censornet.

A PLATFORM PERSPECTIVE FOR THE MID-MARKET:

WHY SECURITY PORTFOLIOS WILL FAIL AS PLATFORMS PREVAIL.

A guide for mid-market organisations on embracing integrated security – and preparing for the new generation of security challenges.

A perfect storm

Cybersecurity teams are facing unprecedented challenges. Increasingly complex threats are being compounded by a huge rise in remote working, which has sounded the death knell for the traditional perimeter.

"The adoption of cloud services, rise of hybrid working, increase in connected devices and extended supply chain ecosystems means almost all organisations have some digital exposure. And with that comes risk."

Richard Walters, CTO, Censornet

Now, security must go seamlessly where the user goes – and trying to do that with legacy, siloed point products is unsustainable.

These challenges coincide with a severe shortage of skills. According to Gartner, "the world also faces a huge shortfall in cybersecurity talent — more than 3.2 million, according to the 2020 ISC2 survey — so operational efficiency is a key requirement[1]."

Only 44% of business leaders will require employees to work in person full-time in 2022[2]

"Security and risk management leaders continue to be asked to do more with less — facing more demand for service, fast-changing threat landscapes and insufficient technical talent[3]."

Gartner

[1] Predicts 2022: Consolidated Security Platforms Are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 1 December 2021

[2] Microsoft 2022 Work Trends Index https://news.microsoft.com/en-gb/2022/03/16/the-uk-is-showing-the-world-that-flexible-working-can-be-a-success/

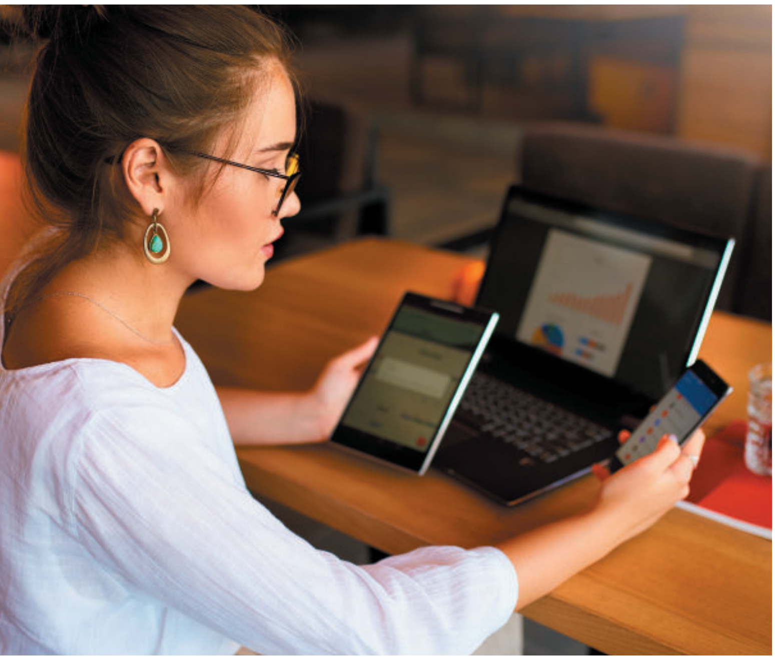
[3] Predicts 2022: Consolidated Security Platforms Are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 1 December 2021

Platforms vs portfolios

Unfortunately, the current reality is that rather than reducing complexity, too many mid-market businesses are managing multiple point products, incompatible dashboards, and struggling to integrate new systems with existing defences.

> **27% of mid-market firms rely on over 31 security solutions.**
> **7% deploy more than 50[4].**

Security Service Edge (SSE) is a Gartner term. "SSE secures access to the web, private applications and usage of cloud services. Capabilities include access control, threat protection, data security, security monitoring and acceptable use control enforced by network-based and API-based integration[5]."



At Censornet we believe that a security service edge platform (SSE) approach relieves this pressure: driving integrated security from a single cloud-based platform. Something that is vital for mid-sized businesses that have limited budgets and resources but are battling a growing volume of threats. It's also important to remember that not all vendors can deliver a truly consolidated platform, so security teams need to be sure they're getting the right support when evaluating vendors.

As Gartner notes, vendors are increasingly divided into 'platform' and 'portfolio' camps, with the former integrating tools to make a whole that's greater than the sum of the parts, and the latter packaging products with little integration[6].

When looking for a solution, Gartner suggests:

- Differentiating between these approaches is key to the efficiency of the suite
- "Look at how integrated the consoles are for the management and monitoring of the consolidated platform."
- "Assess how security elements can be reused without being redefined or can apply across multiple areas seamlessly."

[4] Predicts 2022: Consolidated Security Platforms Are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 1 December 2021

[5] Predicts 2022: Consolidated Security Platforms Are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 1 December 2021

[6] Censornet, The Uk Mid-Market On Code Red, The State of the UK's Cyber Security Response, April 2022

Consolidating security with a co-ordinated approach

Our own research shines a light on the demand for a platform approach: 46% percent of organisations in the mid-market want to see security vendors open up traditionally closed point products to enable an automated response to cyberattacks[7].

A more coordinated approach allows for email, web, identity, and cloud application security systems to work in tandem, identifying and tracking attacks as they proliferate across an organisation.

Portfolio

No integration or synergy between point products

Multiple dashboards, limited visibility, and no shared reporting across security portfolio

Integration must be manually plumbed in and maintained

No centralised vendor support

Siloed products create vulnerabilities for cross channel attacks

Platform

Web, email, cloud, & network security managed in one platform

Seamless data-sharing in a single console

Updates and new products automatically available through platform

24/7 vendor support augments in-house team capacity

Integrated systems track and stop cross-channel attacks

[7] Censornet, The Uk Mid-Market On Code Red, The State of the UK's Cyber Security Response, April 2022

A single platform for effective defence

According to Gartner "As the platforms shift to the cloud for management, analysis and even delivery, the ability to leverage the shared responsibility model for security brings enormous benefits to the consumer[8]."

> **''The concept of the cybersecurity mesh [...] enables these platforms to collaborate via APIs, using current and emerging security standards. Administration can be centralized, while policy enforcement is distributed[9].''**
>
> Gartner

For mid-market organisations that successfully transition to a cloud-based, integrated platform approach, the benefits are significant:

- An autonomous, integrated security platform has the capacity to tackle evolving threats, right across an organisation's attack surface, round-the-clock, at lightning speed.
- Operating a single platform means all your security functions can share relevant data in a single, transparent dashboard, improving speed and accuracy of response and reporting, while helping to mitigate against cross-channel attacks and eliminate complexity.

> "A platform approach gives organisations a modular and integrated approach that is simpler to use, easier to manage and reduces the need for manual intervention. That's not to mention the ease of reporting, transparency on all incoming threats and ability to have a holistic view of your entire security posture in one place."
>
> Richard Walters, CTO, Censornet

[8] Predicts 2022: Consolidated Security Platforms Are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 1 December 2021

[9] Predicts 2022: Consolidated Security Platforms Are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 1 December 2021

Why is a platform approach important for the mid-market?

Q&A with Richard Walters, CTO, Censornet

Q. Why is the mid-market becoming more vulnerable to cyber-attacks?

"The adoption of cloud services, rise of hybrid working, increase in connected devices and extended supply chain ecosystems means almost all organisations have some digital exposure. And risk. Gone are the days when cybersecurity could be written off as the preserve of large companies. Almost all businesses process sensitive information that is valuable for cybercriminals, and many are seen as effective conduits into larger enterprises owing to the business relationships that they maintain. Autonomous, integrated cloud security is a crucial step towards an effective defence that can keep up with evolving cross-channel attacks."

> **"The adoption of cloud services, rise of hybrid working, increase in connected devices and extended supply chain ecosystems means almost all organisations have some digital exposure. And with that comes risk."**

Q. Why is a platform approach crucial in the current threat landscape?

"Our research shows that mid-market firms use an average of 24-point products to protect themselves. Seven percent deploy more than 50-point products. Between each point solution is a security gap that cybercriminals are exploiting. A platform approach enables organisations to reduce those gaps. By connecting email, web and cloud application security with identity and context, organisations can eliminate the vulnerabilities that sit between and across major attack surfaces."

Q. How can a platform approach help mid-market businesses?

"A platform approach enables organisations to move away from the more expensive and time-consuming approach of running separate solutions in silos. Instead, it gives organisations an integrated approach that is simpler to use, easier to manage and reduces the need for manual intervention.

Crucially, a platform approach enables digital business – giving users the freedom to access the applications and data they need regardless of device or location, whilst providing visibility for IT and adequate protection."

Q. How can mid-market businesses future-proof cybersecurity with a platform approach?

"It is undeniable that the next step in the evolution of security will involve zero-trust, with every user and every request granted the least amount of privilege. This change goes beyond keeping threats out of the 'safe zone'. A platform approach that connects email, web and cloud security with identity and context will prepare organisations for this shift. It will empower organisations to validate a user's context and identity at lightning speed using information on geolocation, device integrity, and credentials before they connect to sensitive information and systems."

> **"A platform approach gives organisations a modular and integrated approach that is simpler to use, easier to manage and reduces the need for manual intervention. That's not to mention the ease of reporting, transparency on all incoming threats and ability to have a holistic view of your entire security posture in one place."**

The way forward

As Gartner advises, "Leaders who evaluate where they have an operational or security shortfall and push for a consolidation investment will have a higher rate of security success than those driven by the security team[10]."

In today's inflationary environment, mid-sized businesses are keen to see reductions in the complexity and cost of enterprise-grade security with 37% and 34% respectively ranking these considerations as their top cybersecurity wish for 2022[11]. We believe implementing a consolidated security platform is a key way of responding to the pressures the mid-market is facing. At the same, a unified platform approach that integrates web security, cloud security and application access will help deliver an effective cybersecurity defence that supports the future of digital businesses.

Censornet's top tips for making the transition to integrated security

- **Invest in the right security solutions at the right point on your journey.**
  Think about whether you can consolidate defences. Connect email, web and cloud security with identity and context – so there are no weak spots to target.
- **Eradicate complexity.**
  Instead of managing multiple point products and ploughing time or effort into supporting legacy solutions like VPNs, MPLS and WAF deployments, embrace cloud native security that ensure updates can be applied without the need for manual intervention.
- **Create your own rules.**
  Ensure you can pre-define what can act autonomously and what cannot. Create your own rules based on thousands of attack scenarios for machine speed response to enhance protection.
- **Gain visibility of threats across your entire ecosystem.**
  Stop cross-channel attacks from occurring with shared attack intel. Leverage in-built threat intelligence feeds to proactively stop attacks even entering the kill-chain.
- **Autonomous integration.**
  Enable cyber defences to work together, untouched by the human hand, with full API provisioning and management.

[10] Predicts 2022: Consolidated Security Platforms Are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 1 December 2021

[11] Censornet, The Uk Mid-Market On Code Red, The State of the UK's Cyber Security Response, April 2022

About Censornet

Headquartered in an innovation hub in Basingstoke, UK, Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection. Its Autonomous Security platform integrates attack intel across email, web, and cloud applications to ensure cyber defences react at lightning speed. For its millions of users globally, Censornet synthesises a billion threats a day, to give full protection - wherever attacks start and wherever they move.

It's supported by an award-winning team of customer support specialists. Censornet's clients include Fever Tree, Lotus Cars, Parnassia Groep, Mizuno, Radius Payments, Newlife Disabled Children's Charity, National Portrait Gallery, Hallmark Hotels and Thatchers Cider. It was named Cloud Security Product of the Year (SME) at the Computing Cloud Excellence Awards 2021. For more information, please visit **www.censornet.com**

Find Out Why Gartner Believes Consolidated Security Platforms Are the Future

If you enjoyed reading this guide, check out Gartner's annual predictions report which sets out key insights, recommendations, and strategic planning assumptions for the future of cybersecurity.

Access the report:

www.censornet.com/gartner_reports/consolidated_security_platforms/

censornet

www.censornet.com