UNIT4

White Paper

How Organizations Can Use The Cloud In Confidence

In business for people.

Safety in the Cloud

According to a recent Forrester Research study, spending on public cloud services is expected to reach $106 billion in 2016, a 21% increase over projected 2015 spending levels.

Movement to the Cloud is happening for many reasons:

- Information is always up to date.
- Provides global access, 24x7, from any location or device.
- Presents a simple pay-as-you-go cost model.
- Enables a solutions to easily transform as business needs change.
- Built-in disaster recovery.
- Provides IT with greater agility.

More and more organizations move to the cloud and use its speed, scale and economic benefits to transform their business. This may include reshaping how they engage with customers, enabling employees to do more productive work and driving new and more rapid sources of innovation. The scale and reach of the Cloud, for example, is helping companies leverage massive amounts of data to provide better business insights. Mobile employees are sharing data and applications to improve collaboration, productivity and overall work effectiveness. Executives are developing new business models and inventing new service-based revenue streams.

Despite these clear advantages, some organizations still have concerns about security, privacy and compliance. Cybersecurity has been elevated to CEO and Board-level attention because of its proven potential to negatively impact a company's brand, market share and revenues. This is why choosing the correct cloud option is imperative to your organization's strategy.

The ComputerWorld Forecast Study 2015 found that cloud computing initiatives are the most important project for today's IT departments.

Caution is not unreasonable

News of security breaches continues to dominate headlines and the scale and scope of intrusions are growing. In 2014 alone, data breaches were up by 49% over the previous year and cyber criminals compromised more than a billion data records in more than 1500 breaches (Gemalto, 2014 Breach Level Index Report). While acknowledging that the Cloud can provide increased data security and administrative control, IT leaders are still concerned that migrating to the Cloud will leave them more vulnerable to hackers than their current in-house solutions.

In a global survey of over 2600 IT decision makers, from their "Trusting the cloud" Whitepaper, Microsoft recently found that security, privacy and data control top the list of most pressing business considerations for using the public cloud.

The expanded opportunities of the Cloud have introduced new risks and complex challenges. This raises the importance of privacy and security. Cyber criminals are finding new ways to disrupt commercial and government activities so organizations that adopt the Cloud to modernize their business should demand more control and involvement in how their data is managed and used.

Privacy challenges

Cloud services raise new privacy challenges for businesses given the scale at which public cloud operates. As companies look to the Cloud to save on infrastructure costs and improve their flexibility and agility, they also worry about losing control of where their data is stored, who has access to it and how it gets used.

Even as they enthusiastically exploit the Cloud to deploy more innovative solutions, companies are concerned about losing control of their data, retaining ownership of their data and being responsible for things they cannot control. Many companies are, therefore, looking to choose where their data resides in the Cloud and to control what entities have visibility into that data.

Introducing Unit4's safer cloud

Unit4 already supports over 1000 customers in cloud environments. In July 2015 Unit4 announced an alliance with Microsoft to bring 'Self driving' ERP to people-centric organizations. Azure is Unit4's strategic public cloud deployment platform. Azure enhances Unit4's offering through flexible security, data privacy and residency. With a deep understanding of the challenges facing the modern enterprise, Unit4 business applications with Azure offer highly scalable ramp-up and ramp-down capabilities and provide customers with the flexibility and adaptability they need to run their business without disruption.

Our solutions enable you to secure your private data and adhere to the highest standards of security, compliance and data privacy. This is designed to work not only for technology improvements that secure and protect, but also for updated regulatory requirements and standards, for transparency of process and approach, for proper auditing and, where necessary, for challenges to outdated laws that have not kept pace with the innovation and transformation of cloud computing.

Unit4's Cloud principles

Security	Privacy & Control	Compliance	Transparency
			
We implement strong security measures to safeguard your data.	We provide you with control over your data to help keep it private.	We help you meet your specific compliance needs.	We explain what we do with your data in clear, plain language.

Move to the Cloud with confidence

Few organizations can replicate the technology and operational processes that Unit4 delivers by leveraging Microsoft Azure technology to help safeguard its enterprise cloud services while complying with international standards. When organizations use Unit4's SaaS cloud deployment, they also benefit from Microsoft Azure's scale and experience of running highly secure and compliant online services around the globe. This is where Unit4 customers particularly benefit.

Your security

Microsoft Cyber Defense Operations Center (CDOC)

Microsoft Cyber Defense Operations Center (CDOC) is a 24x7x365 state-of-the-art cybersecurity and defense facility. The CDOC is part of Microsoft's initiative to continuously advance its efforts on cybersecurity, risk management and data protection. The CDOC is the physical hub for Microsoft's real-time security-focused experts, leveraging technology and analytics that protect, detect and respond to threats to Microsoft's cloud infrastructure. The teams that come together in the CDOC manage intelligence collection and correlation from a global threat landscape, real-time analysis and incident response and provide ground zero security crisis management when needed.

Microsoft's Cyber Defense Operations Center

Secure design and operations

Unit4 creates, implements and continuously improves security in our software development, operational and threat mitigation practices. We embed security requirements into our software and services through the planning, design, development and deployment phases. Our SaaS Ops team works together with the R&D teams across the world to identify, mitigate and share information about known risks.

Continuously tested and evolving security

Threat modeling, static code analysis and security testing are useful in enumerating, reducing and managing attack surfaces — but they do not eliminate all security risks. To uncover unforeseen vulnerabilities and refine our detection and response capabilities, we are continually looking into how our services can potentially be breached – and acting accordingly.

The SaaS Ops team that closely monitor and secures Unit4's SaaS operations (cloud infrastructure, cloud services, products, devices and internal resources) continually simulate real-world breaches — testing penetration and improving our ability to protect, detect and recover from cyber threats.

Threat detection, mitigation and response
As the number, variety and severity of cyber threats have increased, so has our diligence in threat detection and response. Centralized monitoring systems provide continuous visibility and timely alerts and additional monitoring, logging, and reporting capabilities provide visibility to customers. Frequent application of security patches and updates helps protect systems from known vulnerabilities. Intrusion and malware detection systems are designed to detect and mitigate risks from outside attacks. In the event of malicious activity, our 24x7 incident response team follows established procedures for incident management, communication and recovery. The team uses industry best practices to alert both internal teams and customers. Finally, security reports monitor access patterns to help proactively identify and mitigate potential threats.

> "75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching."
>
> ***CyberEdge Group, 2014 Cyberthreat Defense Report, No. America & Europe***

Data protection
Data is the currency of the digital economy and we take the responsibility of protecting customer data very seriously. Both technological safeguards, such as encrypted communications and operational processes help keep customer data secured. In the Cloud, data from multiple customers may be stored on the same IT resources. Unit4 uses logical isolation to segregate each customer's data from that of others. To protect static data, we use industry-standard encryption methods such as whole disk and whole database encryption to protect disk volumes and databases. For data in transit, Unit4 uses encryption protocols to protect customer data as it travels from user devices to data centers, from your data center to Azure, or between servers within the Microsoft cloud.

Network protection.
The increasing sophistication of cyber threats makes it vital for us to provide secure connections, both within the Azure cloud infrastructure we use and between your data centers and Microsoft Azure. Unauthorized traffic to and within Microsoft Azure are blocked using a variety of technologies such as firewalls, NATs, Virtual Networks and physical separation of back-end IT resources from public-facing interfaces. Built-in cryptographic technology makes sure communication is encrypted between data center regions and from our Azure to your on-premises data centers. Customers can also use an optional Express Route private fiber link into Microsoft data centers to keep their traffic off the Internet.

> "If you're resisting the Cloud because of security concerns, you're running out of excuses.."
>
> ***Forrester Research***

Identity and access
Managing who has access, what level of access, to what information, from what locations and devices, are all critical elements of your security policy. Unit4's software helps take care of that, but it is necessary for customers to have access controls in place and live by these controls.

Microsoft Azure Active Directory provides a comprehensive identity and access management solution for the Cloud. For example, Unit4 has integrated identity management into Unit4 Business World for use across multiple devices. Multi-factor authentication reduces organizational risk and helps enable regulatory compliance by providing an extra layer of authentication, in addition to a user's account credentials, to secure employee, customer and partner access.

Unit4 supports authorization based on a user's role, simplifying access control across defined groups of users. Unit4's administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Audit trails are an integral part of Unit4 Business World delivering information on who changed what.

Protecting your data privacy

Clear guidelines and choice for data location

For many organizations, knowing and controlling the location of their data can be an important element of data privacy compliance and governance. We share high-level information concerning the geographic location of where your data is stored. Data may be replicated within a selected geographic area for redundancy but will not be transmitted outside it.

Regions where data can reside are:

AZURE REGION	LOCATION	AZURE REGION	LOCATION
Central US	Iowa	East Asia	Hong Kong
East US	Virginia	Southeast Asia	Singapore
East US 2	Virginia	Japan East	Tokyo, Saitama
US Gov Iowa	Iowa	Japan West	Osaka
US Gov Virginia	Virginia	Brazil South	Sao Paulo State
North Central US	Illinois	Australia East	New South Wales
South Central US	Texas	Australia Southeast	Victoria
West US	California	Central India	Pune
North Europe	Ireland	South India	Chennai
West Europe	Netherlands	West India	Mumbai

Scheduled for 2016 are Germany, UK and Canada.

Restricted access

Access to customer data by Unit4 (or Microsoft) personnel is restricted. Customer data is only accessed when necessary to support the cloud service. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of the service, or improvement of features that protect and detect against security threats (such as malware or spam). Access is carefully controlled and logged, and such reports are audited. Within Unit4 Business World audit reports are available and provide information about who has application level access to data. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Unit4 supports using federate authentication and the federated authentication provider can implement MFA/2FA as desired. Access is revoked as soon as it is no longer needed. Unit4 doesn't capture, maintain, scan, index or mine enterprise customer data for any advertising or similar commercial purposes.

Notification of lawful requests for information

Unit4 responds to valid legal requests for customer data. When contacted by law enforcement with a demand for customer data, Unit4 will make all attempts to redirect the law enforcement agency to request that data directly from the customer. If compelled to disclose enterprise customer data to law enforcement, Unit4 will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so. When appropriate, Unit4 is prepared to litigate to protect customer data from overbroad or invalid government demands.

Contractual commitments

Unit4 provides cloud-service-specific privacy commitments and makes strong contractual promises to safeguard customer data and protect privacy. Unit4 makes the standard contractual clauses created by the European Union (known as the "EU Model Clauses") available to customers to provide additional contractual guarantees concerning transfers of personal data. Unit4 has no need and will not transfer data from US to EU or from EU to US, other than on the customer's written request.

Control over data destruction

When customers delete data or leave a Unit4 cloud service, Unit4 executes a complete deletion of data following service termination or expiration. In addition, Microsoft follows strict standards for overwriting storage resources before reuse, as well as physical destruction of decommissioned hardware. Customers are entitled to take their data with them when they leave. Data portability and transferability is a key attribute in our services to avoid concerns of vendor lock-in.

Enabling compliance

Unit4 and Microsoft are committed to ongoing verification by third party audit firms, and share audit report findings and compliance packages with customers to help them fulfill their own compliance obligations.

Certifications and attestations

As the Unit4 Cloud runs on Microsoft Azure it meets a broad set of international as well as regional and industry-specific compliance standards, such as ISO 27001, FedRAMP, SOC 1 and SOC 2 at the infrastructure control level. The strict security controls contained in these standards are verified by rigorous third-party audits that demonstrate services work with and meet world-class industry standards, certifications, attestations and authorizations. On top of that Unit4 has been assessed by third party auditors to ensure compliance with key cloud service quality and security standards like ISO 27001, SSAE16 type II and PCI DSS.

Maintaining transparency

The Unit4 Cloud is built on a firm belief in the need for transparency. When we hold your data, we will explain what we do with it in clear, plain language. We give you visibility into our operations so you can track issues and have an historical view of availability and any changes to the service. We provide a clear, plain-language explanation of how Unit4 uses, manages and protects your organization's data.

Audit standards certifications

Rigorous third-party audits verify Unit4's adherence to the strict security controls these standards mandate. As part of Unit4's commitment to transparency, customers can verify our implementation of many security controls by requesting customer-facing audit summaries under NDA at Unit4.

Law enforcement requests

Unit4 will never disclose customer data to a government or law enforcement agency except as directed by the customer or where required by law. In response to lawful demands for customer data, Unit4 strives to defend our customers' rights and privacy and to ensure due process is followed.

Breach notification

In the event that customer data is compromised, Unit4 will notify the customer. We have comprehensive, transparent policies that govern incident response from identification all the way through to lessons learned.

Summary

At Unit4, we never take customers' trust for granted. We understand that when it comes to the Cloud trust is paramount, so we take our commitment to protecting our users in today's mobile-first and cloud-first world very seriously. This approach is fundamental to how we provide cloud services and technologies — enabling our customers to move to the Cloud with total confidence.

There are a number of opportunities to learn first-hand about Unit4's commitments and investments in security and privacy technology, practices and policies. For more information, reach out to your Unit4 Account Manager with questions, or to arrange for a meeting that is right for your business.

About Unit4

Unit4 is a leading provider of enterprise applications empowering people in service organizations. With annual revenue north of 500M Euro and more than 4000 employees world-wide, Unit4 delivers ERP, industry-focused and best-in-class applications. Thousands of organizations from sectors including professional services, education, public services, not-for-profit, real estate, wholesale, and financial services benefit from Unit4 solutions. Unit4 is in business for people.

unit4.com

Unit4 N.V.
Papendorpseweg 100
3528 BJ Utrecht,
Postbus 5005
3502 JA Utrecht,
The Netherlands
T +31 (0)188 247 17 77
E info.group@unit4.com