JUNIPER NETWORKS | Engineering Simplicity

eBook

Build a Future-Proof Data Protection Strategy

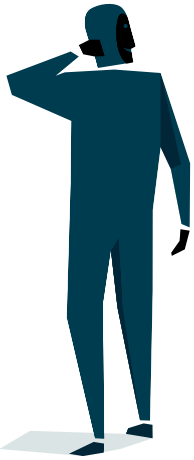
A Juniper Networks eBook

What is data today?

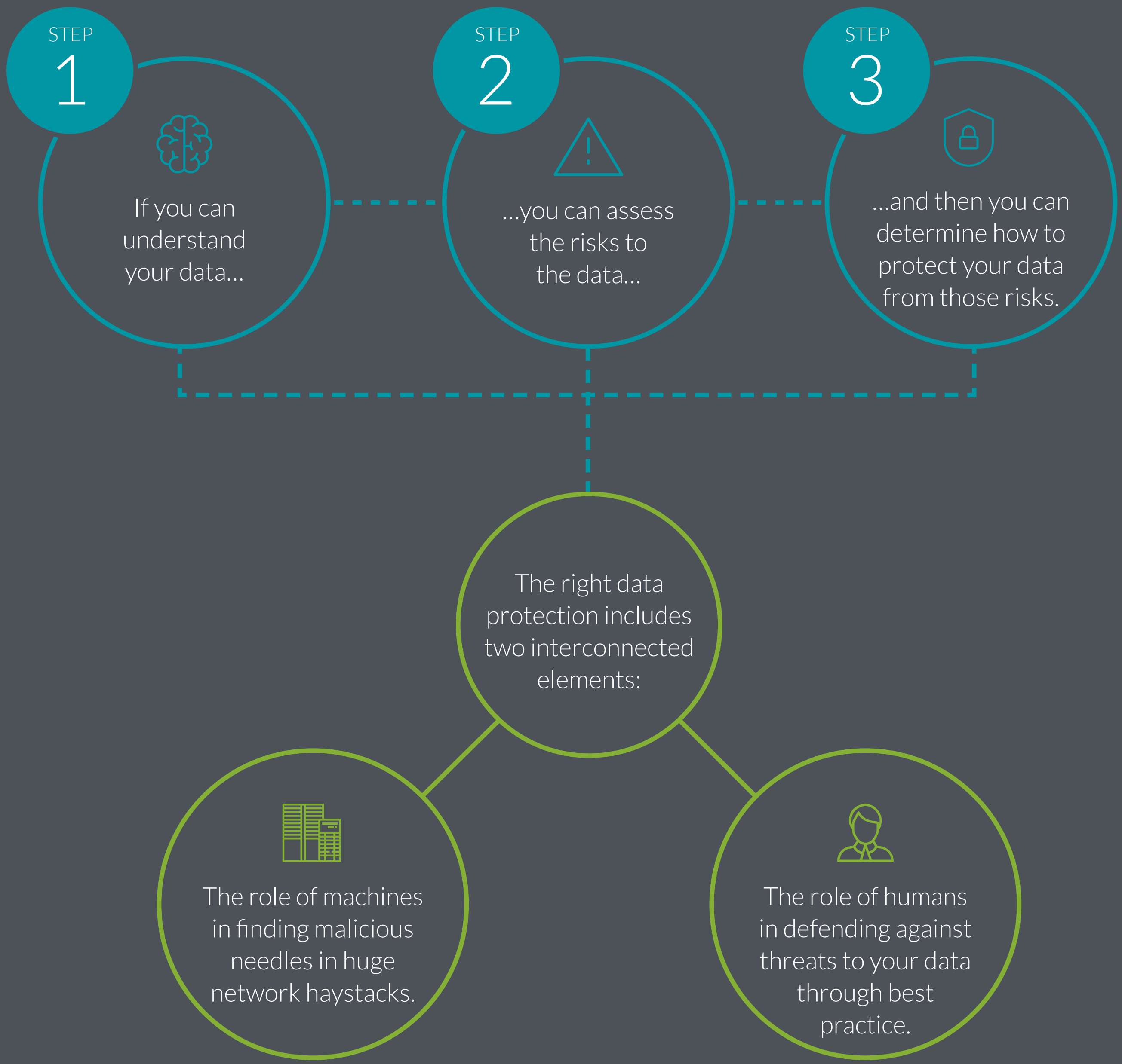
Data is the vital fluid of modern business. Every aspect of business today is kept afloat by data, whether for profit, to innovate, to manage day-to-day practicalities, to communicate or to get ahead of competitors – or perhaps a combination of all of these.

Data has never been more valuable, and in an era of tightened regulation and heightened public sensitivity, protecting data from leaks has never been more important. But if you look beyond the headlines of corporate data breaches and the European Union's **General Data Protection Regulation** (GDPR), what does data protection really mean for your enterprise?

In this eBook, we will highlight several key considerations to help you work out exactly what effective data protection looks like for your organization, from essential enterprise requirements to the potential consequences of leakage. We will then cover several crucial elements of successfully implementing a data protection strategy, including why technology is only part of the answer.



Three helpful steps to working out your data protection needs



STEP 1

If you can understand your data…

STEP 2

…you can assess the risks to the data…

STEP 3

…and then you can determine how to protect your data from those risks.

The right data protection includes two interconnected elements:

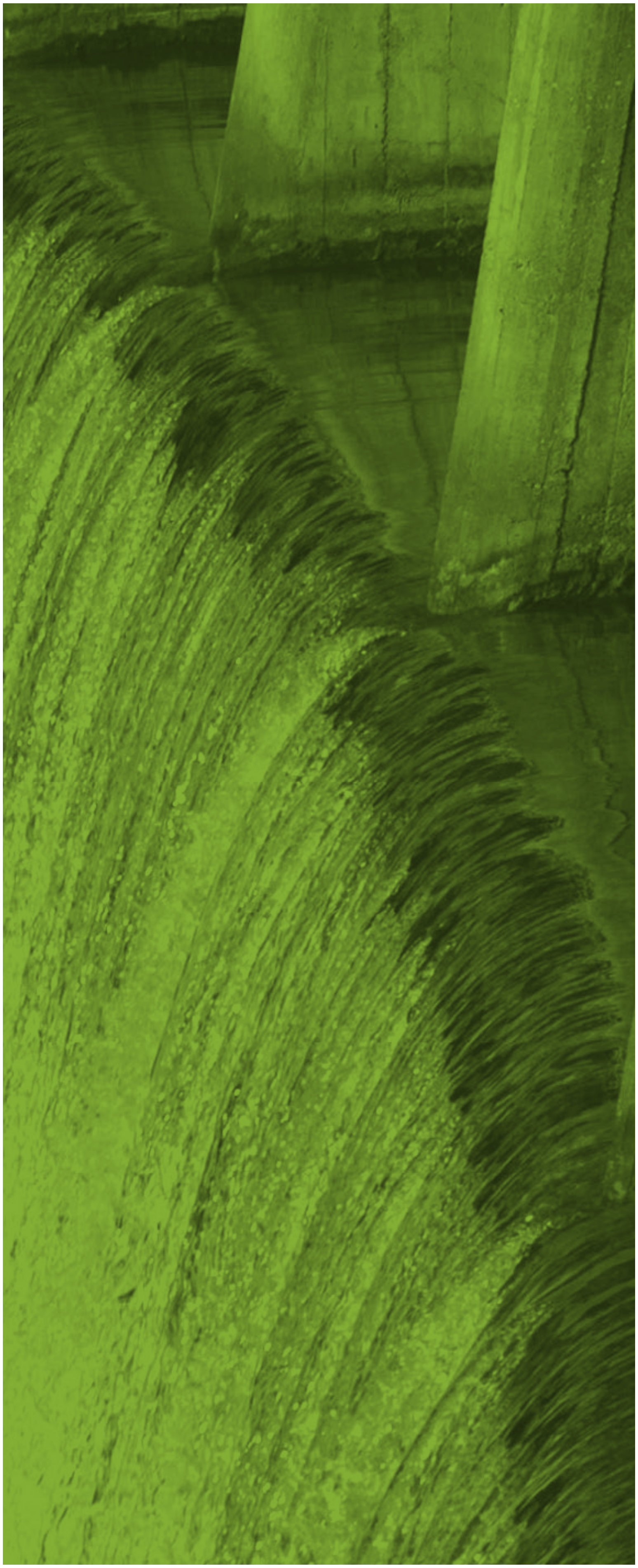
The role of machines in finding malicious needles in huge network haystacks.

The role of humans in defending against threats to your data through best practice.

Step 1: Understanding your data

Before you can do anything around data protection, it is important to establish a foundation and understand what your data is, where it is and what it does. Sounds simple, doesn't it? The modern reality is anything but.

Not so long ago, the typical enterprise's data consisted of simple files in simple databases stored on-premises. Today data comes in a multitude of types, stored on-premises or in the cloud, and is used by – and often shared between – a variety of different applications.



This shift has been organic in order to react to changing business needs, and has taken place alongside a massive, ongoing growth in the volume of data that enterprises must handle. This explosion has forced enterprises to turn to the cloud for reliable and scalable storage capacity, which in turn enables much easier access to data for employees.

The widespread adoption of cloud has created a positive expectation with employees that they will be able to work with their data anywhere, at any time and able to do more with it – but at the same time has also provided the opportunity for departments to spin up new applications without the knowledge, or management, of the IT department.

These factors have contributed to many enterprises dealing with huge, disorganized ecosystems of data and systems over which they don't have full, co-ordinated oversight. Whether it's through cloud applications run by a single department, or data transferred by an employee to a flash drive or laptop's hard drive, enterprise data can now be used, moved or stored more freely and independently of IT than ever before.

So, as the network professional, if you aren't aware of the functionality, location or even the existence of data, how can you take steps to make sure it's protected?

KEY TAKEAWAY

Enterprises are expected to protect every piece of data they have – whether their IT team is aware of its existence or not. Gaining a complete perspective of data – its storage, how it's used and how it flows between departments and applications – is essential for giving context to data protection requirements and measures.

Data’s growing fast…

The global datasphere consisted of **33ZB** of data in **2018.**

That’s expected to rise to **175ZB** by **2025.**

By **2021**, more data will be stored in the public cloud worldwide than in traditional data centers.

…and it will all need to be protected.

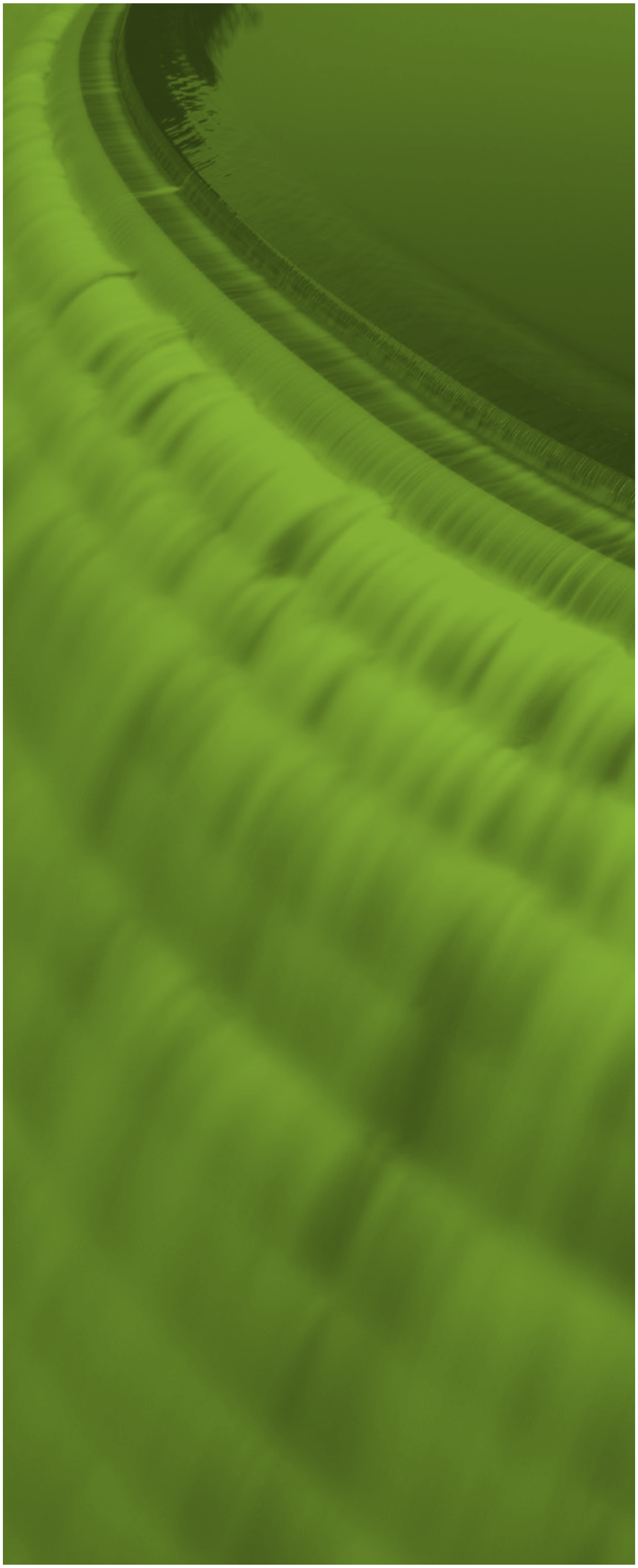
Source: Data Age 2025: The Digitization of the World: From Edge to Core, Report #US44413318, November 2018. Seagate/IDC

Step 2: Understanding the risks to your data

With all that growth comes a danger that you have much more data than you actually need.

For example, someone may be filling in a form on your website to subscribe to your email newsletter. The form you have provided asks them for their name and date of birth, but you do not intend to do any age demographic filtering or analysis. That date of birth is unnecessary information to you, but you're still legally required to protect it if you have it.

And that is just one piece of extraneous data. Think of all the different records and pieces of information you have gathered over the years. You could be holding literally millions of data records that have no positive benefit for your organization, but that could generate huge negative implications if any of them fall into the wrong hands.



Even if you have managed to trim the fat from the data you hold, you still have a huge amount within your estate and unprecedented levels of access to it across your enterprise. In the previous section, we covered the risk of IT teams not having full awareness of all the data within their company – the same principle applies to data access.

Globalized business and the prevalence of cloud mean that databases previously only accessible to a few hundred or even a few thousand users may now be accessed by many – and all of them will have their own ways of doing things. For instance, if they find it too difficult to use the applications provided to access data, they may well store it offline or in their own storage solutions for ease of access, along with all the knock-on risks to data protection, compliance and network security that can bring.

So, what can these risks lead to?

Growth of data, increase of users and lack of user activity awareness are all risks to data protection, and can lead to data threats in one of three ways:

Stolen

Affected data is no longer on the network.

Example:
A hacker removes user information, either to use for malicious activity or to sell for financial gain.

Access Denied

Affected data still exists but access to it has been prevented.

Example:
A hacker is able to deny access to legitimate users and demands money for its restoration.

Changed

Affected data still exists but has been made inaccurate.

Example:
A hacker accesses data and interferes with it to cause disruption to the organization involved.

The weak link in the (supply) chain…

If cybercriminals cannot gain access to your data through your system, they will target your supply chain.

Companies in the supply chain may be smaller than yours. This can mean that they either do not have the resources to put similar levels of data protection in place, or cannot handle the complexity of meeting the requirements of several different partner businesses simultaneously. As a result, it can be easier for cybercriminals to steal, stop or change your data by attacking their systems instead of yours.

These kinds of breaches have become increasingly common recently, so protecting your data that is used by other organizations within your supply chain must not be overlooked.

The Five Rs:
The consequences of a data breach

Regulation

The EU's GDPR and similar regulations being introduced worldwide mandate severe penalties for non-compliance, especially where failures result in data breaches.

Redress

Beyond the regulatory fines, enterprises could face financial damage through litigation from customers whose data has been lost or mishandled.

Reputation

Publicity that shows an enterprise to be careless with data can cause huge, long-term and enduring brand damage.

Repair

If hackers have damaged data or infrastructure through their activity, it will likely cost money and resources to fix whatever's broken.

Replacement

Infrastructure proven to be outdated or unfit as shown by an attack will need to be replaced, at a cost of finances and resources to the enterprise.

Malware attacks on businesses cost an average of

$2.6million*

Information loss accounts for

45% of the cost of cybercrime*

KEY TAKEAWAY

Apply the thoughts here to your own data and consider the extent to which a serious data breach could impact your business. This should then frame the levels of protection you need for your data.

*Source: 2019 Cost of Cyber Crime Study, Accenture

Step 3: Protecting your data appropriately

All your data needs protecting, but it does not all need the same level of protection. If you apply maximum security for everything, you risk making the use and flow of data through an organization too difficult and impractical.

The key to finding the right balance is understanding the difference between your high-value data and low-value data:

High-value data is anything you would not want to end up in public, such as:

- Intellectual property
- Personal information about customers
- Payroll and human resources information

Low-value data is anything that the public can and should be able to access freely, such as:

- General product information
- News and press releases
- Released corporate responsibility information

High-value data obviously requires much higher levels of protection. However, the value of data needs to be reviewed regularly, as it can change over time. For example, marketing information about a new product is highly confidential and, therefore, high-value, prior to product launch. However, those materials would be less sensitive once the product is launched.

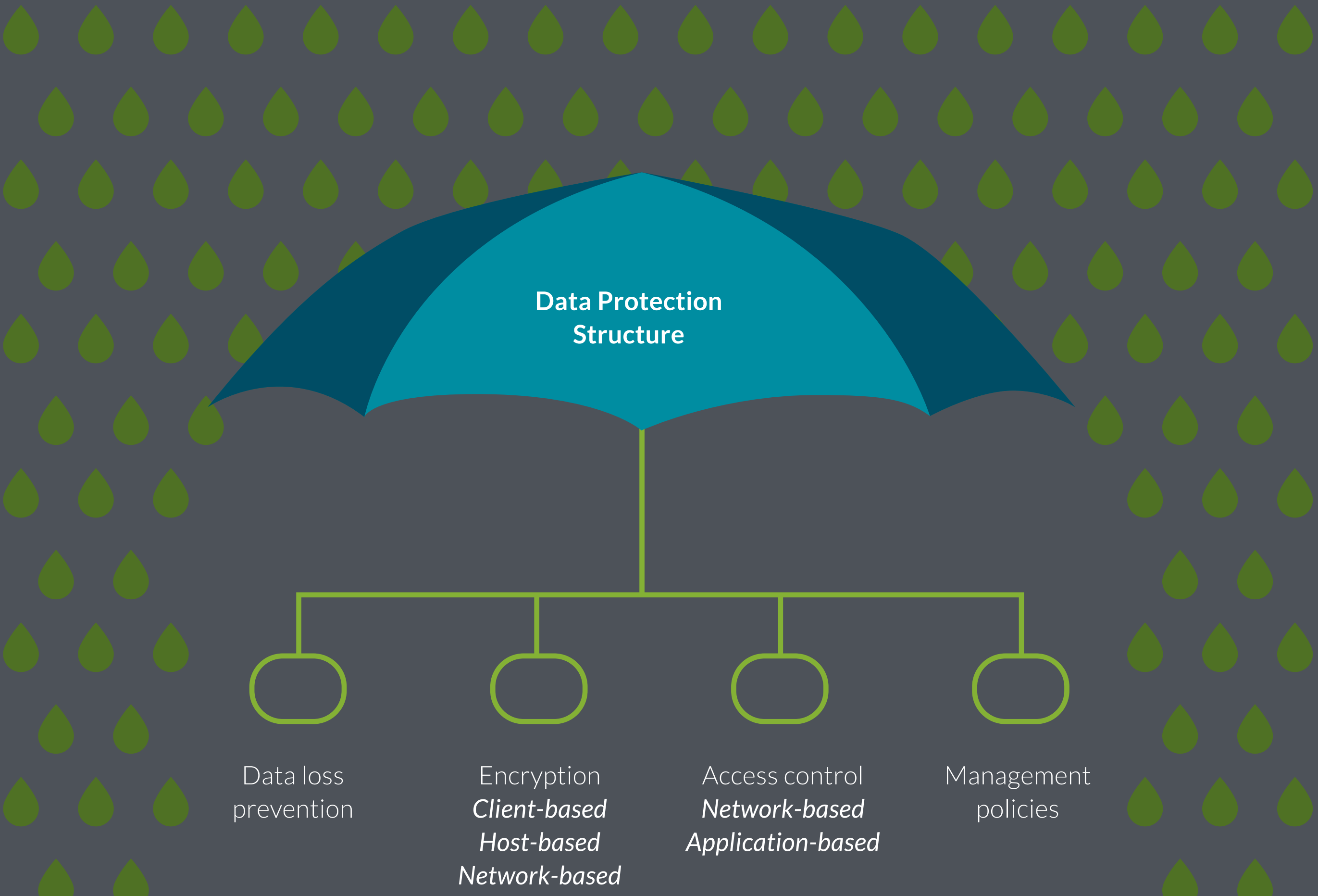
Three key elements of protecting data

1. Access control. Different people within an enterprise will require different levels of access to data, depending on their job roles. At a basic level, people may be able to read data but not modify it. Higher up the chain, modifying rights may be granted. And above that, a small group of senior employees may have additional rights to delete data. Ensuring the right people have the right levels of access at the right times is a constant task, especially to avoid 'toxic access privilege', where people move from one role to another but retain their previous access level that may no longer be appropriate.

2. Encryption. This is essential for high-value data, but how encryption is deployed at different points of data use, storage and transmission processes needs careful consideration, too. For example, different types of data may need to be protected with different kinds or levels of encryption, and the processing costs of actively encrypting and decrypting data in real-time should be considered as well. Encryption is about much more than simple password protection.

3. Version control. Systems that monitor when and how data was last changed can help flag modifications that are unusual. For example, if core files on a website were modified at a time when there was no update planned, that could point towards a wider defacement or attack on the website or network.

What an effective data protection structure should contain



KEY TAKEAWAY

Ensuring the right levels of protection are always in place for the right data is a large and mission-critical undertaking, and one where many data protection projects fail. If done fully and effectively, however, it should provide a long-lasting framework of policies and processes into which future elements can more easily be incorporated.

Finding needles in haystacks: The role of machines in data protection

Now that we have covered several key considerations for achieving effective data protection for your enterprise, we can look at two interconnected elements to help make it work in practice.

A data breach is not a normal situation, and to understand what 'not normal' looks like, first you must define what 'normal' looks like for your organization. 'Normal' is the regular usage of data, as well as its usual flow between applications that legitimately interact with each other based on that data. Knowing what that resembles makes it easier to spot an anomaly, and to quickly find the point where an effective fix can be applied.

Without that baseline, the security posture may have to be unnecessarily strong just to make sure nothing gets through, which would hinder the free and regular flow of data through the business.

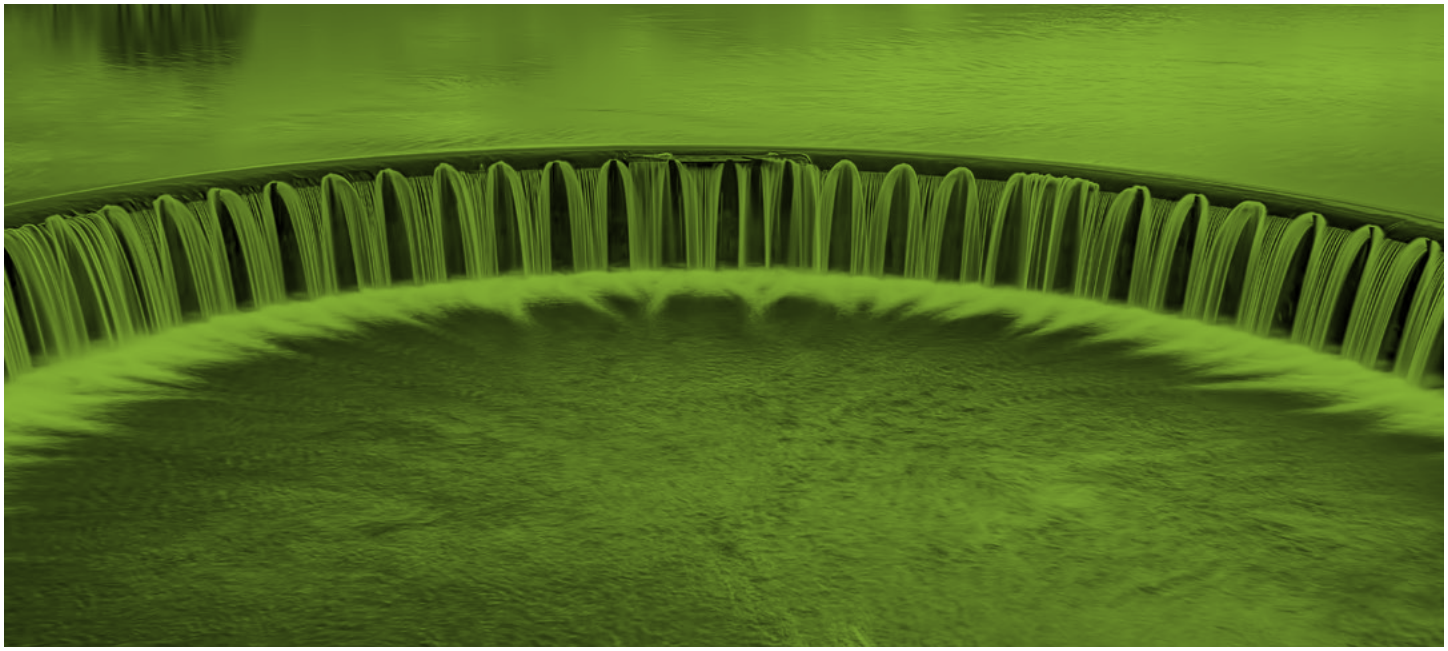
The technical solution: Automation with orchestration

The growth of data, users and networks means that human security teams are being overwhelmed with the sheer volume of things they have to monitor. Faced with huge banks of screens displaying information for hour after hour, alert fatigue makes it easy for anomalous activity to slip through the net. It is not realistic to expect security teams to find every needle in a haystack on their own.

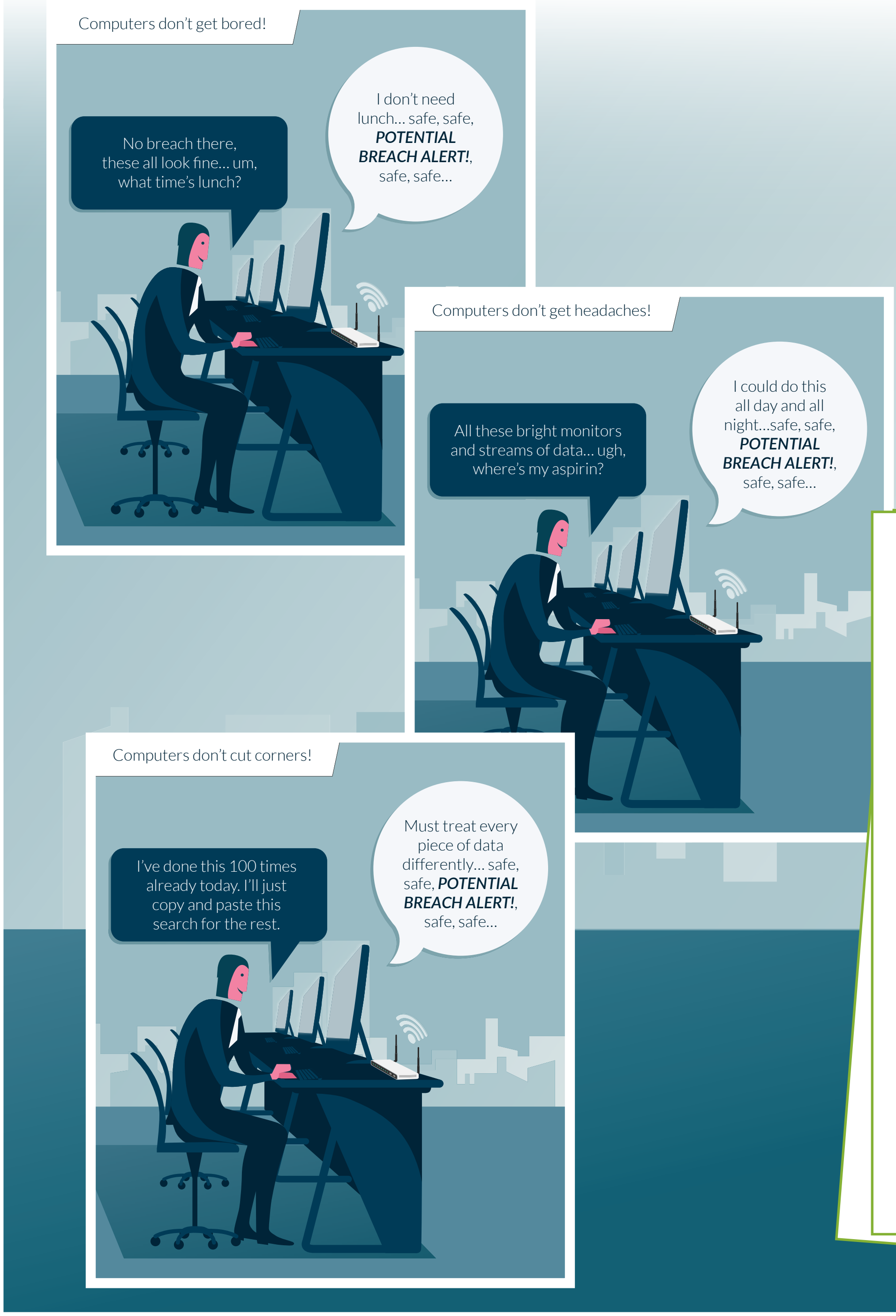
The solution is to use security automation software that can take on the strain of more mundane, repetitive tasks. Automation can learn what's 'normal', quickly and reliably spot things that are 'not normal' and, if they require action, bring them to the attention of the security team. This frees up human resources – an extremely valuable commodity in the modern IT landscape – to focus on advanced threats.

Therefore automation is a real asset to data protection. But it really comes into its own when tied in with orchestration that allows different IT systems – security-related and non-security-related – to communicate with each other. For example, if security automation picks up that there is malware on a workstation, orchestration can quickly cut that device's network access at the switch to prevent the malware spreading. Not only that, it can also cut access for any other devices with which that workstation has communicated.

So, while automation does the hard work of detecting and alerting threats to data, orchestration does the job of extending that protection across all the places your data resides.



The difference automation makes to security


Computers don't get bored!
No breach there, these all look fine... um, what time's lunch?
I don't need lunch... safe, safe, *POTENTIAL BREACH ALERT!*, safe, safe...
Computers don't get headaches!
All these bright monitors and streams of data... ugh, where's my aspirin?
I could do this all day and all night...safe, safe, *POTENTIAL BREACH ALERT!*, safe, safe...
Computers don't cut corners!
I've done this 100 times already today. I'll just copy and paste this search for the rest.
Must treat every piece of data differently... safe, safe, *POTENTIAL BREACH ALERT!*, safe, safe...

KEY TAKEAWAY

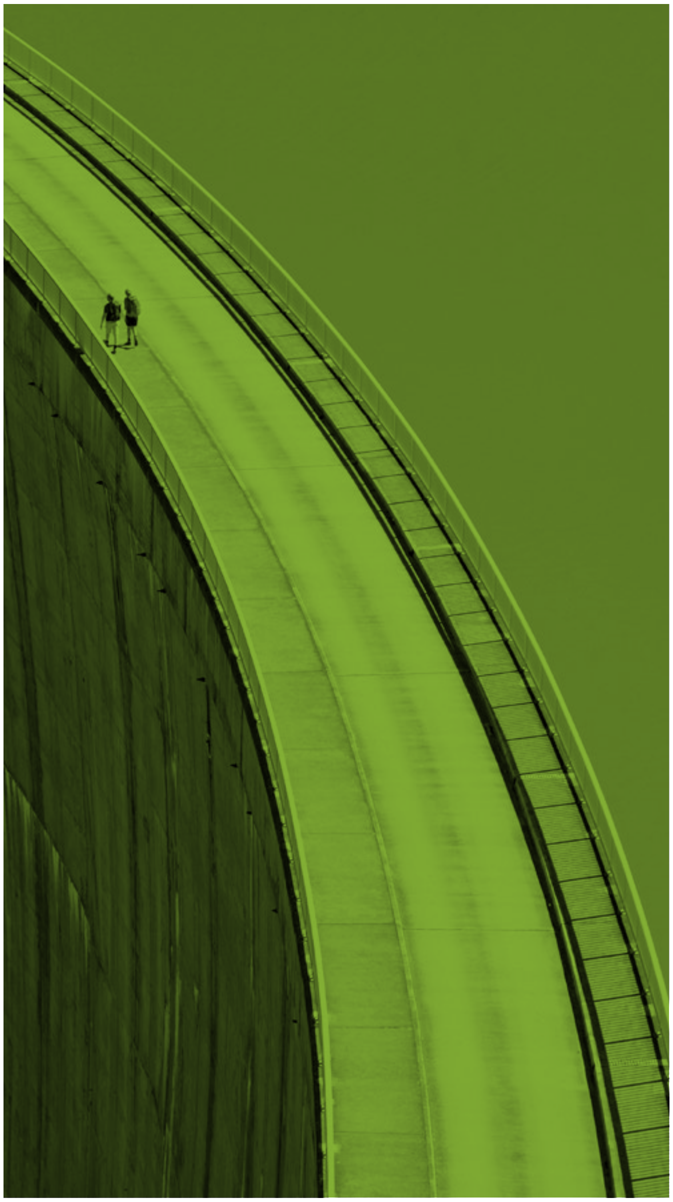
These scenarios are light-hearted, but they do raise a valid point. Security automation can maintain a level of vigilance that even the hardest-working, best-intentioned human security team member simply cannot. A combined approach of automation and orchestration can supply human resources with vital, actionable and consistent security information from across the network, removing the risk of breaches slipping through the net because of alert fatigue and human error.

Protecting against account fraud: The roles of humans in data protection

For all the best automation and orchestration technology in the world, there is only so much data protection can do if an employee opens a malicious email and either clicks on a harmful link or downloads a harmful file.

There are many reasons why these account-based attacks take place. Sometimes, it is 'white-hat hackers' pointing out flaws so they can be fixed, and sometimes it is hackers either being mischievous or trying to build their notorious reputation. But whatever their motives, if they can do it, then cybercriminals who have much more malicious intent – from holding you to ransom all the way to corporate espionage – can do it, too.

Cybercriminals are more sophisticated, organized, ruthless and efficient than ever before, and are often run like enterprises themselves. When they come to attack your enterprise, they will have done their homework. They will already have a clear idea of what they want to target, what they stand to gain from it and how they think they can get there. And that won't always be by trying to break through your technological defenses: they are just as likely to exploit human weaknesses in your systems.



Organized criminals are behind

39%

of data breaches*

*Source: 2019 Data Breach Investigations Report, Verizon

The common types of data fraud – and how to defend against them

Type of attack	Nature of attack	Best practices to avoid infection
Phishing	Untargeted attacks where hackers send millions of malicious emails in the hope that a few people take the bait, innocently respond and provide entry to their corporate network and resources	Contact the alleged sender independently to confirm the email's authenticity Check the alleged sender's email address or URL link closely to ensure that it's correct (hover over the link if necessary) Check the grammar and language within the email to see if it sounds like the normal tone and writing style of the alleged sender
Spear-phishing	Like phishing, but with language and content targeted towards a specific vertical or sector. Emails sent in the thousands but with expected higher success rates	
Business email compromise attacks	Very highly targeted phishing that uses deepfake content, AI and machine learning to create authentic, relevant emails that are extremely convincing to the recipient	
Ransomware	Malware that locks workstations – or increasingly, specific files or applications within a workstation – with demands for payment to unlock the affected areas	
Unauthorized cloud behavior	Employees unilaterally put data in the cloud for ease of access without deploying proper security controls, leaving it open for hackers to exploit and then gain access to other cloud-based confidential data	Strict preventative policies put in place by the business, with heavy penalties for transgressors
Poor password practice	Hackers exploit weak passwords that are easy to guess, or that are easy to find through data access	Stronger password practice (complex passwords, different passwords for different accounts and regular password replacement) Deployment of multi-factor authentication (which is now much more user-friendly than in the past) to ensure only the right users gain access, and to generate alerts if unauthorized access is being attempted
Credential stuffing	Hackers take stolen usernames and email addresses, together with passwords for low-priority accounts, and use them to try and access other, more important, services	

15%

of data breaches are caused through misuse by authorized users*

KEY TAKEAWAY

The frustration with these best practices is that they aren't new ideas. Most people are aware of the dangers of malware and yet many still don't do what's required to keep themselves and their data safe. Improved user awareness and education is an absolute must, to the point where contractually obliging users to follow best practice is worthy of consideration.

*Source: 2019 Data Breach Investigations Report, Verizon

Are you ready for the changing data landscape?

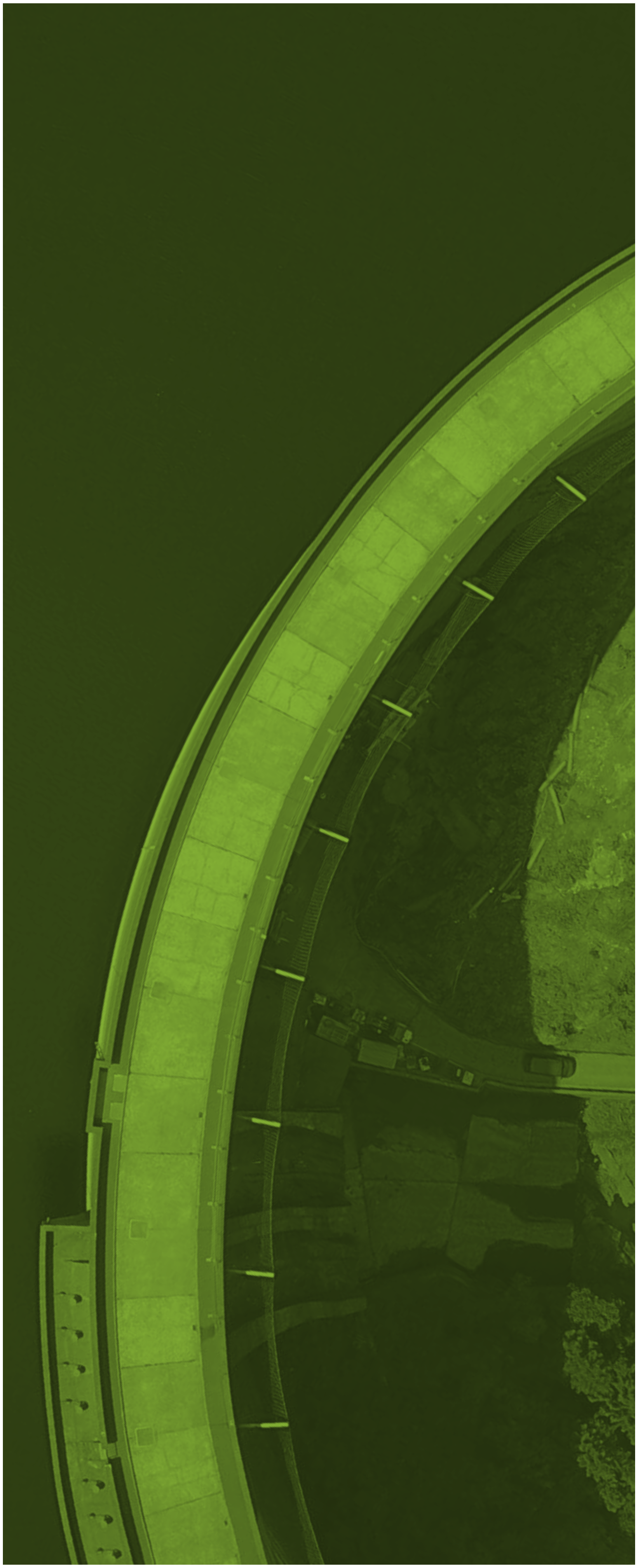
When the GDPR was made enforceable in May 2018, the majority of organizations worked long and hard to adopt its tenets and become compliant. However, now that this initial milestone has passed it is important to ensure data management complacency doesn't creep in. The question of ensuring data protection is as valid today as it has ever been.

Over the coming months and years, data breaches will likely increase in number – hardly a surprise, given the rate at which data will continue to grow. But beyond the big ones that we will see in the news, there will probably be more breaches affecting smaller organizations as cybercriminals target vulnerabilities in cloud solutions.

Because of this, we will see more enterprises being fined for these breaches under data protection regulations – and not only through the GDPR. All around the world, other territories are already developing similar legislation with global reach. For example, in the United States, where the California Consumer Privacy Act has led the way, or Australia, where Breach Notification laws were introduced in 2018.

At the same time, there will be a shift in how user education around data security is treated, from being a noble aspiration to an essential part of employee training. In order to enforce data security standards, it is not out of the question that employees could be held liable and face disciplinary action for their personal lapses in data security best practices.

But if all this sounds negative, it does not have to be. In the short- and medium-term, data protection can actually be a competitive advantage for some enterprises, as those that can demonstrate compliance can inspire customer confidence in their products and brand.



So, what is the answer to all these challenges on the horizon? Juniper Connected Security

Juniper Connected Security is a framework which helps you to understand what needs protecting, and then put in place appropriate controls and processes. This prioritization allows you to focus on the right things and improve their protection as a result.

From a data protection perspective, this means leveraging the intelligence and protection at your disposal as broadly as you can. However, this needs consistency in how controls are applied so that it is effective, efficient and secure. This is where security automation and orchestration play such a vital role.

On a technical level, connected security is a combination of three different activities:

See

Gain full visibility of your data and network.

Automate

Use technology to streamline the application of protection.

Protect

Put the right defenses in place for the right data.

But true Connected Security is more than just joining all the points on your network with technology: it is about connecting the human element of your enterprise, too. This can be deploying valuable human IT security resources efficiently to eliminate the hazards that automation detects, or ensuring the wider workforce is always careful and vigilant in their daily dealings with data. On both counts, humans are just as important as machines in deploying an effective data protection strategy that works enterprise-wide.

Checklist

Use this checklist to guide your approach to establishing effective data protection throughout your enterprise:

☑ Understand your data and network fully

☑ Understand the specific implications to your organization in the event of a data breach or data loss

☑ Develop a comprehensive data security structure with the right levels of protection for different values of data (and be dynamic across its lifecycle, too)

☑ Explore automation and orchestration to relieve the burden on your security teams

☑ Improve user education and awareness enterprise-wide to reduce employee susceptibility to data fraud

Visit Juniper's content hub to find out more about building a future-proof data protection strategy.

www.juniper.net/data-protection

Find Out More

Juniper Connected Security

To make effective data protection a reality for your enterprise, you need a security automation solution that covers every base. One that combines inbuilt threat detection and policy enforcement with the capabilities of partners to safeguard data, users, applications and infrastructure against advanced threats. One that combines automation with a layered approach to defense, so you can respond to both extant and emerging threats, both internal and external.

That solution is Juniper Advanced Threat Prevention (JATP):

- **Fast, flexible defense: protect against malicious activity working alongside any firewall or SIEM device.**
- **Effective detection techniques: stay ahead of the latest cyberthreats and attacks.**
- **Management, visibility and analytics: strengthen your security posture with complete visibility, actionable intelligence and automated enforcement.**

Take a closer look at what Juniper Advanced Threat Prevention can do to help protect your data today.

Request Your Free Trial Now

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way
Sunnyvale, CA 94089 USA

Phone: 888-JUNIPER
(888-586-4737) or +1.408.745.2000

Fax: +1.408.745.2100

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240
119 PZ Schipol-Rijk
Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

PN 7400111-002-EN

Engineering
Simplicity

Please Note:

This guide contains general information about legal matters.
The legal information is not advice, and should not be treated as such.

Any legal information in this guide is provided “as is” without any representations or warranties, express or implied. Juniper Networks makes no representations or warranties in relation to the information in this guide.

You must not rely on the information in this guide as an alternative to legal advice from your attorney or other professional legal services provider. You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this guide.

Information correct at time of publication (April 2020).