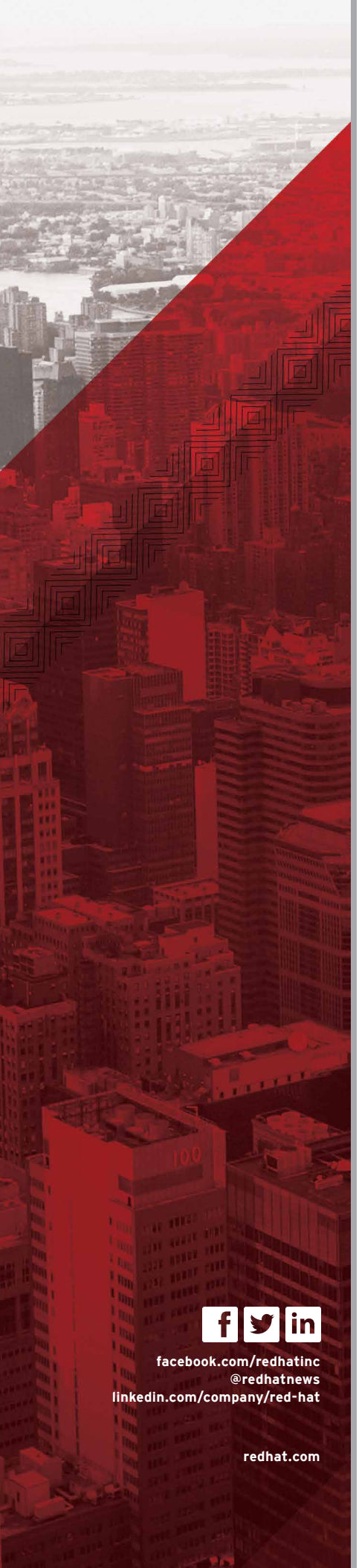

WHITEPAPER

HOW SECURITY AND INNOVATION MEET AT RED HAT

Gordon Haff

EXECUTIVE SUMMARY

Red Hat develops software in collaboration with customers from a range of industries, including government and financial services. This not only leads to innovation but provides valuable guidance for security-related decisions about product features, services, or processes. This approach makes Red Hat® infrastructure software, such as Red Hat Enterprise Linux®, and application platforms, such as Red Hat JBoss Enterprise Application Platform, a foundational part of business in some of the most regulated and sensitive industries.

Today's threat environment means that building in security and operationalizing it across all of your IT, including hybrid cloud environments, is more important than ever.

In this whitepaper, we'll discuss today's security landscape and how you can partner with Red Hat to meet security, risk management, and compliance goals. This includes addressing common, basic requirements for mitigating vulnerabilities, implementing configuration management, and establishing access controls. While these requirements are hardly new, in today's digital world they're amped up for higher threat velocity and volume, IT architectures that are open to the world, and infrastructure that is both heterogeneous and hybrid.

Thus, we'll cover Red Hat's approach to building in security and working in upstream communities to proactively fix vulnerabilities before they become problems. We'll also look at Red Hat Insights, a subscription management service that can proactively identify and resolve technical issues on your systems. We'll discuss the role of automation in operationalizing security and documenting processes in code with products like Ansible Tower and Red Hat Satellite. We'll touch on the role that DevOps plays in enabling a more nimble IT process for pushing out code updates. And we'll see how Red Hat CloudForms provides a centralized point of policy-based control over hybrid IT environments.

However, today's security story isn't about specific security features or solutions that provide a magic bullet. It's about taking a broad view of security (which really means risk management, compliance, and governance) and operationalizing it in a way that makes sense for the business. And that's going to be the real focus.

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

redhat.com

"Open source software projects that leverage development testing continue to increase the quality of their software, such that they have raised the bar for the entire industry."

ZACK SAMOCHA
SENIOR DIRECTOR OF PRODUCTS
COVERITY

THE CHANGING FACE OF SECURITY

The wall and moat of a medieval castle presented a formidable barrier to the would-be attacker. But it was a barrier that was effective only so long as would-be attackers failed to breach a weak spot or employ a novel tactic. Traditional IT security is likewise primarily based on building and protecting a strong perimeter for on-premise hardware, applications, and data. It doesn't ignore insider threats arising through malice or error. But it does rely heavily on firewalls, intrusion detection systems, and access controls to keep the "bad guys" outside the gates.

Today, information security must adapt to a changing landscape. Whether it's providing customers and partners with access to certain systems and data, allowing employees to use their own smartphones and laptops, using applications from Software-as-a-Service (SaaS) vendors, or taking advantage of pay-as-you-go utility pricing models from public cloud providers, there is no longer a single perimeter. Making the most effective use of an organization's information assets may require sharing that information with authorized third parties. Both regulatory compliance and the sheer intensity and sophistication of cyber-attacks further highlight the need for an IT security strategy that runs deeper and is more multi-faceted than the traditional norm in most organizations.

We see this trend reflected both in analyst research and customer discussions. For example, the fact that security regularly tops the list of public cloud adoption concerns in surveys isn't news to anyone. However, it's not familiar aspects of system security like access and control or misconfigured firewalls that are causing the concern. Rather, it's data jurisdiction, auditability, regulatory compliance, and verifiable end-to-end encryption that top the list. And those are just the areas over which the cloud provider has some direct responsibility.

The organization running the workload also has its own part to play in establishing the provenance of software, understanding the governing regulations and certifications, providing the appropriate policy-based controls and access, managing their supplier relationships, and generally establishing formal and repeatable processes for security and incident response.

THINKING ABOUT SECURITY

This paper touches on a number of technologies and capabilities related to information security. However, implementing effective defense, detection, and deterrence isn't about using a particular product or component. It's about establishing a solid foundation that lets you automate business processes, institutionalize good practices, and effectively remediate problems when (not if) they occur. As security expert Bruce Schneier has noted: "Security does not have to be perfect, but the risks have to be manageable."[1]

A common conceptual model of security practices, the CIA Triad, focuses on three aspects of (primarily data) protection:

1. Confidentiality – restricting data access to those who are authorized to use it
2. Integrity – ensuring that data has not been altered or deleted by an unauthorized party
3. Availability – ensuring that data will be available when it's needed

1 https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

"Naive beliefs that cloud providers are totally responsible for their customers' security discourages organizations from ensuring their employees use cloud services appropriately."

GARTNER
"CLOUDS ARE SECURE: ARE YOU USING THEM SECURELY?" SEPTEMBER 2015
G00281279

Security professionals and organizations such as the US National Institute of Standards and Technology[2] have developed more complex models that include additional aspects of security such as risk assessment, timeliness, physical possession, legality, and utility. A complete treatment of security best practices is beyond the scope of this paper. Rather, we'll focus on important or novel technologies and practices relating to hybrid architectures, cloud-native infrastructures, application development using DevOps approaches, and commercial open source security vulnerability response.

It's a measure of the seriousness and sophistication of attacks that strategic chief information security officer (CISO) positions are becoming more common and that incident response plans are starting to look more like those associated with actual firefighting. There are several reasons for this.

The first is that security needs to be approached in the context of the business as opposed to just a technology problem. This means, for example, defining the business' risk appetite in terms of loss tolerance. A credit card issuer knows that it's going to have losses due to fraud. Preventing fraud entirely would make using credit cards so onerous that no one would use them. Instead, the card issuers put sufficient controls in place to keep losses at an acceptable level, while minimizing the overall impact on the user experience.

Another reason security is taken more seriously is that, as with a fire or a car accident, minutes count. Roles, responsibilities, and processes must be established ahead of time. Technical expertise matters, but so does having clear communication plans to share information with those potentially affected by the incident and with broader constituencies such as the press.

GETTING STARTED WITH SECURITY

Security starts with a dream of stability and safety but is often driven by fear, concern, and a need to keep assets from being compromised throughout their life cycle. Whatever complexities today's IT architectures and external threat environment may add, it's still good to start with time-tested technologies and practices that you can extend into today's world.

Open source offers a case in point. The open development model allows entire industries to agree on standards and encourages their brightest developers to continually test and improve technology. Developing software in collaboration with users from a range of industries, including government and financial services, provides valuable feedback that guides security-related discussions and product feature implementations. No one can solve IT security issues alone. Collaborating with communities to solve problems is the future of technology.

Linux has been the beneficiary of a wide range of security-related technologies built using the open source model. These include:

- A dynamically managed firewall.
- SELinux for mandatory access controls.
- A wide range of userspace and kernel hardening features.
- Identity management and access control.
- SHA-512 based password hashes.
- File system encryption.

2 NIST Special Publication 800-27 Revision A

Furthermore, the open source development process means that when vulnerabilities are found, the entire community of developers and vendors can work together to update code, security advisories, and documentation in a coordinated manner.

Red Hat Enterprise Linux is the IT foundation in some of the most regulated and sensitive industries; it's incorporated open source security advances in predictable, consumable ways. These same processes and practices apply across hybrid cloud infrastructures as the role of the operating system evolves and expands to include new capabilities like Linux containers. Furthermore, components are reused in the form of microservices and other loosely coupled architectures that interact using application programming interfaces (APIs). So maintaining trust in the provenance of those components and their dependencies (when making up applications) becomes more important, not less.

OPERATIONALIZING SECURITY

Historically, security was often approached as a centralized function. An organization might have established a single source of truth for user, machine, and service identities across an entire environment and described the information they are authorized to access and the actions they are allowed to perform.

Today, the situation is often more complicated. It's still important to have access control policies that govern user identities, delegating authority as appropriate and establishing trusted relationships with other identity stores as needed. However, application components running on top of Linux or other operating environments may be subject to multiple authorization systems and access control lists.

It's important to have insight into and control over such complex hybrid and heterogeneous environments. For example, real-time monitoring and enforcement of policies can not only address performance and reliability issues before the problems become serious, but they can also detect and mitigate potential compliance issues. Automating in this way reduces the amount of sysadmin work that is required. However, it's also a way to document processes and reduce error-prone manual procedures. Human error is consistently cited as a major cause of security breaches and outages.

Operational monitoring and remediation needs to continue throughout the life cycle of a system. It starts with provisioning. As with other aspects of ongoing system management, it's important to maintain complete reporting, auditing, and change history.

The need for security policies and plans doesn't end when an application is retired. The ownership and policies pertaining to the data associated with an application need to be well understood so that the proper steps can be taken to comply with retention requirements and the sanitization of personally identifiable information (PII).

With traditional long-lived application instances, maintaining a secure infrastructure also meant analyzing and automatically correcting configuration drift to enforce the desired host end-state. This is often still an important requirement. However, with the increased role that large numbers of short-lived "immutable" instances play in cloud-native environments, it's equally important to build in security in the first place. For example, you may establish and enforce rule-based policies around enabled services in the layers of a containerized software stack.

Taking a risk management approach to security goes beyond putting an effective set of technologies in place. It also requires considering the software supply chain and having a process in place to address issues quickly.

For example, it's important to validate that software components come from a trusted source. Containers, an agile and streamlined model for application delivery, provide a case in point. Containers are a simple and efficient way to assemble, distribute, and deploy software. This very simplicity can turn into a headache if IT doesn't ensure that all software comes from trusted sources and meets the highest standards of security and supportability.

As described earlier, incident response goes well beyond patching code. However, a nimble software deployment platform and process with integrated testing is still an important part of quickly fixing problems (as well as reducing the amount of buggy code that gets pushed into production). A continuous integration/continuous delivery (CI/CD) pipeline that is part of an iterative, automated DevOps software delivery process means that modular code elements can be systematically tested and released in a timely fashion. Furthermore, explicitly folding security processes into the software deployment workflow makes security an ongoing part of software development—rather than just a gatekeeper blocking the path to production.

GOVERNANCE AND COMPLIANCE ACROSS HYBRID CLOUDS

While reflexive fears about a lack of security in public clouds may be naive, public and hybrid clouds do introduce risk and compliance considerations and challenges that are different from concerns you have with traditional on-premise datacenters. It's important to understand which areas you still maintain responsibility for when using public clouds. For example, in the case of Infrastructure-as-a-Service (IaaS), you need to exercise the same care in sourcing and maintaining your operating system and applications as you do when running it on-premise.

A variety of frameworks can help IT executives and architects evaluate and mitigate the risk associated with using public cloud providers. A good example is the Cloud Controls Matrix (CCM) from the Cloud Security Alliance (CSA).[3]

The CSA CCM provides a controls framework across 16 domains, including:

- Business continuity management and operational resilience.
- Encryption and key management.
- Identity and access management.
- Mobile security.
- Threat and vulnerability management.

CCM v3.0.1 defines 133 controls and maps the relationship between each control and other industry-accepted security standards, regulations, and controls frameworks such as ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum, and NERC CIP.

3 https://cloudsecurityalliance.org/group/cloud-controls-matrix/

Using the CCM as a reference framework, Red Hat products and partnerships are most relevant in these domains:

- Change control and configuration management.
- Data security and information life-cycle management.
- Encryption and key management.
- Identity and access management.
- Infrastructure and virtualization security.
- Interoperability and portability.

Red Hat also works with partners in all these areas and provides support for other domains, such as threat and incident management, by providing effective and timely response for exploits as they are discovered.

Service design for delivery through hybrid architectures can also be informed by more traditional IT methodologies. For example, the IT Infrastructure Library (ITIL) Service Strategy is one of five ITIL life-cycle modules. It can guide you through designing, developing, and implementing a service provider strategy that aligns with an organizational strategy. Thus, ITIL practices can be used to help design appropriate, complete services for hybrid IT.

From a technology perspective, a key component of governance and compliance is a policy-based hybrid cloud management platform (CMP) like Red Hat CloudForms. An effective CMP provides access to service catalogs with role-delegated automated provisioning, quota enforcement, and chargeback across virtualization and cloud platforms. It supports complex policy-based task and resource orchestration and automation to help ensure service availability and performance. All this helps IT maintain control of applications and infrastructure capacity.

DOMAIN	EXAMPLE PRODUCT AND FEATURES
Application and interface security	Red Hat provides APIs that adhere to industry standards. For example, Red Hat JBoss Middleware products support standard Java™ SE and Java EE APIs, SAML 2.0 for web single sign-on, and WS-Security for securing web services.
Audit assurance and compliance	The audit features in Red Hat CloudForms, as well as logging features in a variety of products, support the auditing process. Red Hat also partners with companies that have logging and analysis products.
Change control and configuration management	Both Red Hat Satellite and Ansible Tower provide configuration management and provisioning tools.
Data security and information life-cycle management	Red Hat Gluster Storage features such as active archive help support information life-cycle management. Red Hat JBoss Data Grid uses Java SE authentication and encryption features to protect sensitive data stored in its distributed in-memory datastore.

DOMAIN	EXAMPLE PRODUCT AND FEATURES
Encryption and key management	Red Hat Enterprise Linux encryption features include SHA-512 based password hashes, file system encryption, and NSA Suite B cryptography enhancements and certifications. OpenJDK, which is included, provides cryptographic algorithms and interfaces for Red Hat JBoss Middleware, as standardized by the Java Community Process.
Governance and risk management	Policy-based automation in Red Hat CloudForms is an example of a feature that organizations can use to enforce governance plans.
Identity and access management	Centralized identity management is part of Red Hat Enterprise Linux, as are the mandatory access controls provided by SELinux. Application-level authentication, authorization, and audit features are available in Red Hat JBoss Middleware.
Infrastructure and virtualization	Red Hat Enterprise Linux, Red Hat Enterprise Virtualization, Red Hat OpenStack® Platform, and Red Hat Atomic Host all provide robust and secure infrastructure.
Interoperability and portability	Red Hat's products adhere to open standards and provide open APIs. Containers provide a new approach for workload portability across environments.
Mobile security	Red Hat Mobile Application Platform provides centralized control of security and policy management.
Security incident management, e-disc and cloud forensics	When security vulnerabilities happen, Red Hat provides customers with the means to address those vulnerabilities and safeguard their systems.
Supply chain management, transparency, and accountability	Red Hat helps to secure the supply chain by digitally signing all released packages (including containers) and distributing them through secure channels.
Threat and vulnerability management	Red Hat Insights is a hosted service that helps proactively identify and resolve technical issues in Red Hat Enterprise Linux and Red Hat Cloud Infrastructure environments. Red Hat also creates and supports Open Vulnerability and Assessment Language (OVAL) patch definitions, providing machine-readable versions of our security advisories. OpenSCAP lets you check security configuration settings of a system and examine the system for signs of a compromise by using rules based on standards and specifications.

Select Red Hat capabilities are mapped to CSA security domains (excluding domains such as data-center security and human resources security that are primarily focused on an organization's internal physical security and business practices).

"Red Hat CloudForms is a Swiss Army knife. You can do many different things in the IT environment with it—including insights and intelligence on our infrastructure. We analyzed the numbers to see what resources we deployed and how much time it took, and we realized that with the Red Hat solution, we saved almost 10 years of time spent waiting for resources to be delivered and almost $5 million in soft savings since 2014. Additionally, with Red Hat Insights, we can resolve critical issues before they occur."

JASON CORNELL
MANAGER OF CLOUD AND INFRASTRUCTURE AUTOMATION
COX AUTOMOTIVE

HOW RED HAT CAN HELP YOU CREATE A SECURE CLOUD

We've touched on some areas of functionality that are important to securing hybrid cloud infrastructures that use Red Hat products. This includes:

- Encryption, mandatory access controls (SELinux), and identity management in Red Hat Enterprise Linux 7.
- Granular, policy-based logging and visible alerting provided by Red Hat CloudForms, which enables rapid automated response across heterogenous workloads and multiple cloud types.
- Automated provisioning and management provided by Ansible Tower and Red Hat Satellite, which also monitors for configuration drift and remediates as needed.
- The ability to use Red Hat JBoss BRMS and Red Hat JBoss BPM Suite to create workflows that watch for and respond to transactions that violate domain-specific business rules.

For example, the Payment Card Industry (PCI) Data Security Standard (DSS) continues to mature and require more stringent enforcement of its requirements. As enterprises deploy new applications and modern technology solutions, they need to consider the compliance ramifications of shared environments. Red Hat CloudForms helps clients gain control of the virtualization environment when building or managing private or hybrid cloud environments. Red Hat CloudForms provides robust mechanisms for cloud infrastructure with advanced virtualization management controls, private or hybrid cloud management capabilities, and operational visibility technologies.[4] This includes aggregate logging capabilities that let you segregate, log, and allocate resources by user, group, location, or other attributes for control granularity aligned with Cgroups and SELinux policies.

However, Red Hat's focus on security is both broader and deeper than even significant investments in product technologies. Helping customers operate secure environments and processes also means having ongoing expertise and direct involvement in upstream projects, implementing reproducible build and testing systems, delivering packages securely, and responding quickly and effectively to vulnerabilities.

When security vulnerabilities happen, our Customer Portal, technical support, and product security teams offer Red Hat customers ways to address those vulnerabilities and safeguard their systems. During the Shellshock and Heartbleed security incidents, Red Hat customers had the knowledge, patches, and applications needed to verify their exposure and successfully remediate potential issues within hours of the bugs being made public.

For example, Red Hat Insights can help you proactively identify and resolve technical issues in Red Hat Enterprise Linux and Red Hat Cloud Infrastructure environments. This service focuses on security and rigorous deployment controls, tapping into a global network of engineers and Red Hat's extensive Knowledgebase of technical solutions and resolved issues. It analyzes system information and checks it against our growing database of deterministic rules. These rules are the result of our Customer Experience and Engagement team's work to identify and document best practices for optimizing workloads and avoiding issues. Red Hat Insights proactively shares this information and suggests steps for remediation in a simple and easy-to-consume format. Red Hat Insights can help you streamline operations and avoid potential business disruptions.

4 For more details about how Red Hat Enterprise Linux, Red Hat Satellite, and Red Hat CloudForms offer a foundation that supports continuous management of PCI-DSS relevant controls and enforcement of policies, see http://www.redhat.com/en/resources/pci-dss-compliance-red-hat

"We hope to guarantee greater security and reliability in our mission-critical applications, which include data management for the entire public network of hospitals and clinics, as well as information from private insurance plans."

JOSE MARQUES
GENERAL COORDINATOR OF ANALYSIS AND MAINTENANCE FOR BRAZIL'S MINISTRY OF HEALTH

Red Hat also helps secure the supply chain by digitally signing all released packages and distributing them through secure channels. Vulnerability and errata information is also provided in machine-readable form so that it can be consumed and acted on at scale—such as through the use of a Security Content Automation Protocol (SCAP) scanner. The Red Hat Container Registry lets you know that components come from a trusted source, platform packages have not been tampered with, the container image is free of known vulnerabilities in the platform components or layers, and the complete stack is commercially supported.

Enterprise open source software also requires code review and testing methodologies. For example, the Red Hat Enterprise Linux 7 release process included not only reviewing new packages for security bugs and packaging problems, but also ensuring that prior fixes had made it into the upstream code base or were otherwise still present. A reproducible build system that logs all actions lets Red Hat know where, when, why, and how a given build happened so that it can be recreated at a future date if required—even years later.

Red Hat can consistently deliver software in this way partly because of experience and a process that works consistently. But it's also because Red Hat engineers maintain expertise in and make extensive contributions to the upstream communities associated with our subscription products. This helps us to affect changes that are important to our customers, including those related to security.

Red Hat maintains a dedicated Product Security team that analyzes threats and vulnerabilities against all our products every day and provides relevant advice and updates through the Customer Portal. This team cuts through the hype and understands the issues that really matter, as opposed to those that are mostly theoretical problems. Customers rely on this expertise to ensure that they respond quickly to address the issues that matter. Red Hat works with other Linux and open source software communities and companies to reduce the risk of security issues through information sharing and peer review.

CONCLUSION

Modern security means shifting from a strategy that is built around minimizing change to one that is optimized for change. An insight-driven workflow must provide visibility into multiple environments, aggregate information, and take remedial action, even for assets that may have a lifetime on the order of minutes. Security needs to be an integral component throughout the software delivery pipeline, rather than a disconnected checkbox.

Red Hat can be your partner in this transformation. Our products provide the technologies and carry the certifications (such as Common Criteria and FIPS)[5] that you may need. We are deeply embedded in the open source software supply chain and have the expertise and the processes to deliver innovative open source products in a way that is reliable, consistent, and secure.

5 http://www.redhat.com/en/technologies/industries/government/standards

ABOUT RED HAT

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

NORTH AMERICA
1 888 REDHAT1

EUROPE, MIDDLE EAST, AND AFRICA
00800 7334 2835
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
apac@redhat.com

LATIN AMERICA
+54 11 4329 7300
info-latam@redhat.com

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

redhat.com
INC0374232_0416