censornet.

THE ABCD OF CYBERSECURITY.

Getting your ABCDs right is key to stopping attacks.

Whitepaper

Users are the perimeter

With the long-term shift to hybrid and remote working, traditional boundaries have dissolved. Applications and information need to be readily accessible to users wherever they are: whether that is 'inside' or 'outside' their network. Today, users are the perimeter. Security must follow them across whatever device, network or location they are using.

What it means for you

The network, and the data sent over it, needs to be secured.

Gartner describes the fusion of security (or Secure Service Edge, SSE) and networking into a single, scalable, cloud-based platform as Secure Access Service Edge (SASE). Since the term was coined in 2019, media coverage has skyrocketed.

Designed to simplify the components required to secure your network, devices and users, the journey to SASE will take several years. Gartner suggests that only 40% of organisations will have a plan to adopt SASE by 2024. As SASE today is only a direction, it's important to avoid taking a dead end in your investment cycle now.

Whilst SASE is further away on the horizon, you can be working on your ABCDs now to keep your organisation safe from cyber-attack.

ACTIVITY

Email, web and cloud applications are the foundations of day-to-day interactions. This means a large proportion of the working day can be tracked. The more time users spend online - using the web browser to access internet content or interact with cloud applications, or reading and replying to email – the more activity can be analysed to determine what normal activity looks like.

By intelligently monitoring user activity, you can extend or retract access permissions in real-time. For example, if a user is authenticated but then persistently attempts to access unusual files, or attempts to download large amounts of sensitive information, their access can be dynamically revoked.

BEHAVIOUR

Over time, activity equals behaviour. A comprehensive view of activity over time, delivers insight into acceptable patterns of behaviour. It makes it possible to understand what constitutes "business as usual" for each user. In turn, this insight can underpin security policies that autonomously protect the business in real-time from the unusual or unacceptable.

For instance, if an endpoint attempts to send out 20,000 identical emails in the space of 90 seconds, then it's easy to identify that activity as abnormal – and a strong indicator that the endpoint is infected with malware.

Rules based on User and Entity Behaviour Analytics (UEBA) can be automatically applied to shut down suspicious, or outright malicious, activity. Or, if a user attempts to log in at an unusual time or from an unrecognised device, an autonomous system can request further authentication, or simply deny access, minimising the risk of unauthorised access. Or worse.

CONTEXT

Context offers a vital layer of intelligence to ensure resources are not compromised. It also raises a red flag if activity goes against the normal pattern of behaviour. It takes into account the attributes, characteristics and usuality surrounding authentication attempts. Everything from the location, the time of day, what application they are trying to access, to the type of device should be evaluated before allowing a user to connect.

Someone trying to access a database with sensitive customer data outside of normal office hours and from an unusual location would result in denial of access. Real-time, accurate and contextual authentication processes across the entire ecosystem can keep your organisation safe.

In a Zero Trust world, context assessment is continuous. It's performed throughout the session, not just at the moment of authentication – with access changing corresponding to changes in context.

DATA

Understanding who's uploaded, shared or sent a file to who or where is no longer enough. It's the data in the file that is critical. Awareness of what the data is within the file is essential to taking security practices to the next level.

It's not always necessary to know how many users have uploaded files to a cloud folder, but you do need to know what information is personal, financial, sensitive or regulated. It's vital to identify files containing sensitive information, like credit card details or bank account details numbers, so uploads can be automatically blocked in real-time.

Data Loss Prevention (DLP) scanning of data at rest and in transit is imperative – to avoid data breach costs, legal fees, fines and reputational damage.

OUR TOP-TIPS FOR GETTING YOUR ABCD RIGHT

01

Control user activity

Adopt a Zero Trust mindset and a least privilege approach to as many protect surfaces as possible.

02

Understand behaviour

Use a single integrated platform to understand patterns in behaviour and provide the foundations for context-based security.

03

Put everything into context

Continuously assess what your users are attempting to access and the activity they're performing.

04

Follow the data

Introduce Data Loss Prevention (DLP) to get visibility of your data in use, at rest and in motion.

+

Rethink identity

Verify the identity of users on premise and in the cloud with high assurance. Use Identity as a Service (IDaaS) to define rules that govern who, when and from where access to what data is granted.

+

Enable adaptive MFA

Multi-Factor Authentication protects user accounts with more than just a password and is the most powerful control against unauthorised access. Combine it with IDaaS to allow MFA across unsupported cloud applications.

To protect information access and prevent the widest range of attacks autonomously requires tight integration of security solutions. Context, and especially identity is key. Together they provide trust that users are who they say they are, that the activities they are performing represent an acceptable risk and that their behaviour is as expected.

Find out how Censornet can support you with your ABCDs. Contact us on +44 (0) 845 230 9590 or drop email us on sales@censornet.com

ABOUT CENSORNET

Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection. Our autonomous security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed. For our millions of users globally, our automated solution is smarter, faster, and safer than is humanly possible.

We are supported by an award-winning team of customer support specialists. Our clients include Fever- Tree, Lotus Cars, Parnassia Group, 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.

censornet.

www.censornet.com