White Paper

Security

Securing Innovation

MICRO FOCUS

Table of Contents

Overview

To win in the marketplace, businesses must grow and innovate. To succeed, they must adopt new technologies, innovate with new products, and find new partners to expand their business. All of these activities increase security risk to the business. If these risks are not addressed, breaches of security, and loss of data and intellectual property can cause significant damage to the company's brand and reputation.

Organizations' Challenges Today and the Future

Which of the following is your organization dealing with currently, or in the next 12 months?

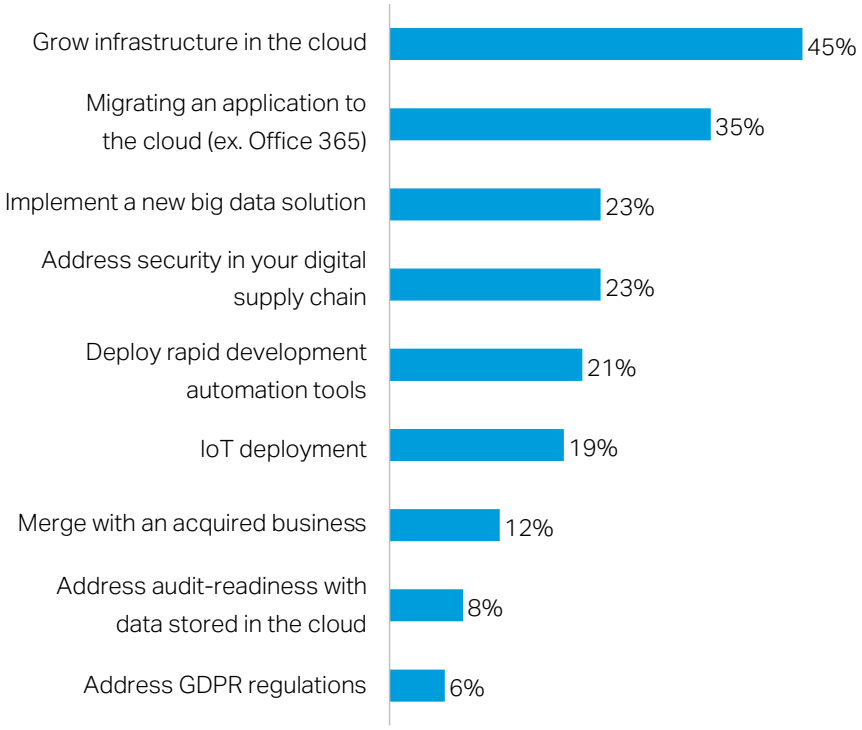
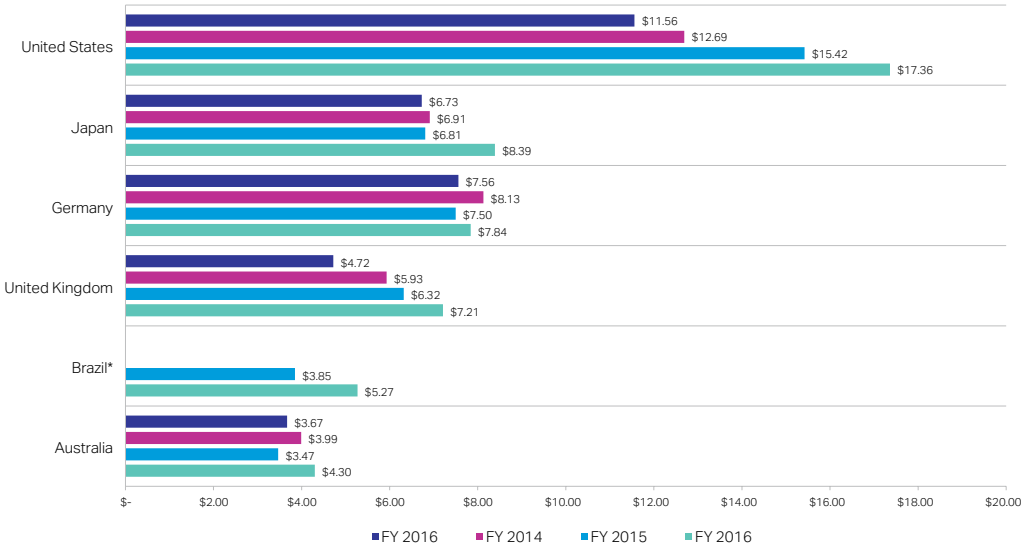


Figure 1. Organizations' challenges today and in the future

Adopting IT Trends: Why Innovation Together with Security Is Important

IT trends are adopted by businesses to increase productivity, profits, and efficiency. To be competitive in the marketplace, organizations must not only innovate to survive and thrive, but they must also be confident that their data, apps, and customers are secure. Security must be an integral part of any innovation program. Without a security component as part of your innovation program, businesses run the risk of data breaches, customer dissatisfaction, and damage to the brand.

The cost to businesses with respect to lost data, revenue, and disruption of operations has only increased. According to a Ponemon Institute, 2016 Cost of Cyber Crime Study & the Risk of Business Innovation shows this rise in the loss of revenue that businesses sustain each year.



*Country-level study was not conducted in the given year.
US $ in millions; n = 237 separate companies

Figure 2. Annual cost of cybercrime

Preplanning with Any Innovation

Before planning projects that embrace innovation, it's important to spend time in the planning phase to evaluate the security aspects of the project so that security is built-in from the ground up.

If you are collecting sensitive data, consider who has access to it and whether you must comply with the myriad government and industry regulations relevant to your business.

"Information loss or theft is now the most expensive consequence of a cyber crime.[1]"
—2016 Cost of Cyber Crime Study & the Risk of Business Innovation

According to a TechValidate study, 63% of surveyed organizations find that the cloud is an important project for their organization this year.[2]

1 **https://software.microfocus. com/products**
2 **techvalidate.com/productresearch/hp-enterprisesecurity/facts/CD2-10C-387**

When in this planning phase, consider how you will protect your data, how you will detect and respond to breaches, and what you will do to recover your business from experiencing a breach.

Innovations or IT Trends

Innovation in IT is continuing at a faster pace than ever, and embracing IT trends is important for business to stay competitive in the marketplace.

Which of the following projects are important in your organization this year?

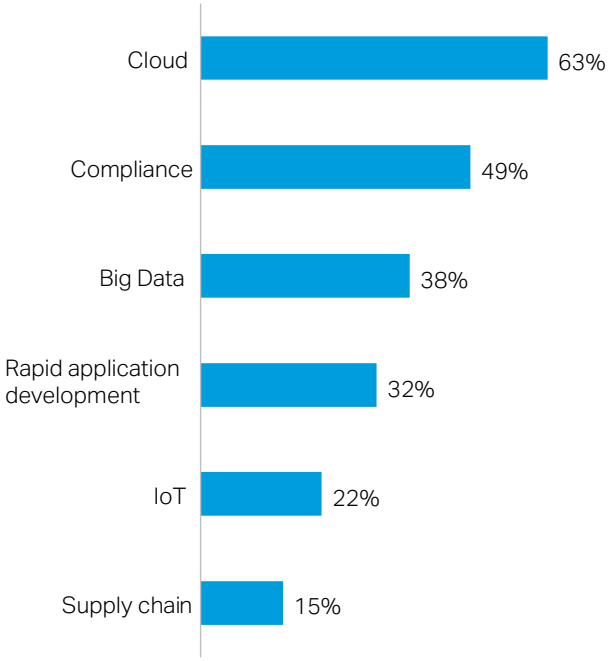


Figure 3. Innovation importance in the coming year

Automation, visibility into what matters most, and changes, expansions, and shifts in how we use and distribute data is continually being transformed by emerging technologies. As important as it is to deliver cutting-edge technologies that drive growth, it is equally important to deliver security alongside those innovations. Innovation without security poses much risk to your business. Therefore, as you adopt new technology into your enterprise portfolio, combine it with a strong security infrastructure to protect your data, customers, and brand.

Cloud

Business customers are asking for the ability to quickly grow infrastructure in the cloud. They need to utilize software-as-a-service (SaaS) applications such as Workday, Salesforce, Office 365, Dropbox, and Google docs, while remaining audit-ready. Transforming to hybrid infrastructure and rapid infrastructure provisioning can empower IT to deliver automated, on-demand infrastructure services in minutes to accelerate time-to-market for new apps and services.

The hybrid infrastructure that cloud technology provides can break down barriers that limit business growth. Businesses are optimizing apps with cloud technology and harnessing the cloud to power traditional applications to deliver increased performance, a superior user experience, and reduced costs. As with any innovation, however, businesses must adapt their existing architecture to meet new demands. The hybrid infrastructure that cloud technology offers also requires new methods of collecting and analyzing data. Businesses need to reconsider not only their existing architecture but also the traditional methods of securing data in a cloud environment.

SECURITY ISSUES

While cloud infrastructure can transform your business, the number one concern of moving to the cloud is security. Trusting a third party with your data is a crucial component of embracing cloud technology, and important questions to consider include the following:

- Who owns the data?
- Who has access to the data?
- Who owns the encryption keys?
- What are the policies?
- Will your company be held responsible if the third-party cloud provider suffers a breach?

RECOMMENDED APPROACH

The reality is that cloud providers are much vested in securing their cloud. Public cloud may even be more secure than your environment. However, even with that reality, organizations must take steps to ensure that security is embedded in any cloud solution. This includes identity management, privacy controls, and data security, and being compliant with legal jurisdictions around the globe.

How Micro Focus Can Help

ENCRYPT DATA

The way you look at the cloud will change the way you look at data security. Best practices include encrypting the data as close to the source as possible, before it goes to the cloud. It should be within audit scope, without losing business functionality with Micro Focus® Voltage SecureData utilizing Micro Focus Format-Preserving Encryption (FPE). Micro Focus FPE protects sensitive data as soon as it is acquired and ensures that it is always used, transferred, and stored in protected form. It uses the National Institute of Standards and Technology (NIST) standard encryption method with a proven algorithm to encrypt data in a way that does not alter the data format. It effectively de-identifies data, rendering it useless to attackers, while maintaining its usability and usefulness.

PROTECT ENCRYPTION KEYS

Protect and manage your encryption keys with Micro Focus Enterprise Secure Key Manager (ESKM). Micro Focus ESKM protects sensitive data-at-rest across storage and server media, including cloud applications. Micro Focus ESKM helps protect sensitive information such as payment cardholder data, customer and employee records, electronic health records, intellectual property, cloud-hosted data, and national security and defense information with strong encryption key management.

MONITOR CLOUD ACCESS AND CONFIGURATION

Build in application security as you spin up a new environment in the cloud with the Micro Focus Security Fortify application security. Azure and Amazon Web Services (AWS) offer elements of Micro Focus Security Fortify application security as part of configuring a new environment. For private cloud deployments, Docker containers can simplify the enterprise-wide deployment of application security agents to monitor custom or third-party applications.

PROTECT EMAIL

Micro Focus SecureMail provides end-to-end encrypted email solution available for desktop, cloud, and mobile that is scalable to millions of users, while keeping personally identifiable information (PII) and personal health information (PHI) secure and private.

IoT

The Internet of Things (IoT) continues to expand to more and more networks and devices. From smart meter monitoring, to bedside devices for healthcare and pharmacy to connected cars, the ease of connectivity that the IoT provides to customers can expand and transform your customer base.

The proliferation of IoT devices also means that businesses need to update and expand their monitoring capabilities and their approach to securing data across an increasing attack surface. As organizations adopt more and more IoT devices, they need more advanced solutions to securely handle the growing amount of data that is produced. From smart meters that need to be monitored for fraud to ensuring HIPAA compliance with IoT healthware devices, companies are becoming more and more concerned about the integrity and safety of their data and apps and want to protect their customers and themselves from pernicious intrusions.

SECURITY RISKS

According to a Micro Focus IoT study, 70% of IoT devices tested raised security concerns with their user interfaces. IoT devices use applications to deliver their functionality, and consumers rely on the IoT device provider to have the whole package tested (software included) to ensure proper security. With this connectivity comes an explosion of data, which introduces threats such as data sets that can be used to identify users and data that can be stolen and distributed. Additionally, especially with healthcare devices, availability of connectivity access and data can be critical, which is why the new Distributed denial of service (DDoS) attacks are so disruptive and damaging.

The additional connectivity that IoT introduces comes with serious risks if data and data pathways are not secure. Increasingly, routers and other IoT devices with no security are being hacked and attackers are able to gain access to wider networks through devices like smart refrigerators. Home security systems have been hijacked to open doors for burglars, and connected cars can be opened with a hacked phone app. The damage to business reputation and loss of revenue can be enormous in cases of hacking.

RECOMMENDED APPROACH

The risks, including uncontrolled access through DDoS (Krebs's recent article on IoT DDoS by trolling default user names and passwords) and sabotage of systems, are too high to ignore the crucial importance of security when connecting IoT devices to wider networks. To ensure that vulnerabilities are not present, these applications must be evaluated and continually monitored for compliance with your security program. Employing encryption, vetting of apps and devices, protecting gateways, and securing IoT data storage are critical aspects of IoT security.

How Micro Focus Can Help

MONITOR IOT DATA

Micro Focus Security ArcSight is designed to ingest logs from IoT connected devices and can handle massive amounts of data that are common in large enterprises. This allows organizations to detect and respond to threats across a wider array of data and connected systems, devices, and applications.

PROTECT DATA END-TO-END

Micro Focus SecureData protects the data end to end with data-centric security. Micro Focus SecureData solutions—including Micro Focus FPE—protect sensitive data from any device immediately and ensure that it is always used, transferred, and stored in its protected form, without breaking existing applications.

EVALUATE IOT APPLICATIONS FOR VULNERABILITIES

Micro Focus Security Fortify or Micro Focus Security Fortify on Demand can rapidly test even third-party apps, identify vulnerabilities, and assess their risk. IoT device vendors can protect their brand by testing an application to identify and address security vulnerabilities. Enterprise application users can use Micro Focus Security Fortify to ensure vulnerability-free IoT devices and applications.

Big Data

Innovation in IT has made it possible for businesses to gather large amounts of data about their customers and the marketplace. Big Data helps business analyze customer behavior and trends, and helps them pivot to customer needs quickly. With the constant streams of data being made available every second, the ability to analyze the data as it arrives is more and more important. This analysis empowers data-driven organizations to respond quickly and make strategic decisions such as assessing risk, analyzing and responding to customer behavior, and detecting failures.

Businesses need secure Big Data solutions to mine the vast amounts of customer data to analyze buying trends or customer behavior. This data may include sensitive PII and PHI data that needs to be in

compliance with security and privacy laws or it may be data in its original format that is housed in a data lake or even in the cloud. They also may need to use live data to test development analytics. The critical importance of safeguarding this sensitive customer behavior can't be overstated. Big Data breaches are on the rise, and potential damage to customer and business reputation is becoming a bigger risk.

SECURITY RISKS

The availability of this data and the ability to analyze it has enormous potential to transform organizations' strategic decisions about their customers. However, the risks are as important to acknowledge as the benefits. How is the data being protected? Protecting confidentiality is vital to protecting your customer and your brand. Risks to using Big Data include unauthorized access, data lake pollution (integrity), exfiltration of large quantities of data, and interception of data as it moves out of storage in and around the Big Data environment. Data is typically exfiltrated through an application, which decrypts data in order to process it. To be protected, you must ensure your application has not been hijacked to behave outside of your control and potentially send data to hackers or act on the data in a malicious manner.

Any organization handling sensitive data in databases today will at some point look at the capabilities Big Data offers for insight and competitive advantage based on existing data assets. Organizations looking to extend data to Hadoop platforms must carefully consider the need to protect data in analytic processes, while avoiding data exposure. At the same time, retaining analytic and logic value of the sensitive information is a critical requirement in any solution. Database-level encryption does not address this need, and only introduces unnecessary overhead.

RECOMMENDED APPROACH

To mitigate security risks for Big Data, it's important to employ a number of safeguards in your security program. These may include protecting and securing your data using encryption, enabling tools for fraud protection, and heightened authentication policies for access. Ignoring the importance of securing Big Data could lead to pollution of a data lake. Take steps to ensure your data integrity.

How Micro Focus Can Help

PROTECT SENSITIVE DATA

Micro Focus ESKM helps protect sensitive data such as payment cardholder data, customer and employee records, electronic health records, intellectual property, cloud-hosted data, and national security and defense information with strong encryption key management.

ENCRYPT SENSITIVE DATA

Micro Focus SecureData Suite for Hadoop protects sensitive data in the data lake—including Hadoop, Teradata, Micro Focus Vertica, and other Big Data platforms. Micro Focus SecureData Suite for Hadoop is a data-centric framework that protects data end-to-end, and delivers secure analytics, enables PCI compliance, scope reduction, and secures PII or PHI for data privacy.

Micro Focus FPE allows data to be encrypted, within audit scope, without losing business functionality, without breaking existing applications. The encryption stays with the data whether atrest, in-motion, or in-use, so if an attacker accesses the data, they get nothing of value. That's the essence of data-centric security.

PROTECT BIG DATA

Micro Focus SecureData Suite for Hadoop with Micro Focus FPE encrypts data, within audit scope, without losing business functionality. That's the essence of data-centric security. A leading healthcare insurance company wanted to open their massive, previously untapped data sets to their Hadoop developers to enable research, discovery, and innovation through developer hackathons. They also had the objective to automate multiple high value use cases, such as identification of prescription fraud, previously hampered by manual processes. Micro Focus FPE technology enabled field-level de-identification of sensitive PHI and PII data across a 1000-node distribution.

INGEST AND ANALYZE DATA

Micro Focus Security ArcSight Data Platform (ADP) allows you to integrate with Hadoop and other technologies to ingest logs and analyze vast quantities of data that are common in large enterprises. Now you can detect and respond to threats across a wider array of data and connected systems, devices, and applications.

DevOps

Application development needs to be modernized to speed business growth. To keep up with consumer trends and to respond quickly to big and fast data, apps are developed faster and faster. To respond more quickly to new opportunities or threats, cloud-native app development and deployment needs to accelerate. The response to this need has been the growing culture of DevOps—the merging of development and operations.

Micro Focus Security Fortify research shows that automation is a key enabler to faster releases and was the number two key characteristic in a DevOps rollout—the first key characteristic was faster releases. However, tool proliferation—which often leads to tool fatigue—was a common thread when discussing automation. When asked what tools are used in support of a DevOps initiative, more than 50 tools were mentioned, and most of these tools play a role in enabling speed and collaboration. The study found that 99% of all respondents agree that adopting a DevOps culture has the opportunity to improve application security[3].

When a DevOps culture is adopted into an organization, it is critical to reevaluate the existing security infrastructure. DevOps can transform application development and speed up the release of new applications. However, changes to how security is embedded into release cycles is critical— including adopting security tools that test applications within the development environment and developing a culture of security within an organization.

SECURITY RISKS

Everyone believes that security should be an integral part of DevOps and that their DevOps transformations will actually make them more secure. However, very few DevOps programs actually have included security

3 **https://software.microfocus.com/en-us/products**

as part of the process because it's a much lower priority than speed and innovation. This problem persists and could worsen in DevOps environments because silos still exist between development and security.

The reality of adoption has proven to be different from the promise. When asked how organizations adopting DevOps currently protect applications, the overwhelming majority cited security practices or controls downstream of the software development life cycle (SDLC), with only 20% stating that **secure SDLC** testing is done throughout development[3]. Most organizations are relying on the technologies downstream, such as preproduction penetration testing and network security.

During qualitative interviews, it became clear that mature security organizations, where application security is historically an integrated part of development, continue to prioritize security and include it as a critical component of DevOps. If organizations were doing it well before, they are most likely doing it well now as part of DevSecOps. However, if they weren't very good at securing the SDLC before, the move to DevOps alone is not going to solve the problem.

RECOMMENDED APPROACH

While securing applications remains a key challenge in most organizations, there are those that have overcome the organizational and process barriers to embed application security into their development lifecycle. Best practices for secure application deployment and better integration between application security and DevOps teams include shared responsibility for security leveraging automation and analytics.

Security should be a shared responsibility across the organization to eliminate barriers. Security must be embedded throughout every stage of the development process, with executive support and metrics to hold teams accountable for secure development.

Bridge awareness, emphasis, and training gaps by making it seamless and more intuitive for developers to practice secure development. Organizations should integrate security tools into the development ecosystem to allow developers to find and fix vulnerabilities in real time as they write code. This makes it easy and efficient to develop securely, and educates the developer on secure coding in the process.

Leverage automation and analytics as application security force multipliers. Organizations should leverage enterprise-grade application security automation with analytics built-in to automate the application security testing audit process and allow their application security professionals to focus only on the highest priority risks. This reduces the number of security issues that require manual review, saving both time and resources, while lowering overall risk exposure.

See how Microsoft responds to the challenges that organizations face in today's modern engineering landscape. The transition included merging development and operations roles and by using agile development principles and tools to shorten release cycles. See the Security for Modern Engineering white paper.

3 **https://software.microfocus.com/en-us/products**

How Micro Focus Security Can Help

BUILD SECURITY INTO THE APPLICATION LIFECYCLE

The Micro Focus Security Fortify ecosystem simplifies how app sec tools are integrated into the DevOps tool chain. Plugs-ins, recipes, and more are made available to help you build security into your applications throughout the SDLC. Micro Focus Security Fortify DevInspect is used to embed security assessments within the developer's IDE. It will identify vulnerabilities as the developer writes the code—for immediate remediation.

CONTINUOUS DEPLOYMENT

Visual Studio Team Services (VSTS) embeds app sec testing into your SDLC to ensure automated build and deployments include automated application security testing.

MONITOR VULNERABILITIES

Micro Focus Security Fortify Application Defender can send application logs and exploit events to Micro Focus Security ArcSight to monitor vulnerabilities in production applications. Meanwhile, Micro Focus Security Fortify Application Defender blocks attacks until the vulnerabilities can be investigated and remediated.

Mergers and Acquisitions

A merger and acquisition (M&A) scenario can bring tremendous growth for a company or companies. Sometimes, this could mean one company buying another to acquire new and innovative technology. Sometimes it could mean two companies merging their operations and supply chains together to form a more powerful and competitive entity in the marketplace. The benefits can include a leap in the ability to innovate and compete, or to become stronger and more resilient in a crowded marketplace.

SECURITY RISKS

Whichever scenario is pursued, the pace of technology has created the need for secure solutions to protect customer data, identity management, and the digital supply chain. When merging with or acquiring another organization, the security risks must be assessed and mitigated. These risks can include insider threats, vulnerable acquired applications, and digital supply chain management.

RECOMMENDED APPROACH

In any M&A scenario, it's critical to take steps to audit for data security, data discovery, and classification. Assess vulnerabilities in applications, monitor high-risk employees, and increase network visibility.

How Micro Focus Security Can Help

ASSESS VULNERABILITIES

Micro Focus Security Fortify on Demand can be used to quickly assess vulnerabilities, and Micro Focus Security Fortify Application Defender protects those vulnerabilities while you decide the proper course of action. Sometimes with M&A, it may take time to retire an app. If you have a major security flaw, you need to manage that risk. With Micro Focus Security Fortify Application Defender, you can protect the flaw while you either remediate it or use it safely until it can be retired. This can buy you essential time to execute your M&A plan while managing risk of acquired applications.

Big Data Needs a Data Centric Security Focus
CISOs should not treat Big Data security in isolation but require policies that encompass all data silos to avoid security chaos. New data-centric audit, protection solutions, and management approaches are required.

Micro Focus Security Fortify Application Defender can send application logs—showing application and user behavior—to any security information and event management (SIEM) or log manager for further correlation and investigation. This can be particularly insightful for insider threats where a legitimate user—or someone using their credentials—is causing the application to behave in a malicious manner.

MONITOR HIGH-RISK EMPLOYEES

Micro Focus Security ArcSight can be used to monitor high-risk employees by setting baselines and alerting abnormal behavior. User behavior analytics can identify suspicious behavior for security analysts to quickly investigate and tack action.

GAIN NETWORK VISIBILITY

Micro Focus Security ArcSight can provide visibility into network assets and monitor for threats and breaches in real time. Increased inputs can increase your organization's situational awareness for fast detection and remediation of security incidents.

Compliance and Privacy Regulations

General Data Protection Regulation (GDPR) sets the foundation for how multinational organizations protect, and derive value from, sensitive customer information. Organizations need to review their entire security posture with a view of understanding the processes and controls needed to be implemented to protect the privacy of European Union (EU) citizens. For example, the EU requires the designation of a data protection officer (DPO) for companies with over 250 employees based in EU, or that process data of over 5000 people per year. Some businesses must prepare for GDPR, others are in the process of collecting EU citizen data and need to comply with GDPR, and some are in the process of hiring a DPO.

RISKS FOR NONCOMPLIANCE

The risks for not complying with GDPR in the EU include high monetary fines and regular data protection audits. The reach of the regulation extends far beyond the EU countries, and organizations around the world will have to comply with the tight data protection and notification requirements:

- Unnecessary data collection
- Short notification timelines
- Continuous audit readiness
- Extent of in-scope data

RECOMMENDED APPROACH

GDPR is not prescriptive in the technologies required to enable compliance, but it strongly hints at the use of encryption and pseudonymization as approaches to protect sensitive data. The following are three main reasons why these technologies receive particular attention in the text of GDPR:

- **Encryption can be used to mitigate the risks** inherent in data processing, such as unauthorized disclosure of, or access to, personal data. Although not explicitly stated in GDPR, the extensive rules around data transfers outside the EU can be simplified by encrypting the data and managing keys in-country (including on-premises).

- **The requirement to notify data subjects (such as consumers or employees) of a data breach is removed if the data is rendered unintelligible** using a measure such as encryption.
- **The use of pseudonymization can reduce the risks to data subjects** while helping data controllers and processors meet their compliance obligations by minimizing both the exposure of personal data and the opportunities to identify data subjects.

Servicemaster Case Study
ServiceMaster deploys cyber-safeguards to enable DevOps speed

How Micro Focus Can Help

Micro Focus delivers a flexible, modular, intelligent set of solutions to help customers identify and take action on customer data in accordance with GDPR.

PROTECT PERSONALLY IDENTIFIABLE INFORMATION

Micro Focus FPE can be used to mitigate the risks inherent in data processing. Although not explicitly stated in GDPR, the extensive rules around data transfers outside the EU can be simplified by encrypting the data and managing keys in-country

Micro Focus SecureData with Micro Focus FPE can protect and encrypt sensitive PII data across the enterprise, at-rest, in-motion, and in-use, to ensure that when a breach occurs the information remains confidential. Micro Focus ESKM helps protect sensitive PII and PHI with strong encryption key management for data-at-rest.

Micro Focus ESKM helps maintain compliance and reduces operational costs with a central management approach by protecting sensitive data with volume-level encryption and integrated key management. If not properly protected, email can be one of the most vulnerable systems in a company's infrastructure. Micro Focus SecureMail encryption protects PII data and ensures that the intended recipient can only read it. Use Micro Focus SecureMail for endpoint-toendpoint encryption for sensitive emails and attachments.

SHORTEN TIME TO INCIDENT DETECTION AND INVESTIGATION

Micro Focus Security ArcSight monitors for security incidents in real time and enables for quick investigation, scope determination, and remediation that can help meet strict breach notification requirements.

REDUCE APPLICATION VULNERABILITIES AND BREACHES

Micro Focus Security Fortify can help protect your organization against security breaches—84% of which are due to application vulnerabilities. GDPR mandates very high fines for breaches. Micro Focus Security Fortify Application Defender can monitor production applications for actual exploits of vulnerabilities that may not have been tested and discovered preproduction. You can take immediate action to block these exploits.

HARDEN APPLICATIONS TO IDENTIFY AND ADDRESS VULNERABILITIES

Micro Focus Security Fortify offers static, dynamic, and integrated application security testing. All of these capabilities can be provided on-premises or on-demand as a service. Ideally, you should test your applications (both custom and third party) preproduction. However, it is inevitable that you will have vulnerabilities in

GDPR Compliance

- Micro Focus—Why the EU's strict data privacy law may be good for global IT security
- Micro Focus—How EU GDPR compliance enables enterprises
- How European GDPR compliance enables enterprises to both gain data privacy and improve their bottom lines
- There's no FUD in GDPR
- EU Data Protection Reform Will Drive Growth in European Security and Storage Markets
- Simplifying GDPR Compliance
- Enable GDPR Compliance Through Innovative Encryption AND Key Management Approaches

your production applications. Micro Focus Security Fortify Application Defender offers Runtime Application Self Protection (RASP) capabilities on-premises or on-demand as a service.

Conclusion

Innovation is a necessity for organizations in today's fast-changing marketplace. To remain competitive and to address customers evolving needs, organizations must evaluate and adopt new IT innovations. You can offer customers a safe environment in the midst of innovation if your security programs evolve and you address security issues from the start. Micro Focus Security can help.

Automation is a huge part of a healthy security program. Using automation to discover and protect code from known threats, frees up your most valuable resources to focus on other aspects of security such as investigation and remediation. With a mature security program and tools in place to help automate scans, organizations can be ready to adapt to changes and shifts in customer behavior and data flows. With Micro Focus security tools such as Micro Focus Security Fortify on Demand and Micro Focus Security ArcSight, your security resources can focus on your larger security program and can devote time to investigation and analysis while Micro Focus tools handle the heavy lifting of scanning millions of lines of code. Used as part of a mature security program, your data will be more secure.

Data-centric security is paramount for enterprises to safeguard data throughout its entire lifecycle, at-rest, in-motion, and in-use. Micro Focus Data Security provides continuous data protection across the cloud, on-premises, and in Big Data and IoT environments.

About Micro Focus Security

Micro Focus Security software products can help secure efforts to adopt innovative solutions that businesses need to adopt to not only stay competitive in the marketplace but also protect customer data and business reputation.

Micro Focus Security ArcSight

Micro Focus Security ArcSight ESM can identify and prioritize threats in real time, so you can respond and remediate quickly. It provides a single pane of glass to connect with Kafka-based data lakes like Hadoop to monitor events and respond to security threats. With Micro Focus Security ArcSight, you can improve security events' response time and productivity. Micro Focus ArcSight ESM helps detect and respond to internal and external threats, reduces response time from hours or days to minutes, and addresses ten times more threats without additional headcount.

Contact us at:
www.microfocus.com

Micro Focus Security Fortify

Test your applications (both in-house and third party) to assess security vulnerabilities. Micro Focus Security Fortify offers testing both on-premises and as a service. Thorough testing includes static, dynamic, and integrated application security testing.

Remediate the vulnerabilities, and if you are unable to do so in a timely manner, use Micro Focus Security Fortify Application Defender to block attacks and protect the vulnerabilities from exploitation. Potential exploits and application logs can also be sent to your SIEM or any log manager for further correlation and insight.

The Continuous Application Monitoring service of Micro Focus Security Fortify on Demand can continuously monitor production environments for new apps and new vulnerabilities. Often shadow IT appears with new applications unbeknownst to IT. Reduce your security risk from these by watching for them, with quick assessments to identify the most egregious security flaws.

Micro Focus Data Security

Micro Focus Data Security protects sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission-critical transactions, storage, and Big Data platforms. Micro Focus Security—Data Security solves one of the industry's biggest challenges: how to simplify the protection of sensitive data in even the most complex use cases.

Learn More At

www.microfocus.com/arcsight