IBM UK Newsroom

IBM Unveils New Mainframe for Encrypted Hybrid Clouds

-- World's most secure server, built for hybrid cloud, available for mid-sized organizations (i) -- System encrypts data at twice the speed of previous generations, new z Systems Cyber Security analytics identify malicious behavior based on learned behaviors (ii) -- IBM and partner security solutions now provide stronger total network protection

ARMONK, N.Y. - 16 Feb 2016: IBM (NYSE: IBM) today unveiled a new mainframe, bringing the security of data encryption without slowing down system performance to mid-sized organizations.

The new system, IBM z13s, is enabled and optimized for hybrid cloud environments and can help secure critical information and transactions better than before. IBM also announced new security partnerships and highly integrated innovations for the mainframe:

- Security embedded into hardware – The new z13s has advanced cryptography features built into the hardware that allow it to encrypt and decrypt data twice as fast as previous generations, protecting information without compromising performance.

- Intelligent security capabilities – IBM is integrating mainframe technology with IBM Security software solutions to create a more secure foundation for a hybrid cloud infrastructure. IBM also is offering a new Cyber Security Analytics service to z Systems customers that can help identify malicious activity by learning user behavior over time.

- Expanded partner ecosystem – IBM is working with leaders in the cyber security industry through the "Ready for IBM Security Intelligence" partner program to help deliver enterprise-wide solutions and offerings tailored to specific client needs. The new partners for z Systems are BlackRidge Technology, Forcepoint (a joint venture of Raytheon and Vista Equity Partners) and RSM Partners.

As digital business becomes the standard and transactions increase, the need for increased security has become paramount. The typical enterprise can face an average of 81 million security incidents annually.iii The incidents and threats are escalating and evolving as companies increase interactions to their network through mobile devices and cloud networks, with industry analyst IDC forecasting 80 percent enterprise hybrid cloud adoption by 2017.iv Cyber criminals nowadays are manipulating data, rather than stealing it, compromising its accuracy and reliability.v The z13s provides access to APIs and microservices in a hybrid cloud setting while keeping data integrity intact.

"Fast and secure transaction processing is core to the IBM mainframe, helping clients grow their digital business in a hybrid cloud environment," said Tom Rosamilia, senior vice president, IBM Systems. "With the new IBM z13s, clients no longer have to choose between security and performance. This speed of secure

transactions, coupled with new analytics technology helping to detect malicious activity and integrated IBM Security offerings, will help mid-sized clients grow their organization with peace of mind."

Mainframe portfolio deepens security capabilities

IBM's z13s, the new entry point to the z Systems portfolio for enterprises of all sizes, is packed with security innovations.

z Systems can encrypt sensitive data without compromising transactional throughput and response time, eliminating what has traditionally been a barrier for IT departments in implementing encryption. The z13s includes an updated cryptographic and tamper-resistant hardware-accelerated cryptographic coprocessor cards with faster processors and more memory, providing encryption at twice the speed as previous mid-range systems. This means clients can process twice as many high-volume, cryptographically-protected transactions as before without compromising performance. This equates to processing twice as many online or mobile device purchases in the same time helping to lower the cost per transaction.

z Systems clients can take advantage of the z Systems Cyber Security Analytics offering, which delivers an advanced level of threat monitoring based on behavior analytics. The solution, being developed by IBM Research, learns user behaviors and is then able to detect anomalous patterns on the platform, alerting administrators to potential malicious activity. Along with IBM® Security QRadar® security software, which can correlate data from more than 500 sources to help organizations determine if security-related events are simply anomalies or potential threats, z Systems now delivers breakthrough intelligent security solutions that offer end-to-end protection based on advanced analytics. z Systems Cyber Security Analytics service will be available as a no-charge, beta offering for z13 and z13s customers.

IBM Multi-factor Authentication for z/OS (MFA) is now available on z/OS. The solution adds another layer of security by requiring privileged users to enter a second form of identification, such as a PIN or randomly generated token, to gain access to the system. This is the first time MFA has been tightly integrated in the operating system, rather than through an add-on software solution. This level of integration is expected to deliver more streamlined configuration and better stability and performance.

Enhanced security for the hybrid cloud

Hybrid cloud infrastructure offers advantages in flexibility but can also present new vulnerabilities. With more than half of all attackers coming from the inside, organizations must automate monitoring, removing human error or meddling.vi To address this, IBM is integrating the mainframe with IBM Security solutions that address privileged identity management, sensitive data protection and integrated security intelligence. When paired with z Systems, these solutions can allow clients to establish end-to-end security in their hybrid cloud environment.

IBM Security Identity Governance and Intelligence can help prevent inadvertent or malicious internal data loss by governing and auditing access based on known policies while granting access to those who have been cleared as need-to-know users. IBM® Security Guardium uses analytics to help ensure data integrity by providing intelligent data monitoring, which tracks which users are accessing what specific data, helping quickly identify threat sources in the event of a breach. IBM Security zSecure and QRadar use real-time alerts

to focus on the identified critical security threats that matter the most to the business.

Security partner ecosystem expands to mainframe platform

Total system security requires deep knowledge of specific industries and threats. That is why IBM is working with other leaders in the field to augment its own solutions. IBM's strategic partnership program for security, "Ready for IBM Security Intelligence," now includes more software applications from key ISVs integrating their solutions for z Systems. As the program extends to z Systems, it will provide an additional layer of protection and access governance to critical applications, resources and data that reside on the mainframe.

- BlackRidge Technology delivers identity-based network security that operates before network connections are established and security defenses engage at the application layer. BlackRidge determines and authenticates user or device identity on the first packet before network connections are established. This provides the equivalent of secure caller ID for the network that allows only identified and authorized users or devices access to enterprise systems, stopping known and even unknown threats.

- Forcepoint's Trusted Thin Client® secures sensitive and mission critical data at the endpoint – where it is most at risk. With a read-only endpoint device, there is no residual data on the device – if compromised nothing can be stolen or leaked.

- RSM Partners offers deep expertise in application readiness, penetration testing and security reviews. It also has software products that help ease security administration and provide dashboards that give a view into an organization's overall mainframe security posture.

Banco do Nordeste, Latin America's largest regional development bank, has purchased two new z Systems to support its growing mobile and banking automation transformations. Security, and specifically fraud prevention, is a primary concern for the bank. With z Systems as a core part of its technology infrastructure, it can use analytics capabilities to detect anomalies and prevent fraud.

"As our business continues to grow, we need a computing platform that can grow with us – while at the same time offering the security and reliability banks require," said Claudio Freire, Superintendent of Information Technology, Banco do Nordeste. "The combination of performance and security on the mainframe with the openness of Linux provides us with an optimal platform to analyze user engagement and manage massive amounts of sensitive client data while keeping it secure."

The new z13s' planned availability will be March of this year. IBM Global Financing leases and payment plans are available from IBM and IBM Business Partners and provide flexible terms and conditions that can be tailored to meet each customer's needs to upgrade from older models to z13s, convert an owned z system to leasing while upgrading or acquiring a net new z13s. Promotional offers include 90 days deferred payment for new credit-qualified customers.

To learn more about IBM Security, visit http://www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

To learn more about the IBM z Systems portfolio, visit http://www.ibm.com/systems/z/ or the IBM Systems blog.

###

Partner Quotes:

BlackRidge

“Key to protecting the enterprise and new cloud deployments is managing access at the earliest possible time based on user and device identity. Even being able to identify endpoints via network scanning can be an entry point for malicious hackers, whose methods are becoming more and more advanced. As a member of the Ready for IBM Security Intelligence partner program for z Systems, we have been able to offer our identity-based network protection for the mainframe to provide a new level of protection against today’s advanced threats.” – *Bob Graham, CEO, BlackRidge Technology*

Forcepoint

“The vast majority of security concerns today revolve around the endpoint device. No matter how secure the infrastructure is, if endpoints are not secure, vulnerabilities exist,” said Ed Hammersla, Chief Strategy Officer at Forcepoint and President, Forcepoint Federal. “By integrating Forcepoint Trusted Thin Client with an IBM z Systems mainframe customers will benefit from a highly secure environment that will help prevent leakage of sensitive data at the endpoint.”

RSM Partners

“Cyber threats are constantly changing and evolving as attackers look for new ways to compromise systems. By working with IBM, RSM Partners is able to use its expertise in mainframe security to help organizations take full advantage of new technology to build comprehensive solutions that stay ahead of new threats.” – *Mark Wilson, Director, RSM Partners*

i Based on Common Criteria EAL5+ security rating for z Systems mainframe; May the Cyber Security Force be with You, a Solitaire Interglobal Ltd study; and 2015 Global Server Hardware and Server OS Reliability Survey, a joint survey by ITIC and Strategy Analytics.

ii Based on IBM tests of z/OS and hardware performance that showed the CryptoExpress5S card to be capable of delivering more than 21,000 full SSL handshake operations per second, per card using System SSL; and internal lab measurements that show the Central Processor Assist for Cryptographic Function (CPACF) has been optimized to provide up to 2.3x faster encryption functions on z13s when compared to zBC12.

iii Based on "IBM 2015 Cyber Security Intelligence Index"

iv IDC, "IDC FutureScape – Worldwide Cloud 2015 Predictions – Mastering the Raw Material of Digital Transformation," Doc # 259840, November, 2015.

v Based on National Security Administration testimony, September 2015.

vi Based on IBM 2015 Cyber Security Intelligence Index.

Related resources

Photo

Enhancing the World's Most Secure System

The z13s introduces new embedded mainframe security features with advanced cryptography features embedded in every chip core and tamper-resistant hardware-accelerated cryptographic coprocessor cards.William Santiago-Fernandez and Brian David Flores both worked to develop the system's embedded advanced cryptography in their roles as cryptographic hardware engineers at IBM's Poughkeepsie, NY site. (Feature Photo Service for IBM)

IBM Unveils New z13s Mainframe

Optimized for hybrid cloud workloads, the new IBM z13s brings the security of data encryption to mid-sized organizations at twice the speed of previous generations. (Feature Photo Service for IBM)

IBM z13s microprocessor chip

The new IBM z13s mainframe features embedded cryptography features that allow clients to process twice as many high-volume, encrypted transactions without compromising performance. The z13s bring the benefits of the mainframe to mid-sized organizations and makes it so that they no longer need to choose between security and performance. (Feature Photo Service for IBM)

The New CryptoExpress5S Card for IBM z13s

The z13s can encrypt and decrypt data twice as fast as previous generations with technologies like the CryptoExpress5S card. (Credit: IBM)
