEED TO BE_

As an industry, it's time to stop patching the problem – adding more management layers over too many point products – and instead define a properly integrated, automated approach that removes the problem entirely.

We need a really, truly, fully automated security response – to the extent that attacks can be prevented before they occur, thus taking an organization into the happier land of low risk, low cost and limited liability.

Here's how it might work. Let's say a new vulnerability is identified through a security news or threat intelligence feed. What if this were to kick off a vulnerability scan against critical systems to determine which are vulnerable, with corresponding tickets automatically opened or – in some environments – even updates applied? Or perhaps changes could automatically be made at the network layer, if and when a new piece of malware is identified that propagates over a particular port?

But it's the application layer where the real action is today. Email and web are still far and away the most common vectors for the initial infection and attack – so to whet your appetite further, here are some examples of how powerful a properly integrated and automated security response could be: ⟶

SCENARIO 1_

A user is sent a possible phishing email that contains a malicious link and the email security gateway identifies and quarantines it. The user sees the email in their quarantine, thinks it is legitimate and releases it to their inbox – and then forwards it to other users internally. In an adaptive, automated world, when the email security gateway first identifies the email, the web security solution is immediately updated to block the malicious URL for all users.

SCENARIO 2_

An organization is being heavily targeted with customized malware over web and email channels. If the email security gateway sees a file attachment containing the malware, then file details are immediately shared with the web security solution to prevent infection via the web (or cloud) vector.

SCENARIO 3_

A user attempts to upload a file to a cloud storage app, such as Dropbox or OneDrive, that contains confidential information. A hash of the file is shared with email and web security services so that the user cannot send the file externally as an attachment to an email or webmail message. Data exfiltration infiltrated.

SO WHY HASN'T THIS HAPPENED?

Where's the stumbling block that's preventing us reaching this happier land?

Understandably perhaps, there's a deep-rooted reluctance for individual vendors to open up their products to enable a fully automated response. Some argue this makes them less secure or more susceptible to attack but, whatever the reason, the vendors' black boxes remain firmly closed.

There is some hope on the horizon. Moves are afoot to establish standardized language for cyber operations command and control, and to crowdsource threat intelligence data (see box-out), both potentially powerful ways to move towards integrated, automated security solutions. The snag here is that universal standards generally take a disappointingly long time to reach widespread adoption and support.

FUTURE SOLUTIONS_

Within the next five years... maybe:

OASIS OPENC2_

The OpenC2 Technical Committee of OASIS – an international, non-profit consortium – is working on a standardized language for cyber operations command and control. This will enable defenders to respond to cyber attacks at machine speed and allow greater interoperability among products. By providing a common language for machine-to-machine communication, OpenC2 should make it possible for defenders to conduct automated, coordinated, tactical threat responses more accurately and at speeds greater than those previously possible.

STIX, TAXII AND CYBOX_

The Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII) and Cyber Observable Expression (CybOX) are a set of free tools that define a standardized language to represent threats, along with services and message exchanges to help with the automated exchange of cyber threat information.

CROWDSOURCING THREAT INTELLIGENCE_

Sharing threat intelligence data can be a very powerful approach, as the Quad9 DNS initiative ably demonstrates. See https://www.quad9.net.

DEPARTMENT OF HOMELAND SECURITY_

The National Cybersecurity and Communications Integration Center (NCCIC), part of the U.S. Department of Homeland Security's Office of Cybersecurity and Communications, is well aware of the power of information-sharing initiatives, but the Information Sharing Standards for Cybersecurity are still in their early stages.

The uncomfortable truth is that for the next two to five years at least, and possibly a fair while longer, a fully automated security response won't be possible unless a vendor integrates multiple point products into a single platform and 'joins the dots' themselves.

And even more challengingly, these multiple point products will need to address the full spectrum of cyber threats, from email and web security, to cloud application security and multi-factor authentication. With, ideally, a single portal (or 'pane of glass') to monitor the full range of security across the entire organization.

THE GOOD NEWS... THE FUTURE HAS ARRIVED_

Censornet's Unified Security Service (USS) is a single, simple, integrated platform that includes email and web security, cloud application security and multi-factor authentication. In other words, it's the 'single pane of glass' that cyber security professionals have long been seeking.

But it also opens the way for the industry to move to another level, shifting integrated security products from reactive to proactive and enabling attacks to be prevented. Automatically.

Once all security products are integrated within a single platform, there's no longer a barrier to sharing and exchanging short-term security data on users, user actions, devices and content, so that any single product could, in theory, automatically take action based on observations drawn from other products.

The industry is on the verge of a beautifully simple solution that will have the power to stop even the most sophisticated cyber threats – reacting to, and preventing, attacks in real-time. Looking back at the three security scenarios we described earlier, the adaptive, automated world that will allow those attacks to be automatically prevented is within our grasp.

Genuine integration; genuine automation; across every major threat infection vector – and all from a single console.

UNIFIED SECURITY SERVICE_

A 360-degree view across web, email and cloud applications at a single glance.

With Censornet's innovative cloud platform, you won't have to consider point products and silo'd solutions. Your organization's core security services are combined on a single cloud platform giving you full visibility and advanced threat protection.

The vision for the Unified Security Service is to make things simple again. To put your security team back in control by being able to see and respond to threats from both outside and inside the organization - all in real time, and all from a single dashboard.

W. WEB

WEB SECURITY

Provide a safe internet experience for all the people within your organization

E. EMAIL

EMAIL SECURITY

A cloud based solution to keep your organization safe from email threats

M. MFA

MULTI-FACTOR AUTHENTICATION

Keep your systems and data safe with multi-factor authentication

C. CASB

CLOUD APPLICATION SECURITY

Secure adoption of cloud services and applications in your organization

WANT TO LEARN MORE?

VISIT CENSORNET.COM

KEY POINTS TO TAKE AWAY_

1_ There are too many point products, each addressing only a very small part of the threat spectrum.

2_ So-called industry 'solutions' to this problem have been limited, as there's currently no way to integrate the many point products (from many vendors) into a single platform.

3_ Vendors are reluctant to 'open up' their products to allow a fully automated response. So the point products remain as closed black boxes.

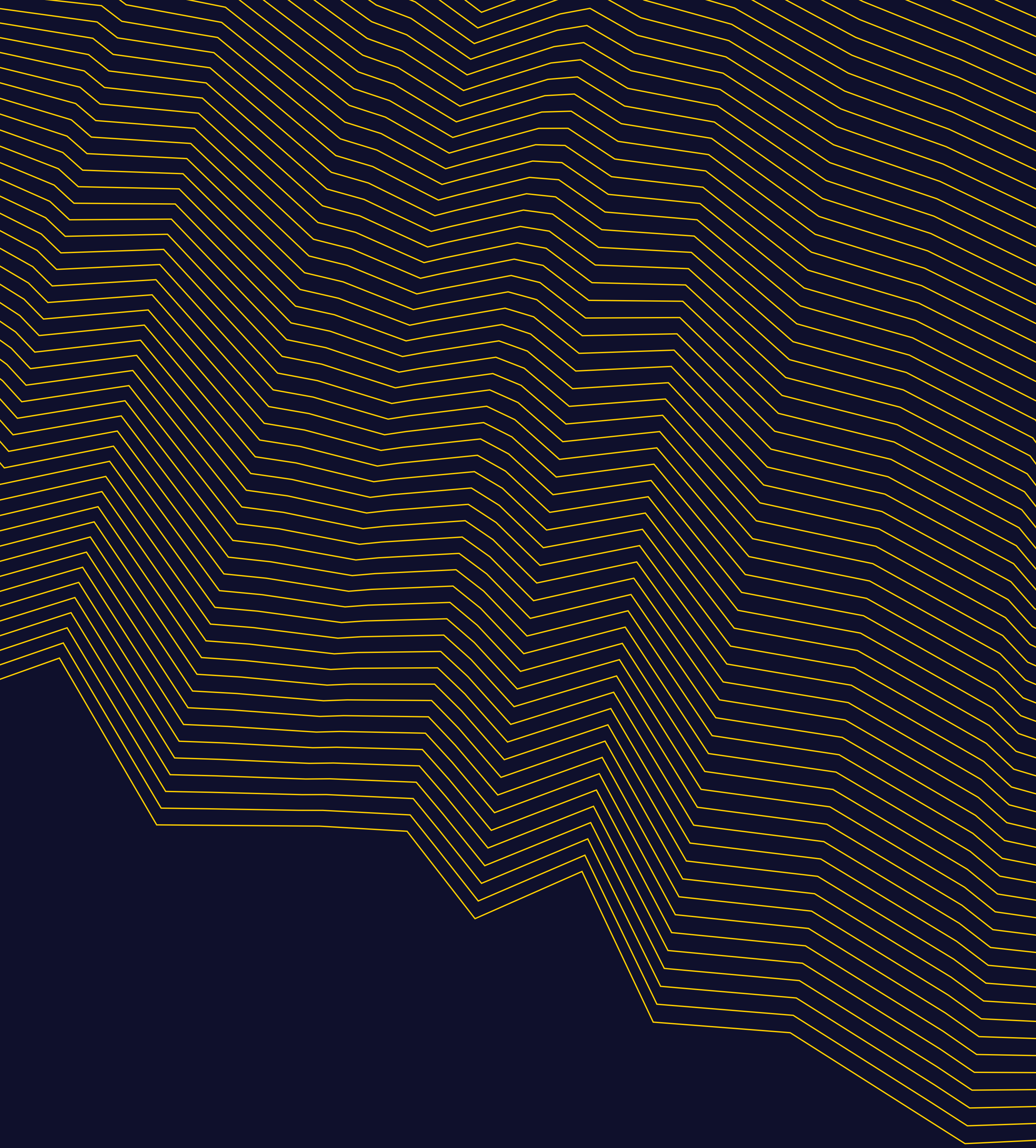
4_ Existing attempts to aggregate products and alerts usually mean – at best – adding yet another layer, yet another console.

5_ As it is, security professionals are drowning in thousands of alerts that there aren't the resources to investigate.

6_ What's needed is a genuinely integrated, automated approach that allows even sophisticated attacks to be proactively prevented.

7_ The industry (along with governments) is working on a number of information-sharing solutions and standardized language that will allow point products to be integrated – but we're looking at two to five years, or possibly more, before this becomes a reality.

8_ There is, however, an effective solution much closer to being realized. In the very near future, it should be possible to harness the potential of a single, integrated platform that addresses every major threat infection vector – enabling it to share information between products and automate the response to attacks in real-time.



Censornet LTD

Network House, Basing View,
Basingstoke, RG21 4HG, UK
Phone +44 (0) 845 230 9590

Censornet A/S

Park Allé 350D, 2605 Brondby,
Denmark
Phone +45 70 22 55 33

Censornet INC

11801 Domain Blvd, Austin TX
78758, USA
Phone: +1 888 440 8456

Censornet.com