3 REASONS THE SECURITY INDUSTRY IS PROTECTNG THE WRONG THING

3 Reasons the Security Industry is Protecting the Wrong Thing

Why is it that the security industry talks about network security, but data breaches? It's clear that something needs to change, and according to Paul German, CEO, Certes Networks, the change is simple. For too long now, organisations have been focusing on protecting their network, when in fact they should have been protecting their data. Paul outlines three reasons why the security industry has been protecting the wrong thing and what they can do to secure their data as we move into 2021.

One: They're Called Data Breaches, Not Network Breaches for a Reason

Looking back on some of the biggest data breaches the world has ever seen, it's clear that cyber hackers always seem to be one step ahead of organisations that seemingly have sufficient protection and technology in place. From the Adobe data breach way back in 2013 that resulted in 153 million user records stolen, to the Equifax data breach in 2017 that exposed the data of 147.9 million consumers, the lengthy Marriott International data breach that compromised the data from 500 million customers over four years, to the recent Solarwinds data breach at the end of 2020, over time it's looked like no organisation is exempt from the devastating consequences of a cyber hack.

When these breaches hit the media headlines, they're called 'data breaches', yet the default approach to data security for all these organisations has been focused on protecting the network - to little effect. In many cases, these data breaches have seen malicious actors infiltrate the organisation's network, sometimes for long periods of time, and then have their pick of the data that's left unprotected right in front of them.

So what's the rationale behind maintaining this flawed approach to data protection? The fact is that current approaches mean it is simply not possible to implement the level of security that sensitive data demands as it is in transit without compromising network performance. Facing an either/or decision, companies have blindly followed the same old path of attempting to secure the network perimeter, and hoping that they won't suffer the same fate as so many before them.

> *...the change is simple. For too long now, organisations have been focusing on protecting their network, when in fact they should have been protecting their data.*
>
> **Paul German, CEO, Certes Networks**

However, consider separating data security from the network through an encryption-based information assurance overlay. Meaning that organisations can seamlessly ensure that even when malicious actors enter the network, the data will still be unattainable and unreadable, keeping the integrity, authentication and confidentiality of the data intact without impacting overall performance of the underlying infrastructure.

Reason Two: Regulations & Compliance Revolve Around Data

Back in 2018, GDPR caused many headaches for businesses across the world. There are numerous data regulations businesses must adhere to, but GDPR in particular highlighted how important it is for organisations to protect their sensitive data. In the case of GDPR, organisations are not fined based on a network breach; in fact, if a cyber hacker were to enter an organisation's network but not compromise any data, the organisation wouldn't actually be in breach of the regulation at all.

GDPR, alongside many other regulations such as HIPAA, CCPA, CJIS or PCI-DSS, is concerned with protecting data, whether it's financial data, healthcare data or law enforcement data. The point is: it all revolves around data, but the way in which data needs to be protected will depend on business intent. With new regulations constantly coming into play and compliance another huge concern for organisations as we continue into 2022, protecting data has never been more important, but by developing an intent-based policy, organisations can ensure their data is being treated and secured in a way that will meet business goals and deliver provable and measurable outcomes, rather than with a one-size-fits-all approach.

Reason Three: Network Breaches are Inevitable, But Data Breaches Are Not

Data has become extremely valuable across all business sectors and the increase in digitisation means that there is now more data available to waiting malicious actors.

From credit card information to highly sensitive data held about law enforcement cases and crime scenes, to data such as passport numbers and social ID numbers in the US, organisations are responsible for keeping this data safe for their customers, but many are falling short of this duty. With the high price tag that data now has, doing everything possible to keep data secure seems like an obvious task for every CISO and IT Manager to prioritise, yet the constant stream of data breaches shows this isn't the case.

But what can organisations do to keep this data safe? To start with, a change in mindset is needed to truly put data at the forefront of all cyber security decisions and investments. Essential questions a CISO must ask include: Will this solution protect my data as it travels throughout the network? Will this technology enable data to be kept safe, even if hackers are able to infiltrate the network? Will this strategy ensure the organisation is compliant with regulations regarding data security, and that if a network breach does occur, won't risk facing any fines? The answer to these questions must be yes in order for any CISO to trust that their data is safe and that their IT security policy is effective.

Furthermore, with such a vast volume of data to protect, real-time monitoring of the organisation's information assurance posture is essential in order to react to an issue, and remediate it, at lightning speed. With real-time, contextual meta-data, any non-compliant traffic flows or policy changes can be quickly detected on a continuous basis to ensure the security posture is not affected, so that even if an inevitable network breach occurs, a data breach does not follow in its wake.

Trusting Information Assurance

An information assurance approach that removes the misdirected focus on protecting an organisation's network and instead looks at protecting data, is the only way that the security industry can move away from the damaging data breaches of the past. There really is no reason for these data breaches to continue hitting the media headlines; the technology needed to keep data secure is ready and waiting for the industry to take advantage of. The same way that no one would leave their finest jewellery on display in the kitchen window, or leave their passport out for the postman to see, organisations must safeguard their most valuable asset and protect themselves and their reputation from suffering the same fate as many other organisations that have not protected their data.

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

CERTES NETWORKS

Tel: 1 (888) 833-1142
sales@certesnetworks.com

www.certesnetworks.com