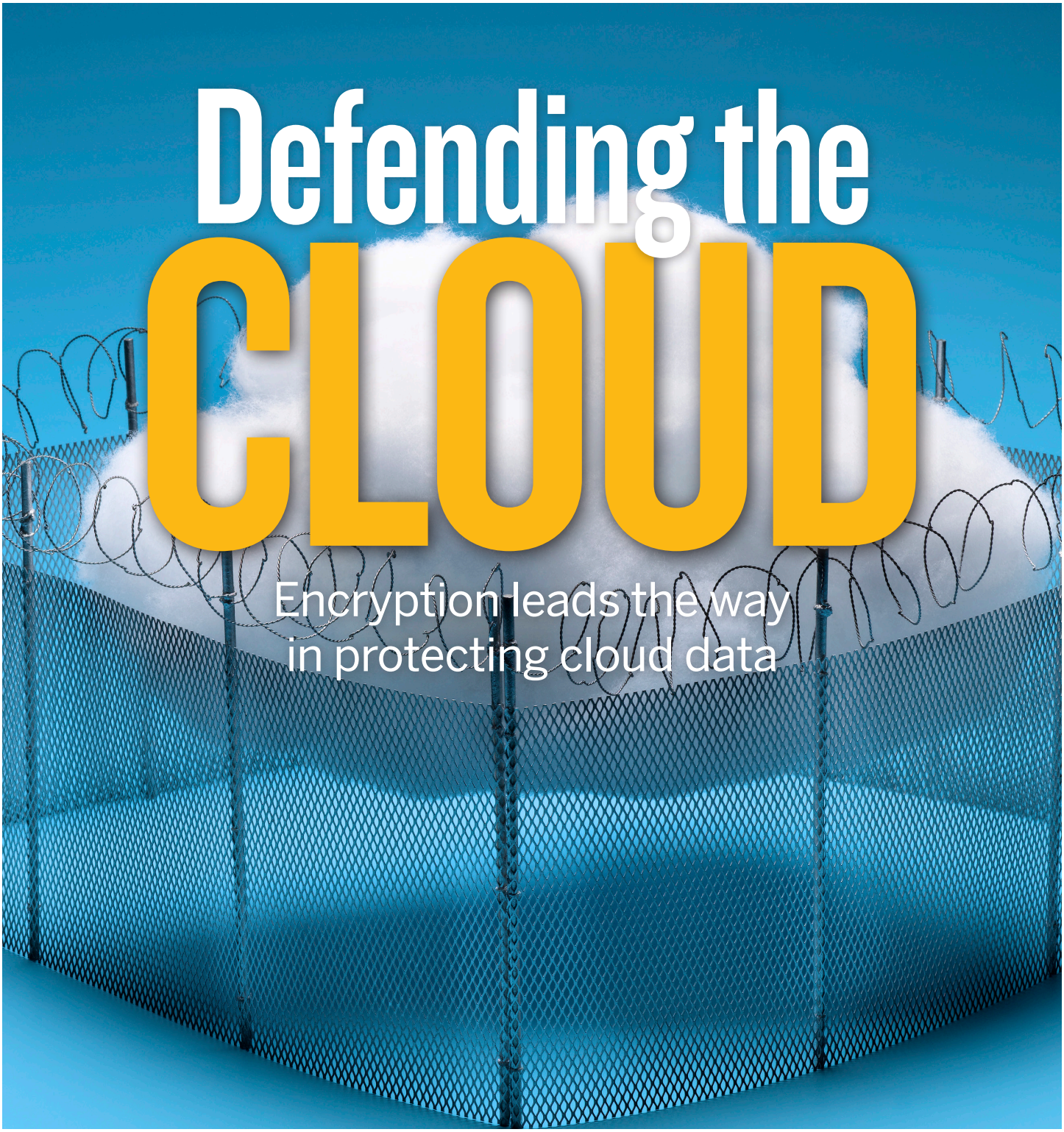


ebook

An SC Media publication

Sponsored by

ExtraHop

Rise Above the Noise.

Mostly cloudy with network detection and response

Strong cloud-based network defenses, coupled with encryption and NDR tools, bode well for protecting corporate data. Bob Violino reports

Almost a decade ago, Richard A. Clarke, the former national security counter-terrorism expert who served under Presidents Bill Clinton and George W. Bush, asked a gathering of security pros in Seattle how many knew there were cyberattackers within their networks. A few hands went up. Then he asked how many in the audience didn't know they had attackers within their networks — he told the rest of the attendees to raise their hands since nearly all of them likely had breached networks. Understanding that your on-prem networks probably are already breached puts the challenge of protecting cloud assets into perspective.

As a CISO, understanding an organization's threat profile is a cornerstone of the job. Defending against threats becomes more problematic when your network extends off premises and into the cloud where physical access to the servers holding data is essentially nonexistent. The CISO is still required to protect data, but without the same access and abilities once available.

This becomes even further complicated today for many organizations where it is no longer a question of whether to shift data and workloads to the cloud, but when and how. Cloud services have become essential components of the IT strategies of countless enterprises around the world. How these services protect data and identify potential breaches create challenges to test the mettle of even the most tenacious CISO.

The pragmatic question is how best to defend cloud resources against cyberattacks. This can be a huge challenge, and it is not getting any easier as organizations move to create increasingly complex multi-cloud and hybrid cloud environments.

One of the go-to technologies for cloud security is encryption because it can keep bad actors from getting hold of sensitive information. For many, encrypted data in the cloud in transit, in memory, and at rest are no longer nice-to-have capabilities; they are considered a must.

Encryption, however, can be a double-edged sword. Organizations need it to ensure the confidentiality of their data in the event it is compromised in an attack. But it also can cause performance and security challenges when companies are defending against possible vulnerabilities and breaches. And encryption alone cannot ensure the legitimacy of the data and prove it has not been altered.

Ultimately, detecting network attacks and responding to them quickly when the data is encrypted can be problematic. For example, if you do not know what the data is, how do you protect it?

One potential solution to the problem is deploying cloud-based network detection and response (NDR) technologies that manage encrypted data packets and other cloud-based data activity. The technology can help security teams respond to possible breaches

OUR EXPERTS: Cloud Security

Deven Bhatt, CISO, Varo Money; former CISO and CPO, Office of the Comptroller of the Currency

Patrick Black, senior advisor and CSO, E2E Global; senior director of technology, Visionary Technology Consultants

Bill Bonney, president and founder, the Cyber Advisory Group

Tom Dugas, CISO, Duquesne University

Steve Hunt, principal consultant, Hunt Business Intelligence

David Levine, vice president, corporate and information security and CSO, Ricoh USA

Cloud security

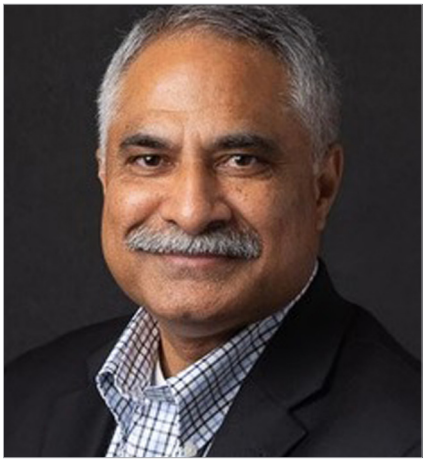
64%

Percentage of U.K. workers who admitted to violating GDPR by sending customer emails to their home email accounts

– Probrand.co.uk

quickly and efficiently, preventing significant losses due to data breaches and other attacks.

Companies are looking into these products and deploying other tools and services to ensure strong cloud security. And whichever path they choose, cloud security is sure to be a major priority for the next few years.



Deven Bhatt, CISO, Varo Money; former CISO and CPO, Office of the Comptroller of the Currency

Cloudy with a plan for growth

It is becoming increasingly difficult to discern where the cloud begins and ends within the typical IT infrastructure today because cloud services have become ubiquitous for many organizations.

Whether it is through software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), or some other derivation, the cloud has taken center stage as a major corporate resource for businesses.

The potential agility, efficiency gains, and cost savings offered by the computing model makes it a compelling choice for many IT shops — in many cases urged on by lines of business eager to provide end users with easier access to applications and data.

> "There are very few instances where data just flows through your network in a permanently encrypted state."
>
> *– Bill Bonney, president and founder, the Cyber Advisory Group*

In an August 2019 report, Portland, Ore.-based technology research firm Canalys said worldwide spending on cloud infrastructure services grew 38 percent year-over-year in the second quarter of this year to $26.3 billion. Total cloud infrastructure revenue grew by $7.2 billion compared with the same period of the previous year, the largest ever quarterly increase in terms of value. This highlights the continued robust health in cloud spending, according to the firm.

And research firm International Data Corp. (IDC) of Framingham, Mass., in a July 2019 study reported that worldwide spending on public cloud services and infrastructure will more than double over the 2019 to 2023 forecast period. At a five-year compound annual growth rate (CAGR) of 22 percent, public cloud spending is estimated to grow from $229 billion in 2019 to nearly $500 billion in 2023.

Three industries in particular — professional services, discrete manufacturing, and banking — are expected to account for more than one third of all public cloud services spending throughout the forecast, IDC says. While SaaS will be the leading category of investment for all industries, IaaS will see its share of spending increase significantly for industries that are building data and compute-intensive services.

Protecting data and applications in the cloud can be a highly complex endeavor, however. That is especially true for hybrid cloud and multi-cloud environments, which many organizations are striving to create.

A June 2019 report by Baltimore-based research firm Cybersecurity Insiders notes that security professionals continue to face a number of major challenges as more organizations move legacy IT operations to cloud infrastructure and applications, and traditional security tools often fall short.

The study, based on feedback from IT security professionals in the 400,000-member Cybersecurity Insiders community, shows that the top cloud security concern is

68%

Percentage of large companies that said they don't understand the importance of DNS for security

– EfficientIP

data loss and leakage (cited by 64 percent).

Unauthorized access through misuse of employee credentials and improper access controls (42 percent) is the single biggest perceived vulnerability to cloud security, tied with insecure interfaces and application programming interfaces (APIs).

Most respondents (54 percent) say cloud environments are at higher risk of security breaches than traditional on-premises environments, a 5 percent increase from a similar report the previous year.

Encryption Pluses and Minuses

As data breaches continue to make headlines — whether the breaches are inside or outside the realm of the cloud — encryption has taken on even greater importance for protecting sensitive data such as customer records.

The security and privacy of data in the public cloud is a particular concern for corporate IT and security executives, especially with the rise of data privacy regulations such as the European Union's General Data Protection Regulation (GDPR).

"Up until the last five years, networks, especially internal networks, were designed with a certain amount of trust assumed," says Bill Bonney, president and founder of the San Diego-based eCyber Advisory Group, a security consulting firm that provides virtual CISOs. He also is a co-author of the *CISO Desk Reference Guide*.

"Once inside the network, it was assumed the data flow was secure," Bonney says. "The same for data at rest. Unless it was highly sensitive, it was assumed safe inside the 'walls' or inside the firewall. We're now designing networks that inherently assume little or no trust, including the zero-trust networks some companies are experimenting with now."

Encryption might or might not be part of that design, depending on what the network is used for, Bonney says. "The upside to encrypting data, in transit or at rest, include the obvious: data presumed to be protected is in fact less exposed," he says.

A less obvious benefit, depending on the nature of the data, is that encrypting data could be either necessary for regulatory compliance or contract requirement, or a significant selling point for customers who want to ensure their data is safe.

> "Reduced performance is one of the trade offs of encryption, but it is marginal and worth the cost."
>
> *– Patrick Black, senior advisor and CSO, E2E Global; senior director of technology, Visionary Technology Consultants*

"The downsides also include the obvious: Technology can be expensive and can slow down transaction volume or transfer speed," Bonney says. "The slowdown can be imperceptible or may render operations inoperative depending on volume and scale."

A less obvious detriment is users can have a lack of visibility into the data that is flowing through a network. "This could be benign, data that isn't really harmful," Bonney says. "It could be harmful, exfiltrating data you wished to be protected; or existential, [a] massive data breach or a complete hijack of your network facilities."

In most cases, the value in encrypting data outweighs the downside of the cost and penalties, Bonney says, because the potential sanctions imposed by regulating authorities and public opinion often are more serious than the costs.

How a company protects data depends on what it is worth and what technical challenges are posed because of the nature of the business. In most cases, organizations need to unencrypt the data to use it, either for internal purposes or for the customer's benefit.

>2700

Number of attempted hack attacks by an Iranian group on US presidential campaigns, journalists and US officials in a 30-day period in 2019

– Morning Consult

"There are very few instances where data just flows through your network in a permanently encrypted state," Bonney says. "Excepting those that process communications packets on behalf of their customers [messaging applications, for example] or cloud storage providers, those points where data goes from the encrypted to unencrypted state and back again give you your inspection window."

Patrick Black, senior advisor and CSO, E2E Global; senior director of technology, Visionary Technology Consultants

This is necessary for data integrity as well as to combat inappropriate activity. If users cannot inspect the data, they cannot clean it or manipulate it to ensure its usefulness.

Besides pre-planned points of inspection for data integrity, the other strategy for addressing this challenge is to be thoughtful about what data needs to be encrypted and how. If the data is not sensitive and not regulated, perhaps locking down the data store itself is enough.

One way to better manage encryption in the cloud is through cloud-based network detection and response technologies that manage encrypted data and other cloud-based data activity.

> "You should take a risk-based approach to deciding what the right controls are and what level and type of encryption is appropriate and reasonable."
>
> *– David Levine, vice president, corporate and information security and CSO, Ricoh USA*

"Cloud-based network detection and response is growing fast and many unique, innovative solutions are available from many different companies," says Deven Bhatt, currently CISO at Varo Money and formerly the CISO and chief privacy officer in the federal Office of the Comptroller of the Currency.

Bhatt researched and reviewed many of these products and continues "to be fascinated by the progress in this domain, where the endpoint detection and response is merging with network detection and response," he notes.

These products provide benefits of predictive detection aided by machine learning, artificial intelligence and significantly higher levels of visibility from a cloud perspective, Bhatt says.

Cloud Security Strategies

One company that is using this technology is E2E Global, a Raleigh-Durham, N.C.-based organization that provides a variety of offerings including rapid-response systems integration and consulting.

The firm is leveraging the cloud for a number of reasons, including reducing its on-premises attack surface by moving its public-facing presence to the cloud using virtual private cloud networks, servers, load balancing, and automation.

E2E has deployed cloud-based network detection and response tools from a combination of vendors, along with custom-built detection and mitigation tools, says Patrick Black, senior advisor and CSO. The fact that these products are based in the cloud is what makes the strategy work.

"Having the tools in the cloud, close to the data they are to protect, is mandatory to ensure high availability and enterprise flexibility and agility," says Black, who also serves as senior director of technology

54%

Percentage of companies that said public cloud management is more difficult than on-prem system management

– ESG

at consulting firm Visionary Technology Consultants in Fulton, Md. "Having access to automation and cutting-edge tools in the cloud also help reduce detection time and thus response time."

E2E Global is striving to create a "centralized security stack," using a transit virtual private cloud from Amazon Web Services (AWS) to route all traffic; moving its security capabilities to a central site in the cloud; and routing all ingress and egress traffic through this central stack.

Tom Dugas, CISO, Duquesne University

The organization is providing publicly accessed sites from the cloud, which allows specific rule sets to focus on threats per application and improves throughput efficiency, says Black.

To better protect data in the cloud, E2E Global is using encryption for data in transit, in memory, and at rest, he notes. The key drivers for doing this include regulatory compliance, industry best practices, and defense against theft or loss of data, Black says.

Deploying encryption of data in the cloud does have its drawbacks. "Reduced performance is one of the trade offs of encryption, but it is marginal and worth the cost," Black says.

Other organizations have not yet deployed cloud-based network detection and response technologies, but are putting together strategies to ensure that data is safe in the cloud.

Duquesne University considers itself an "opportunistic" cloud adopter. "This means that we entertain any and all cloud services if it provides the right value in terms of price, functionality, and efficiency," says Tom Dugas, CISO.

The Pittsburgh-based university is using SaaS, IaaS, and PaaS offerings from cloud providers, for functions including collaboration, email, Web services, backup services, and others.

Duquesne uses encryption in the cloud for data at rest and in transit, Dugas says, and has not seen any significant performance issues as a result of encrypting data.

"Cloud technologies certainly add complexity in terms of security considerations," Dugas says. "Ensuring that our data is secure is very challenging."

The university spends "a tremendous amount of time" on third-party risk management efforts including reviews of the security controls, practices, and policies of the cloud vendors it does business with.

"We also validate those controls and ensure the vendor is following their own policy," Dugas says. "It has added tremendously to our workload when adopting new technologies and services, but it is time well spent."

In order to ensure the confidentiality of its data in the cloud, Duquesne is levering single sign-on tools along with multi-factor authentication (MFA). In some cases, it also uses virtual private cloud designs so that the cloud vendors' systems it uses only communicate directly with its campus systems and services.

As a large global provider of products and services across many industries, Ricoh USA has a variety of cloud architectures including SaaS, IaaS, and PaaS either in place or in the works. The company relies on the cloud both to support its internal operations and to provide services to customers.

To provide security across its cloud environments, the company is using a mix of encryption, email security, cloud access security brokers (CASB), vulnerability scanning, and breach detection and response, according to David Levine, vice president,

49%

Percentage of IT and infosec pros who say their companies employ only native security controls from their email provider

– ESG

corporate and information security and CSO at Ricoh USA in Malvern, Penn.

"As a general rule we encrypt at rest and in transit," Levine says. "However, there can always be exceptions based on factors such as other mitigating controls in place, and/or the sensitivity of the data involved."

David Levine, vice president, corporate and information security and CSO, Ricoh USA

Where appropriate, strong encryption and key control is a significant component of the overall cloud security program, to reduce the risks associated with breaches and to help ensure the confidentiality of data.

"Encryption always carries with it some degree of overhead," Levine says. "Like many implementations, planning in advance is key. If you are building out a new environment, we recommend double checking that you are accounting for the overhead and size all relevant aspects of the [encryption product] to avoid performance issues."

Having a good key management strategy is also important. "You want to be sure you can decrypt the data when and if needed, as well as dutifully protect the keys," Levine says.

Companies might also need to invest in products that allow them to decrypt the traffic as appropriate, given the data involved. "You should take a risk-based approach to deciding what the right controls are and what level and type of encryption is appropriate and reasonable," Levine says. If the data is in the public domain or low risk, then the added overhead and expense might not be justified.

Mastering the Soft Skills

Building a strong cloud security strategy goes well beyond deploying the right tools and services. Security executives need to know how to generate support for cyber initiatives from the highest levels of the organization.

"Those technology leaders who master communications and the 'soft skills' of leadership are the ones who build the most resilient organizations," says Steve Hunt, a principal consultant at Bristol, U.K.-based Hunt Business Intelligence, who advises IT and security executives on leadership skills.

"It doesn't matter how many certifications you have, or how gifted you are as a cloud security architect," Hunt says. "If you cannot sell your ideas to management, if you cannot get buy-in from all constituents, if you do not master the art of dealing with difficult personalities, you will fail at securing the organization."

Among those within an organization who might need to sign off on big cloud projects or help develop the cloud security strategy are IT and business unit leaders, as well as the CFO, COO, and CEO. Each has opinions on what is needed.

"That's a lot of internal politics," Hunt says. "Not to mention IT folks who throw up obstacles or objections. The CISO either [needs to] master these situations, or they change jobs. The fact that most CISOs last two years or less shows you that they are not very good at winning this game."

With the cloud having become a fact of life for many enterprises, learning how to work with in collaboration with all stakeholders in the organization is vital for ensuring data protection in this emerging environment. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at (347) 480-1749, or via email at david.steifman@cyberriskalliance.com.

191

Number of days organizations take on average to identify a data breach, and 69 days to contain it

– IBM

www.scmagazine.com | © 2019 CyberRisk Alliance

Sponsor

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business.

For more info, visit extrahop.com

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@cyberriskalliance.com
SPECIAL PROJECTS EDITORIAL DIRECTOR
Stephen Lawton
stephen.lawton@cyberriskalliance.com
SPECIAL PROJECTS COORDINATOR
Victor Thomas
victor.thomas@cyberriskalliance.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@cyberriskalliance.com

SALES
VP, PUBLISHER David Steifman
(347) 480-1749 *david.steifman@cyberriskalliance.com*
VP, SALES Matthew Allington
(707) 651-9367 *matthew.allington@cyberriskalliance.com*

WILL YOUR CLOUD CONFIDENCE COME BACK TO BITE?

See and stop hidden threats and vulnerabilities with Reveal(x) Cloud,
cloud-native network detection and response.
extrahop.com/cloud

ExtraHop

Rise Above the Noise.