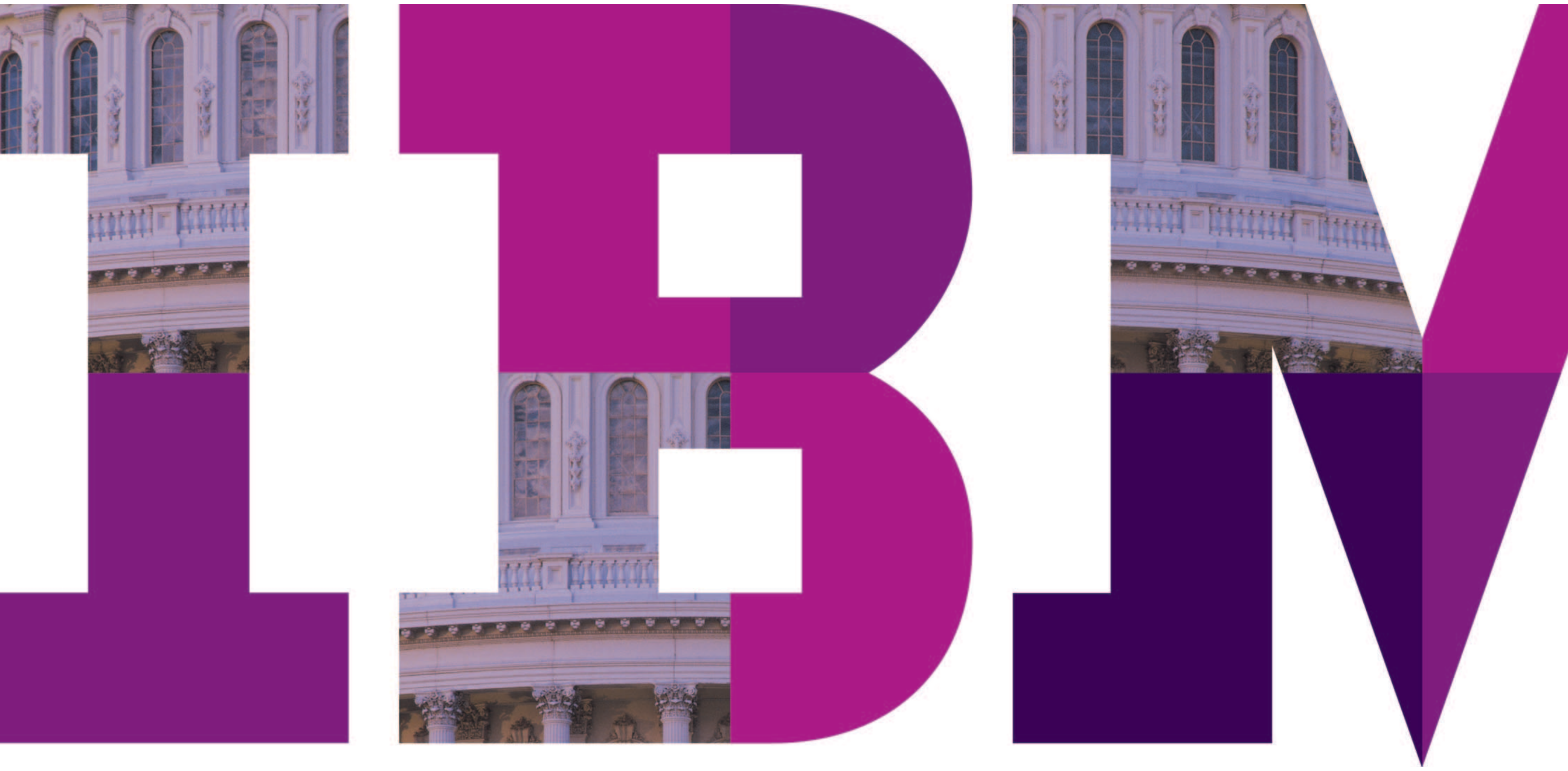
IBM Security products provide intelligence, integration, expertise for federal environments

A comprehensive framework helping secure today's complex federal infrastructures, comprising mobile, cloud, social media and more



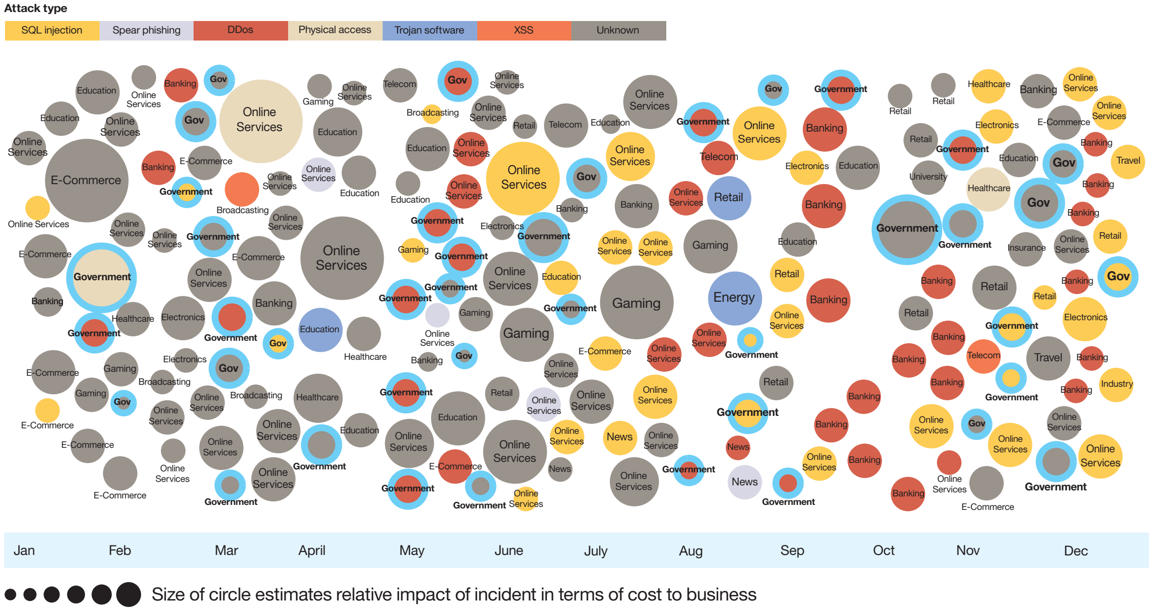
A hyper-connected cyber world

On today's increasingly connected smarter planet, a fundamentally different approach is needed to secure federal infrastructures. The explosion of structured and unstructured data accessed from and stored on virtualized cloud and social platforms, instrumentation, and mobile devices belonging to both the user and the government, creates an overwhelmingly complex IT environment—with unlimited possible attack points. And siloed environments with point defense solutions that make it difficult to share security information to erect and manage comprehensive protection only make matters worse.

Adversaries are now perpetrating sophisticated penetration operations—or *advanced persistent threats*—using focus and persistence to gain access to sensitive data. These attacks, which utilize both old and cutting-edge methodologies, can last indefinitely and are specifically designed and targeted. The increased diversity of today's threats erodes the effectiveness of traditional IT defenses, such as firewalls and anti-virus protection—even bypassing these controls completely in many cases. A new approach is required, one that balances protection with detection, and advanced technology with mature processes. This need is particularly true for government agencies, with their requirements to prioritize the detection of sophisticated cyber threats, meet and exceed stringent compliance mandates, and strive to prevent insider data loss.

2012 sampling of security incidents by attack type, time and impact*

Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



*The circles outlined in blue denote security breaches to the government sector.

Security breaches were heavy and continued to increase throughout 2012—and they show no signs of abating.

Security intelligence for a new world

Only those federal departments and agencies deploying solutions to monitor, correlate and analyze the massive amounts of real-time events and alerts generated from a comprehensive, integrated security infrastructure—as well as from a well-researched external threat feed—possess the capabilities to cost-effectively maintain an extremely strong security posture. IBM calls this *security intelligence*. In addition to helping detect and remediate missed breaches, this approach enables federal organizations to:

- Shift from a traditional, reactive approach to a proactive approach, eventually evolving to a predictive approach that better aligns with mission objectives
- Deploy innovative initiatives faster than otherwise possible
- Automate compliance activities
- Reduce security operations staff requirements

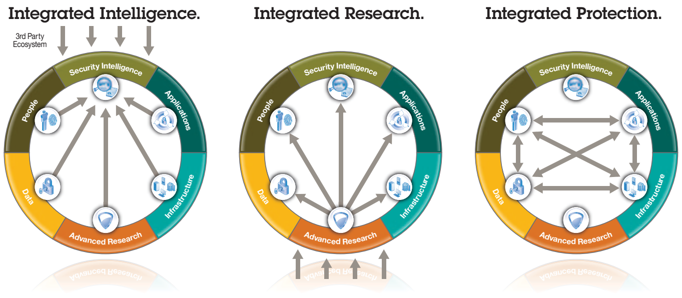
A unique, comprehensive approach

With leading products and services across segments and an overarching strategy based on three main tenets—intelligence, integration and expertise—IBM helps its government customers realize true security intelligence.

Intelligence

Intelligence requires knowledge, information and the ability to analyze this information to reach conclusions. In the realm of organizational security, this translates to needing relevant network, infrastructure, and visibility into external threat intelligence, plus real-time correlation and security analytics to flag and remediate suspicious activities. IBM® Security offers:

- **Internal visibility:** IBM security intelligence solutions analyze information from IBM and non-IBM products and services in real time, providing comprehensive analysis and insight across four key security domains—people, data, applications and infrastructure—measured against risk.
- **External threat visibility:** The IBM X-Force® threat intelligence feed provides critical information from one of the world's largest repositories of threat and vulnerability insights, real-time monitoring of 15 billion security events per day, scanning of more than 20 billion URLs and a constantly updated list of more than 40 million spam sites. This insight flags behavior usually associated with sophisticated threats from a wide range of adversaries.
- **Pinpoint analysis in an age of big data:** IBM security intelligence solutions can drill down to individual data elements to analyze and query diverse activity. They provide insight on network access at the periphery, external cloud services, and mobile devices, as well as database activity, internal and external identity and access management, and everywhere in between.

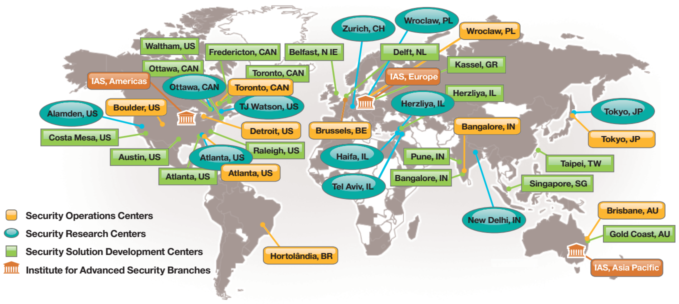


The integration of security intelligence, X-Force research and core protection assets helps close the coverage gaps left by point-product approaches.

Integration

Integrating the comprehensive IBM portfolio of security intelligence, X-Force research and asset core protection can reduce vulnerability compromises and attackable weaknesses arising from cobbled-together security point products. It also can ease deployment, collapse data silos for easier compliance reporting and improved security intelligence, reduce complexity, and lower the cost of maintaining a strong security posture. Other cost-saving and security-improving capabilities include:

- External and internal contextual information for breach detection, prediction and remediation
- Automated device and software updates for researched vulnerabilities
- Authentication and authorization links to suspicious database activity
- Automated compliance and risk assessment activities
- Integrated operational management to decrease staff requirements



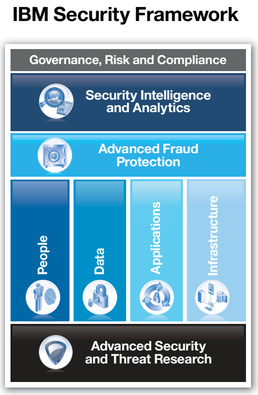
IBM operates one of the world's broadest security research, development and delivery organizations.

Expertise

With more than 6,000 researchers, developers and subject-matter experts engaged in security initiatives, IBM operates one of the world's broadest enterprise security research, development, and delivery organizations. This powerful combination of expertise is made up of the award-winning X-Force research and development team—with one of the largest vulnerability databases in the industry—and includes 10 security operations centers, 10 IBM research centers, 17 software security development labs and the IBM Institute for Advanced Security with chapters in the United States, Europe and the Asia-Pacific region.

Product portfolio

The IBM Security Framework is designed to help ensure the correct people have access to the correct resources at the correct times while protecting critical data in transit and at rest; identifying emerging threats to support breach prevention, internal threats and remediation; and providing protection across all IT resources. This integrated approach to federal security includes appliances, software products and managed services, as well as technical, risk consultation and implementation services.


IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

IBM approaches security by addressing tailored security requirements across multiple domains through integration, intelligence and expertise.

Security Intelligence and Analytics

360 Degree View

Help prevent, detect and remediate security breaches and compliance risks.

Challenge and solutions highlights

IBM security intelligence products assist with:

- **Detecting advanced threats:** Arm yourself with comprehensive and accurate security intelligence.
- **Addressing compliance:** Automate data collection and reporting for audits and risk assessment.
- **Detecting insider threats and fraud:** Identify and understand suspicious user or privileged user activity in context.
- **Predicting risks to your mission:** Proactively identify and prioritize security vulnerabilities and gaps.
- **Consolidating data silos:** Collect, correlate and report on data using one integrated solution.

Products

Integrated security intelligence products based on next-generation security information and event management (SIEM) and log management include:

- **IBM Security QRadar® SIEM:** Security information and event management encompassing log management, threat management and compliance management; sophisticated event and network flow correlation; and network behavioral anomaly detection analysis
- **IBM Security QRadar Log Manager:** Turnkey log management supporting hundreds of data sources out of the box, offering pre-packaged reports and dashboards and easy customization
- **IBM Security QRadar Risk Manager:** Security configuration monitoring and auditing; predictive threat modeling and simulation; and advanced threat visualization and impact analysis
- **IBM Security QRadar Network Anomaly Detection:** Anomaly detection of network traffic and real-time correlation of security and network data, built to enhance IBM Security SiteProtector™ System
- **IBM Security QRadar QFlow and VFlow Collectors:** Integrated network traffic collection and content capture, including Layer 7 application analysis, for both physical and virtual environments
- **IBM Security QRadar Vulnerability Manager:** Integrated network vulnerability scanning and reporting with network context-aware vulnerability management workflow also fully integrated with QRadar SIEM; available as a software option or as an appliance

People

Track
Plan
Enforce

Control, monitor and authenticate user access to protected data and applications.

Challenges and solutions highlights

IBM Security identity and access management products assist with:

- **Managing users and their access rights:** Enroll, manage and terminate user profiles and access rights throughout the lifecycle. Flag expired accounts and role conflicts.
- **Streamlining/tracking user access to protected resources:** Integrate lifecycle access rights with single sign-on, password management, and access auditing and reports. Support strong authentication of devices for extra security.
- **Safeguarding access in cloud, mobile and software-as-a-service environments:** Provide a common identity service for user provisioning, role-based access and federated identity. Centralize security management for user entitlements and policies.

Products

Integrated solutions governing users' access activities and privileges throughout their lifecycle include:

- **IBM Security Identity Manager:** Management of user accounts, access rights, permissions and passwords from creation to termination
- **IBM Federated Identity Manager:** Federated single sign-on for sharing information between trusted business partners and simplifying application integration across distributed portal and mainframe environments
- **IBM Security Access Manager for Web:** Highly scalable user access management and web application protection to guard against advanced threats
- **IBM Security Access Manager for Cloud and Mobile:** Extension of user access protection to mobile and cloud environments using federated single sign-on, user authentication and risk scoring
- **IBM Security Access Manager for Enterprise Single Sign-On:** Integrated authentication, access workflow automation, user switching and audit reporting to simplify and strengthen access security
- **IBM Security Identity and Access Assurance:** Management of user accounts, access permissions and passwords with convenient single sign-on to federal applications and resources
- **IBM Security Privileged Identity Manager:** Centralized management of privileged and shared accounts to monitor the activities of privileged users for more effective governance

Data

Monitor
Encrypt
Assess
Redact

Help protect critical data assets across key control points without impacting productivity.

Challenges and solutions highlights

IBM data security products assist with:

- **Preventing data breaches:** Monitor transactions without requiring changes to databases or applications. Create realistic test sets while masking sensitive data value. Encrypt regulated data to help prevent loss—particularly via theft of backups and media. Redact standalone or embedded unstructured sensitive data in forms and documents.
- **Maintaining the integrity of sensitive data:** Compare all transactions to policy and block violations in real time.
- **Reducing the cost of compliance:** Automate and centralize controls to streamline compliance validation.

Products

IBM InfoSphere® Guardium® offerings designed to assure the privacy and integrity of trusted data include:

- **IBM InfoSphere Guardium Database Activity Monitoring:** A solution to help prevent leakage of sensitive data from databases and files, enable information integrity maintenance in government data centers, and provide compliance control automation
- **IBM InfoSphere Guardium Vulnerability Assessment:** Automated database vulnerability detection with prioritized remedial actions
- **IBM InfoSphere Guardium Data Redaction:** A solution that guards against unintentional disclosure of sensitive data by detecting and removing data from openly shared document versions
- **IBM InfoSphere Guardium Data Encryption:** Encryption for federal data without sacrificing application performance or creating key management complexity
- **IBM InfoSphere Optim™ Data Masking:** Confidential data de-identification to protect privacy and support compliance initiatives

- **IBM Tivoli® Key Lifecycle Manager:**[1] Encryption key lifecycle management with centralized and strengthened processes leveraging the industry-standard Key Management Interoperability Protocol
- **IBM InfoSphere Discovery:** Ability to capture data relationships and determine applied transformations and business rules through data identification, data location and data linkages

Applications

Protect
Test
Control

Help secure, protect and harden applications against attacks.

Challenges and solutions highlights

IBM application security products assist with:

- **Finding and remediating mobile and web vulnerabilities:** Correlate results with static, dynamic, runtime and client-side analysis.
- **Building applications that are secure by design:** Enable effective communication between security and development teams by integrating security testing throughout the design process.
- **Controlling access to application data:** Manage and enforce fine-grained entitlement and security policy management.

Products

Solutions designed to protect your applications include:

- **IBM Security AppScan® Standard:** Automated web application security testing for IT security, auditors and penetration testers
- **IBM Security AppScan Enterprise:** Enterprise-class application security testing and risk management with governance, collaboration and security intelligence
- **IBM Security AppScan Source:** Static application security testing to identify vulnerabilities in web and mobile applications during the development lifecycle
- **IBM Security Policy Manager:** Capabilities for authoring application entitlements and fine-grained access control policies for distributed policy decisions based on identity, transaction and service/resource context
- **IBM WebSphere® DataPower® XML Security Gateway:** A real-time web services security and XML threat protection solution

Infrastructure: Network

Pre-emptive
Fast
Extensible

Help provide security for the entire network infrastructure.

Challenges and solutions highlights

IBM network security products assist with:

- **Keeping pace with emerging threats:** Provide evolving threat protection against zero-day vulnerabilities with network intrusion prevention capabilities.
- **Balancing security and performance without disruption:** Address most demanding service quality requirements, leveraging inspected traffic up to 20+ Gbps, without compromising security breadth and depth.
- **Reducing infrastructure cost and complexity:** Consolidate point solutions and integrate across security solutions to reduce cost and complexity.
- **Protecting non-network assets quickly when new threats emerge:** Protect data as well as client, web and enterprise applications with an extensible engine.

Products

IBM offerings for network infrastructure security include:

- **IBM Security Network Protection:** Core threat protection combined with application visibility and control innovation to reduce risk and conserve bandwidth
- **IBM Security Network Intrusion Prevention System:** Appliance-based network intrusion prevention for core protection against network attacks
- **IBM Security SiteProtector System:** Centralized management with a single point of control for security policy, analysis, alerting and reporting

Infrastructure: Endpoints

Assess
Remediate
Enforce
Report

Help secure and manage distributed endpoints.

Challenges and solutions highlights

IBM endpoint management and security products assist with:

- **Maintaining continuous endpoint compliance, regardless of location or connection:** Deploy an intelligent agent to monitor, report and automatically remediate compliance status.
- **Achieving high patch compliance:** Provide patching capabilities for Microsoft Windows, UNIX, Linux and Mac environments, and for mobile devices, from a single management console and a single management server.
- **Protecting endpoints with rapid response:** Automatically identify rogue or misconfigured endpoints and respond to incidents in minutes.
- **Streamlining compliance and risk-management:** Achieve automated and robust audit and compliance reporting with deep, proactive security configuration auditing.
- **Securing virtualized endpoints:** Obtain a centralized security view of physical and virtual server environments with automatic protection for virtual machines as they come online or move.

Products

IBM offerings that help protect distributed endpoints include:

- **IBM Endpoint Manager:** Endpoint and security management combined into a single solution enabling visibility and control of physical and virtual endpoints; rapid remediation, protection and real-time endpoint reporting; and automation of time-intensive tasks across complex networks to help control costs while helping reduce risk and support compliance
- **IBM Security Virtual Server Protection for VMware:** Protection for every layer of the virtual infrastructure with defense-in-depth, dynamic security with virtual machine rootkit detection, virtual infrastructure auditing and network traffic monitoring through hypervisor integration
- **IBM Security Host Protection:** Protection designed to guard against both internal and external threats for network assets including servers and desktops
- **IBM Trusteer[2] Enterprise Malware Protection:** Protection designed to block execution of files written by malware and stop execution of untrusted code that exhibits data exfiltration, while automating whitelisting of legitimate application states and unifying malware protection for managed and unmanaged endpoints through a single web-based console

Infrastructure: Mainframe

Compliance
Administration

Leverage the mainframe as the enterprise security hub to help protect mission-critical production systems and data.

Challenges and solutions highlights

IBM mainframe security products assist with:

- **Verifying compliance manually, with alerts only after a problem occurs:** Get real-time alerts on external threats, inappropriate data access or misconfiguration with automated compliance monitoring. Help prevent privileged-user abuse by blocking IBM Resource Access Control Facility (RACF®) commands in real time.

- **Coping with the complexity of identifying and analyzing threats in mainframe environments:** Automatically analyze and report security events and detect exposures. Monitor intruders and identify misconfigurations.
- **Maintaining a highly skilled IT staff to provide manual mainframe security:** Simplify RACF administration with a Windows-based graphical user interface (GUI).

Products

The IBM Security zSecure™ suite, designed to provide infrastructure mainframe security, includes:

- **IBM Security zSecure Admin:** Efficient and effective RACF administration using significantly fewer resources
- **IBM Security zSecure Visual:** Reduced need for scarce, RACF-trained expertise through a Windows-based GUI for RACF administration
- **IBM Security zSecure CICS® Toolkit:** Mainframe administration from an IBM Customer Information Control System (CICS) environment, freeing up native-RACF resources
- **IBM Security zSecure Audit:** Automatic analysis of and reporting on security events and detection of security exposures
- **IBM Security zSecure Alert:** Real-time mainframe threat monitoring to identify misconfigurations that hamper compliance efforts
- **IBM Security zSecure Command Verifier:** Policy enforcement supporting compliance with company and regulatory policies by preventing erroneous commands
- **IBM Security zSecure Manager for RACF z/VM®:** A user-friendly layer added to the mainframe that enables superior administration coupled with audit capabilities for IBM z/VM RACF and Linux on IBM System z®

Advanced Security and Threat Research

The world-renowned X-Force research and development team provides the foundation for the IBM preemptive approach to security. These experts focus on researching and evaluating vulnerabilities and security issues, developing IBM product assessments and countermeasure technologies (updated in real-time via the X-Force threat intelligence feed) and educating the public about emerging threats and trends.

X-Force research and development is instrumental in helping protect IBM customers against threats. Its vulnerability database contains more than 74,000 documented vulnerabilities, with detailed analysis of every notable public vulnerability disclosure since 1994. The Trend and Risk Report, published bi-annually, is one of the oldest and most comprehensive security research reports of its kind. It dives deeply into security challenges, including threats, operational and development practices, and emerging trends.

This team also provides insight into and context for security situations that involve suspicious IP addresses. IP reputation data uses threat data collected from myriad sources to categorize IP addresses into separate threat categories. Individual IP addresses are then assigned a reputation score to help determine the risk level for malicious activity. This score is designed to help users prioritize threats and determine which to address first. They can also use IP reputation data to look up IP addresses for security events affecting all traffic coming across the network; next-generation products can block traffic, filtered by category and by user-defined thresholds. IP reputation data is updated every five minutes to provide IBM users with the most current data available.

Certified for federal standards

IBM understands federal organizations' standards and compliance requirements to protect critical—and often classified—data. Thus IBM includes certification roadmaps as part of IBM Security product development lifecycles. Currently, most IBM Security products are certified to many federal standards, including National Information Assurance Partnership (NIAP)/

Common Criteria (CC), National Institute of Standards and Technology (NIST) 800-131A and Federal Information Processing Standards (FIPS) 140-2.

Solutions for today's challenges

The IBM Security Framework, built to deliver security intelligence, helps secure today's and tomorrow's government platforms against known and unknown threats. Today, the biggest security trends and challenges are mobile security, cloud security, big data security, sophisticated threats, and continuous diagnostics and mitigation.

Mobile security

Mobile devices are rapidly gaining popularity in federal environment departments and agencies, due to the productivity and flexible access to information they enable. But unprotected endpoint devices are like open doors into sensitive information. Organizations must guard the data on these devices—whether the data is at rest or in motion over unsecured networks and infrastructure. IBM helps federal organizations embrace both agency- and employee-owned mobile devices in a security-rich environment by providing capabilities including:

- Enabling device security and management
- Guarding secure access to department resources, data and applications
- Ensuring safety for the design, development, testing, delivery, use and management of mobile applications
- Delivering security intelligence via internal visibility and an adaptive mobile security posture

Highlighted products

- Security AppScan Source
- Security Access Manager for Cloud and Mobile
- IBM Endpoint Manager for Mobile Devices

Cloud security

Federal departments and agencies are looking for cloud security solutions to provide visibility, control, isolation and automation across multiple cloud infrastructures. IBM Security solutions help create a cloud infrastructure that can drive down costs while offering dynamic capabilities aligning with today's operational requirements. These solutions enable federal organizations to reduce and manage risks associated with cloud computing by:

- Managing identities and single sign-on access across multiple cloud services
- Monitoring access to shared databases
- Scanning cloud-deployed web applications for the latest vulnerabilities
- Helping defend cloud users and workloads from sophisticated network attacks
- Monitoring cloud-based and traditional resources with a single, unified approach
- Providing endpoint and patch management of virtualized machines for security compliance
- Increasing the cloud activity visibility and enhancing auditing within multi-tenant environments

Highlighted products

- Security Virtual Server Protection for VMware
- Federated Identity Manager
- Endpoint Manager

Big data security

The explosion of federal data is both a significant challenge to manage and a significant opportunity to leverage for security insight. IBM solutions extract insight from an immense amount of real-time and historical data—in context and beyond what was previously possible. Data is the underlining principal used to form information, knowledge and intelligence. IBM helps protect this valuable asset and strengthen enterprise security by:

- Correlating large amounts of security-relevant data across silos, using integrated and intelligent security analytics to better predict and detect mission risks
- Helping reduce operational risk from threats facing structured (databases) and unstructured (documents) data by guarding against data loss and unauthorized access

Highlighted products

- QRadar family
- IBM InfoSphere BigInsights™
- InfoSphere Guardium

Sophisticated threats

Federal organizations face increasing complexity in defending themselves from skilled and determined adversaries. These attackers target critical IT assets and public infrastructure using sophisticated and off-the-shelf techniques to gain access—and no single solution offers enough protection. Organizations must go beyond traditional patch-monitor-remediate processes and employ both continuous monitoring and layers of defense capable of working in concert with one another to identify, analyze and respond to targeted threats. IBM helps protect against sophisticated threats by:

- Identifying and defending against known and unknown sophisticated attacks by combining network security, worldwide threat intelligence and advanced security analytics
- Integrating threat intelligence with security intelligence to identify the threats associated with malicious IP addresses
- Protecting against network-based threats masked in common network traffic while preventing attackers from exploiting vulnerabilities at the network, host and application layers

Highlighted products

IBM Advanced Threat Protection Platform includes:

- Security Network Intrusion Prevention System
- Security SiteProtector System
- QRadar Network Anomaly Detection
- IBM X-Force Threat Insight

Gartner recognizes IBM Security in the Leaders' Quadrant

- **Magic Quadrant for Security Information and Event Management, by Mark Nicolett, Kelly Kavanagh, May 7, 2013**
- **Magic Quadrant for Application Security Testing, by Neil MacDonald, Joseph Feiman, July 2, 2013**
- **Magic Quadrant for User Administration/Provisioning, by Earl Perkins, December 27, 2012**
- **Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms, by French Caldwell, John Wheeler, October 4, 2012**[3]

Continuous diagnostics and mitigation

Federal departments and agencies should apply continuous diagnostics and mitigation solutions providing visibility, control, automation and mitigation across their organizations. IBM Security Systems helps to create an integrated security infrastructure that can dynamically manage the network and drive down costs—while increasing the security/risk posture and compliance reporting capabilities. Information security groups can increase their security management capabilities by:

- Identifying hardware assets attached to their networks
- Cataloging and managing software installed on hardware assets
- Enforcing department configuration management policies on these assets
- Scanning the network for vulnerabilities on the hardware and software attached to their network
- Managing endpoint and patch management of machines for security compliance
- Increasing visibility and situational awareness within multi-tenant environments

Highlighted products

- Endpoint Manager
- QRadar SIEM
- QRadar Log Manager

- QRadar Risk Manager
- QRadar Network Anomaly Detection
- QRadar QFlow and VFlow Collectors
- QRadar Vulnerability Manager
- Security AppScan Standard
- Security AppScan Enterprise
- Security AppScan Source

Conclusion

In a more sophisticated, data-driven world, where information empowers mission success and persistent attacks on federal data and IT assets erode the effectiveness of traditional IT defenses, a fundamentally new approach to security is paramount. Such an approach must be based on three main tenets—intelligence, integration and expertise—delivering the infrastructure visibility, cross-organizational links and optimized controls necessary not only to help protect mission-critical data but also to support compliance activities. The IBM Security Framework delivers a unified approach to federal security by managing key functions ranging from threat detection to user access, compliance cost reduction and configuration management—and much more—all with a foundation in world-renowned research and development to help reduce the risk of today's advanced threats.

For more information

To learn more about IBM Security, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/federal/security or **ibm.com**/security

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
September 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle

[1] IBM Tivoli Key Lifecycle Manager will be renamed on Oct. 29, 2013, becoming IBM Security Key Lifecycle Manager.

[2] An IBM company.

[3] Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.