Insight and Control

Putting Data Privacy and Protection at the Center of Your Security Strategy
Introduction: The Art of Data Protection

Periods of great change produce great art. They can also drive major business transformation. The COVID-19 pandemic is a crisis unlike anything in living memory. But there are also opportunities for those organizations best able to leverage digital transformation to empower the distributed workforce and lead the way to a global recovery.

These efforts should be based around four key pillars: speed, agility, security and insight. It is security, and more specifically data privacy and protection, that will be the focus of this report.

At the center of any great art you can also find people. And it is the same with data protection. These people are your staff, your partners and your customers. They’re the ones buying your products, making the business more productive, and helping to drive competitive differentiation. It is these “data subjects” whose personal information and IP organizations must find better ways of protecting.

As any great work of art goes through multiple revisions and stages before the finished product is delivered, so data must be managed and secured through its entire lifecycle. For too long, the approach taken by many organizations has been siloed and incomplete, exposing them to reputational and financial risk. This paper will uncover the key data challenges facing CISOs, Chief Privacy Officers and their peers today, and how a more focused, end-to-end lifecycle approach to data privacy and protection can deliver cyber-resilience and be a true platform for innovation and growth.

An Explosion of Data

COVID-19 is putting pressure on IT and business leaders to innovate their way out of global recession. But innovation at any cost will only expose organizations to unnecessary risk. Already, cyber-criminals are looking to take advantage of distracted remote working employees, stretched IT teams and vulnerable endpoints to monetize attacks. Attempts to steal sensitive customer and corporate data and disrupt operations with ransomware have spiked during the first few months of the crisis. Google alone says it has been blocking 18 million COVID-themed malware and phishing emails every single day.

In many ways, these schemes can be seen as part of an overall increase in enterprise threat levels over recent years. A cybercrime underground worth an estimated $1.5 trillion annually provides both a bustling, anonymous marketplace for stolen data and a peerless source of hacking tools and knowledge. Nation state attackers have also become more fearless of late in their targeted efforts to steal from a wide range of verticals.
The results speak for themselves. Some 3,813 breaches were reported in the first half of 2019 alone, amounting to the exposure of over 4.1 billion records, a year-on-year increase of 54% and 52% respectively. In the US alone, an estimated 165 million records were exposed in 2019. Associated costs vary significantly with vertical and geography, but on average are said to be nearly $4 million per breach as of 2019, with the US the most expensive country and healthcare the most costly industry. It’s concerning that on average it takes 279 days to identify and contain a breach.

The rise in data breach volumes is undoubtedly due in part to escalating threat activity. But it’s also the inevitable result of a data explosion which has seen consumer and employee data stored in ever greater quantities by the organizations they work for and interact with. Analysts have predicted that the sum total of the world’s data will grow from 33 zettabytes in 2018 to a staggering 175ZB by 2025, a compound annual growth rate of 61%. Increasingly, this data is stored in the cloud and on mobile devices, where it is at risk of loss or theft. Human error compounds the challenge of data protection. Mistakes such as mis-delivery of emails and misconfiguration of cloud accounts were behind 22% of breaches last year, while malware accounted for just 17%, according to Verizon.

Reducing Risk

The challenge for organizations is in securing data against accidental disclosure or theft, without compromising their ability to use data to generate crucial customer insight and drive productivity. They must do so in the context of a tightening regulatory regime which imposes strict financial penalties for non-compliance whilst hangding new rights to consumers on what happens with their personal information.

Leading the way in this regard is the EU's General Data Protection Regulation (GDPR), which:

- Broadens the scope of what constitutes personal information
- Levies penalties of up to €20m or 4% of global annual turnover
- Enshrines data minimization and privacy-by-design principles
- Allows consumers new rights to access, object to, and request the erasure of their data, as well as have it ported to another provider
- Mandates 72-hour breach notifications to the regulator

The GDPR applies to all EU citizens’ data wherever it is held, making the regulation globally important. But it is not the only one. California’s recently enacted CCPA, India’s Personal Data Protection Bill of 2018, Brazil’s General Data Privacy Law 2018, Turkey’s KVKK, Thailand’s PDPA, and Australia’s Notifiable Data Breaches Act 2017 all contain elements of the EU law. That’s not to mention industry-specific regulations, such as HIPAA for US healthcare providers, which have their own prescriptive requirements.
The bottom line is that organizations must find a better way to reduce risk in this new era of: digital transformation, empowered consumers, stringent data protection regulations, escalating cyber-threats, and IT complexity. This will first require the development of rigorous data privacy and security governance policies that cover the entire data lifecycle, and then investments in a holistic technology platform to automate and optimize the management and protection of this data, wherever it resides in the organization—while enabling its utility and usability.

**Data-Centric Security, End-to-End**

Historically, organizations have struggled to discover, identify and protect data across the entire lifecycle, exposing themselves to non-compliance, reputational and financial risks. Instead, they've focused on protecting data in specific silos or parts of the technology stack—in databases or in storage for example—but not across the whole. Thus, when it moves from one layer to another, data is exposed.

To address these deficiencies, data privacy and security leaders should consider a range of technologies and processes to protect structured and unstructured data, including encryption, masking, policy and governance, classification, pseudonymization, key management, cloud data security, big data security, and access management. But most importantly they must be combined into a holistic framework covering three key areas:

**Find and Analyze**—Quickly and cost efficiently determine which data falls within the scope of the organization's privacy policy and regulations. Use analytics tools to automate the identification of data ready for disposition according to privacy rights, policies, and requirements.
Store and apply policy—Apply and enforce data- and identity-based policies for cost efficiency, and to ensure a quick response to litigation/investigations. Protect personal data from gaps in protection without breaking processes. Investigate security alerts quickly with better insights.

Secure and Encrypt—Prevent unauthorized access to data, and automatically apply data-in-use encryption, tokenization, data masking, and other data protection technologies, to eliminate security gaps and reduce data risk. With this kind of insight and control organizations are able to discover and protect sensitive data and reduce neutralize data breach risks. Sophisticated analysis and classification of data enables effective application of policy to minimize the data organizations hold on customers, partners and employees. This helps to reduce risk further in line with best practices, and thereby ensure that an organization’s most valuable asset doesn’t become its biggest liability.

How Micro Focus Can Help

Micro Focus is uniquely positioned to provide end-to-end data-centric risk management across the three-point framework outlined above. Our industry leading capabilities empower customers to accelerate their privacy controls from data discovery through to governance. Built-in analytics enable customers to automate the: discovery of sensitive data; application of governance policies; and protection of data in use, in transit, and at rest.

Data Privacy Protection framework

97% of companies recognized they were realizing benefits such as competitive advantage or investor appeal from their privacy investments.
Thanks to our comprehensive product portfolio organizations benefit from:

**Personal data assessments:** to determine in-scope data across multiple privacy regulations and apply policy to move, redact, encrypt and/or dispose of it.

**Defensible disposition:** to automatically identify data subject to right to erasure.

**Policy-based governance:** to better manage information and access.

**Field-level Encryption:** to protect personal data without breaking business processes, enables data usability and utility in its protected form, reducing risk from data exposure while supporting data use in business transformation initiatives.

Micro Focus also works with a range of industry leading partners and global consultancies to optimize solution implementation, by focusing on the “people” and “process” of data privacy and protection projects.

The result is a comprehensive, integrated approach to support customers no matter where they are in their data privacy and protection journeys. With Micro Focus in place, your organization can reduce costs and minimize reputational and financial risk, while maximizing customer insight and generating new business value by safely exposing data to the right applications and users.

With this foundation in place, customers have the springboard they need to drive innovation-fueled growth in a new post-pandemic era.

**Powering Digital Transformation**

At Micro Focus we help you run and transform your business. Driven by customer-centric innovation, our software provides the critical tools you need to build, operate, secure, and analyze the enterprise. By design, these tools bridge the gap between existing and emerging technologies—which means you can innovate faster, with less risk, in the race to digital transformation.