Breaking down silos of protection: An integrated approach to managing application security

Protect your enterprise from the growing volume and velocity of threats with integrated IBM solutions
Introduction
An enterprise today runs hundreds, if not thousands, of applications, many of which harbor vulnerabilities that make them gateways for attack. Web applications, which provide a two-way path for employees to access the outside world and outsiders to access enterprise resources, now account for 31 percent of all security vulnerabilities.1 More than half of those vulnerabilities involve cross-site scripting.

The necessary response to this widespread threat is to move beyond using point products to protect merely the perimeter of enterprise computing—and to put into place strong integrated solutions to protect valuable business assets. These solutions must do more than address vulnerability in a gap-by-gap and product-by-product basis. They must break down silos of protection with an integrated approach. Yet they must accommodate the fact that in most organizations it is impossible to protect 100 percent of applications.

Managing application security is critical for the enterprise
For organizations that store sensitive or confidential information such as intellectual property or customer data on internal networks, that run externally facing websites accessed by thousands or even millions of people, or that face regulations requiring they maintain strict control over their infrastructure, application security is a must.

A security breach can take the credit card numbers of your customers—or erase the contents of your database. It can shut down a power grid—or appropriate source code from a new product in development.

It can be the result of an unintended error by an authorized user, a sophisticated attack by the growing number of organizations seeking to steal business and personal information, or malicious destruction by hacktivists seeking to make a point for political or other causes.

This white paper will discuss the challenges organizations face in protecting their applications from threats and remediating vulnerabilities. It will examine solutions for enabling risk-based application security management, from identifying and prioritizing applications based on their business impact to assessing applications for vulnerabilities, putting vulnerabilities in context to determine the risks they pose, and mitigating risk by fixing vulnerabilities or implementing virtual patches.

The white paper will conclude with a look at how the organization can make application security risk management real by using the IBM portfolio of security solutions. It is an integrated and comprehensive portfolio designed to provide application discovery, automated vulnerability assessment, security intelligence for understanding the risk that vulnerabilities present, remediation guidance and capabilities for implementing layers of defense.

Introduction
An enterprise today runs hundreds, if not thousands, of applications, many of which harbor vulnerabilities that make them gateways for attack. Web applications, which provide a two-way path for employees to access the outside world and outsiders to access enterprise resources, now account for 31 percent of all security vulnerabilities.1 More than half of those vulnerabilities involve cross-site scripting.

The necessary response to this widespread threat is to move beyond using point products to protect merely the perimeter of enterprise computing—and to put into place strong integrated solutions to protect valuable business assets. These solutions must do more than address vulnerability in a gap-by-gap and product-by-product basis. They must break down silos of protection with an integrated approach. Yet they must accommodate the fact that in most organizations it is impossible to protect 100 percent of applications.

This white paper will discuss the challenges organizations face in protecting their applications from threats and remediating vulnerabilities. It will examine solutions for enabling risk-based application security management, from identifying and prioritizing applications based on their business impact to assessing applications for vulnerabilities, putting vulnerabilities in context to determine the risks they pose, and mitigating risk by fixing vulnerabilities or implementing virtual patches.

The white paper will conclude with a look at how the organization can make application security risk management real by using the IBM portfolio of security solutions. It is an integrated and comprehensive portfolio designed to provide application discovery, automated vulnerability assessment, security intelligence for understanding the risk that vulnerabilities present, remediation guidance and capabilities for implementing layers of defense.

Introduction
An enterprise today runs hundreds, if not thousands, of applications, many of which harbor vulnerabilities that make them gateways for attack. Web applications, which provide a two-way path for employees to access the outside world and outsiders to access enterprise resources, now account for 31 percent of all security vulnerabilities. More than half of those vulnerabilities involve cross-site scripting.

The necessary response to this widespread threat is to move beyond using point products to protect merely the perimeter of enterprise computing—and to put into place strong integrated solutions to protect valuable business assets. These solutions must do more than address vulnerability in a gap-by-gap and product-by-product basis. They must break down silos of protection with an integrated approach. Yet they must accommodate the fact that in most organizations it is impossible to protect 100 percent of applications.

This white paper will discuss the challenges organizations face in protecting their applications from threats and remediating vulnerabilities. It will examine solutions for enabling risk-based application security management, from identifying and prioritizing applications based on their business impact to assessing applications for vulnerabilities, putting vulnerabilities in context to determine the risks they pose, and mitigating risk by fixing vulnerabilities or implementing virtual patches.

The white paper will conclude with a look at how the organization can make application security risk management real by using the IBM portfolio of security solutions. It is an integrated and comprehensive portfolio designed to provide application discovery, automated vulnerability assessment, security intelligence for understanding the risk that vulnerabilities present, remediation guidance and capabilities for implementing layers of defense.

Introduction
An enterprise today runs hundreds, if not thousands, of applications, many of which harbor vulnerabilities that make them gateways for attack. Web applications, which provide a two-way path for employees to access the outside world and outsiders to access enterprise resources, now account for 31 percent of all security vulnerabilities. More than half of those vulnerabilities involve cross-site scripting.

The necessary response to this widespread threat is to move beyond using point products to protect merely the perimeter of enterprise computing—and to put into place strong integrated solutions to protect valuable business assets. These solutions must do more than address vulnerability in a gap-by-gap and product-by-product basis. They must break down silos of protection with an integrated approach. Yet they must accommodate the fact that in most organizations it is impossible to protect 100 percent of applications.

This white paper will discuss the challenges organizations face in protecting their applications from threats and remediating vulnerabilities. It will examine solutions for enabling risk-based application security management, from identifying and prioritizing applications based on their business impact to assessing applications for vulnerabilities, putting vulnerabilities in context to determine the risks they pose, and mitigating risk by fixing vulnerabilities or implementing virtual patches.

The white paper will conclude with a look at how the organization can make application security risk management real by using the IBM portfolio of security solutions. It is an integrated and comprehensive portfolio designed to provide application discovery, automated vulnerability assessment, security intelligence for understanding the risk that vulnerabilities present, remediation guidance and capabilities for implementing layers of defense.
But the devastating results can be the same: loss of profitability, disruption of business operations, interruption of the supply chain, diminishment of brand image, and threat of legal action or regulatory censure.

The importance of application security is clear. But the challenges are complex. And without the necessary infrastructure visibility and security solutions, the prospect of tackling them can be daunting.

Understanding application deployments is essential for protecting key assets

In many cases, IT does not have a sound understanding of either the number of applications the enterprise is running or the ways in which those applications fit into the computing environment. And for virtually any organization, this lack of visibility can be an impediment to security. Lack of visibility can be especially acute for organizations that have undergone a merger or an acquisition in which applications from multiple environments have been combined.

In meeting the visibility challenge, questions arise naturally that reflect the range of issues the organization must address. Executives will want to know about policy and impact—for example: What is the security risk? How do we ensure compliance? In order to mitigate security risk, the IT security team will need to know: What assets do we have? Which ones are most important? How secure are they? Which are the critical vulnerabilities? The development team will focus on tasks—for example: What vulnerabilities do I need to address—and how do I fix them?

Undertaking an application inventory and assessment can both answer questions and lay the groundwork for putting security measures into place. But in many cases, inventory and assessment also reveal a size and a complexity that can make it impossible to protect the entire infrastructure—certainly not right away, and perhaps never.

And if it is not possible to achieve 100 percent application security, the next question becomes: How can the organization mitigate the security risk—and what solutions can it put into place to achieve the required security?
Breaking down silos of protection: An integrated approach to managing application security

Web application vulnerabilities by attack technique

Source: “IBM X Force 2013 Mid-Year Trend and Risk Report”

In 2013, 31 percent of attacks targeted vulnerabilities in web applications. More than half of application vulnerabilities involved cross-site scripting.

A narrow view of application security is no longer enough

The point products and manual processes that many organizations use for gaining infrastructure insight and managing application vulnerabilities are not sufficient for today’s security needs. Requirements for human intervention make them labor intensive, time consuming, expensive—and, with the ever-present chance of human error, often unreliable. Point products can result in siloed data that typically remains unused across the larger IT environment because it does not provide the visibility and security intelligence the IT team needs to take effective actions.

In place of point solutions, deploying integrated and automated solutions for application security can provide more streamlined, cost-effective and reliable outcomes. Leveraging integrated solutions can provide deep, cross-enterprise security intelligence that IT can use to identify and understand vulnerabilities within their context and priority, and then support the management of application security.

Integration also makes possible a risk-based approach that tackles the impossibility of immediately protecting all applications. Security intelligence into areas such as data traffic, gathered by an integrated portfolio of security tools, for example, can be key to prioritizing applications and determining which ones should be addressed when and how.

Integrated solutions for insight and analysis can give IT the depth and coverage needed to prioritize business needs and application use according to the risks they face. And integrated solutions for mitigation and remediation help ensure critical applications receive the necessary protection against risk or fixes to their vulnerabilities in order to maintain continuity and compliance.

“Number one, we have to confirm that we have a strong network and that our servers have the right set of security. Number two, we have to make certain that the applications serving our commercial and consumer entities don’t have weaknesses or vulnerabilities. Finally, we believe that security intelligence will differentiate us and allow us to proactively address a threat before a problem occurs.”

—Tony Spinelli, Chief Security Officer, Equifax
Risk-based management takes the broad security view

An application that processes and stores personally identifiable customer information will be a high priority for any protection plan. A vulnerability in this kind of application can have serious consequences in diminished customer trust, lost business reputation, and fines or sanctions for noncompliance.

But a risk-based approach to application vulnerability management provides a broad view that considers much more than risk to an individual application. The IT security team needs to gather and analyze data on a range of details in order to build the security intelligence necessary for prioritizing applications to be addressed, testing applications for vulnerabilities and mitigating the risk that each application faces. Each consideration contributes toward a proactive response to comprehensive security risk management.

Solutions for application vulnerability management, for example, can provide insights that take into account not only the weaknesses that occur in individual applications, but also the context in which the application operates. An intrusion detection system might uncover the types of probes or attacks that have been aimed at the application during a defined period. But by integrating information such as the application’s location in the network or any dependencies the application might have, the security team can determine whether an attack might create a domino effect that extends beyond the individual application. The team can use this information to support actions such as temporarily taking the application offline, erecting a firewall, patching or otherwise mitigating risk.

Similarly, risk-based security management draws a distinction between new applications in development and existing applications in production. For new applications, it is important to ensure that security is built into the design early, as developers work through processes such as threat modeling, security reviews and quality assurance. For existing applications, it is important to assess and understand a broad variety of issues, beginning with the fact that deployed applications almost certainly come from different sources—with some purchased from third-party vendors and others developed in-house. Age also can be an issue, as older applications may have been designed with fewer, different and less severe security issues in mind than those existing today. Legacy applications may, in fact, never have been tested to determine if vulnerabilities exist.

“A lot of companies keep security close to the InfoSec [information security] organization and they can’t scale. For us, the question was: How can we put this skill into the DNA of the application development teams so that it wasn’t just a challenge for the security team, it was an opportunity to improve software quality overall?”

—Sujata Ramamoorthy, Director, Information Security, Cisco

Full enterprise protection requires integrated solutions

With multiple vulnerabilities the norm in large organizations, comprehensive, proactive capabilities are essential for risk-based application security. If certain areas are to be left exposed while repairs and protection are provided for the highest priority applications, the ability to protect against the full range of threats and vulnerabilities—and to anticipate when and how a vulnerability might be exploited—must be deployed across the full enterprise.

Only integrated solutions can do this job. Only solutions that work together to put applications and their vulnerabilities into the context of enterprise infrastructure and provide a view of
Breaking down silos of protection: An integrated approach to managing application security

application security from a level-of-risk perspective can live up to the overwhelming task of securing the large numbers of legacy and in-development applications in today’s enterprise environments.

When it comes to security, an application cannot be viewed in isolation. In evaluating risk to an application, it is also necessary to consider vulnerabilities in the network, host and database. IT security teams have to understand the business purpose of applications and the potential impacts of a breach.

Integrated solutions can pull data from a variety of extensive data sources—including security devices, servers, network activity, configurations and user activities—to create the deep security intelligence that is necessary. Solutions can work together to correlate logs, flows and locations; detect anomalies in user, database, application or network activity; and identify the credibility, severity and relevance of offenses—delivering accurate and actionable insight on how to deal with suspected incidents.

IBM solutions provide application security intelligence

From discovering vulnerabilities in applications and threats in information flows to analyzing findings and providing repositories and dashboards for utilizing security intelligence, solutions from IBM® Security deliver the integrated capabilities that risk-based application security requires.

The ability of IBM Security AppScan® to integrate with IBM Security QRadar® solutions, for example, combines capabilities for maintaining and updating information about each host system’s services, applications, vulnerabilities, traffic/use level and Internet exposure, providing users with information on detected application vulnerabilities to calculate risk levels for each asset.

**Integrated solutions for application security risk management**

- Application discovery and context
- Risk-based vulnerability analysis
- Security policies and alerts

**IBM QRadar Security Intelligence Platform**

- Application vulnerability assessments
- Database vulnerability assessments
- Database activity monitoring

Integrated IBM solutions enable IT security teams to identify application assets, assess their level of security, prioritize any vulnerabilities discovered and mitigate risks that the vulnerabilities present.
The holistic IBM approach correlates application vulnerability information with intrusion prevention data so that security teams can assess threats to vulnerable applications within the context of threats to the larger infrastructure.

- **IBM Security AppScan** supports organization-wide application security risk management with automated testing that includes scanning applications, identifying vulnerabilities and generating reports with recommendations for fixes. Utilizing a wide range of testing techniques—including dynamic, static and interactive analysis—Security AppScan enables deep analysis of applications in development and production. Security AppScan integrates with other IBM Security solutions to provide additional context and security intelligence for analyzing and prioritizing vulnerabilities and mitigating the risks they present. Security AppScan exports application vulnerability information into IBM Security SiteProtector™ System and QRadar solutions, where information can be correlated with real-time data collected by IBM Security Network Intrusion Prevention System—as well as with other information such as the application's location in the network, firewall rules, user traffic, or host and database vulnerabilities.

- **IBM Security Network Intrusion Prevention System** combines detection and prevention capabilities to make vulnerabilities visible and stop threats before they impact the business. Security SiteProtector System provides centralized management of IBM intrusion prevention solutions, including the ability to define security policy and monitor detected events. Security Network Intrusion Prevention System is also capable of receiving vulnerability information from Security AppScan, which it can correlate with web application attack events to show if vulnerabilities are being actively exploited. In addition to providing protection for web application attacks such as SQL injection and cross-site scripting, Security Network Intrusion Prevention System can protect against other threats such as malware, denial-of-service attacks, data loss and targeted attacks related to advanced persistent threats.

- **IBM InfoSphere® Guardium®** monitors database activity with support for fine-grained auditing, automated compliance reporting, data-level access control, database vulnerability management and auto-discovery of sensitive data. Designed to prevent unauthorized or suspicious activities by privileged insiders and hackers alike, InfoSphere Guardium enables the organization to assess database vulnerabilities and configuration flaws, ensure that configurations are locked down after changes, and capture and examine transactions with secure, tamper-proof audit trails.

- **IBM QRadar Security Intelligence Platform** provides a unified architecture for integrating security information and event management data with log, flow, vulnerability, user and asset data—for near real-time correlation and behavioral anomaly detection to help identify high-risk threats. Intelligence, integration and automation deliver 360-degree network insight into application and user activity, correlating known application vulnerabilities with other events and alerts, and enhancing proactive risk-management assessments by prioritizing critical application vulnerabilities.

- **IBM Security QRadar Vulnerability Manager** delivers a unified view of vulnerability information integrated with security intelligence data and context that it gathers using an embedded, scalable scanner. Integrated with Security AppScan, it can provide a complete network context to application vulnerabilities including correlation with attacks, exploitability from potential threats or untrusted sources, and user activities—for an improved incident response based on complete visibility in a single system.
Conclusion

Application security is a cornerstone of any enterprise security plan. But to keep up with application vulnerabilities and the growing complexity and velocity of threats, enterprises need to break through siloed solutions to integrate security architectures. IBM delivers intelligent, integrated, end-to-end application security solutions designed to help manage risk, demonstrate compliance and reduce costs.

For more information

To learn more about IBM solutions for application vulnerability management, please contact your IBM representative or IBM Business Partner, or visit: 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

© Copyright IBM Corporation 2013

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2013

IBM, the IBM logo, ibm.com, AppScan, InfoSphere, Guardium, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

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.

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

WGW03035-USEN-01