WHITEPAPER

FIVE PILLARS FOR ORGANIZATIONAL RESILIENCY

Build a secure foundation that can support your agency's expanding security.

EXECUTIVE SUMMARY

A secure structure is anchored by strong footings. This especially holds true for the security infrastructure that protects government data and networks. By every measure, the attacks on government systems are growing in sophistication and numbers. At the same time, IT environments are growing more sophisticated and complex—and thus more difficult to defend. And so agencies must build their security on a resilient foundation that can meet their current security needs while also expanding their digital capabilities.

In our work helping federal organizations secure their digital environments, Red Hat has identified five security "pillars" that are essential for building a resilient organization. Each pillar addresses key areas of concern for agencies operating in traditional IT environments, as well as for those who are moving aggressively to adopt cloud, mobile, and other advanced technologies. These pillars also help federal organizations comply with strict government security requirements. The five pillars for security and resiliency are:

- **Secure multitenancy** provides secure, role-based access for multiple levels of security clearance, while also protecting data in multitenant cloud environments.
- **Identity management** ensures only authorized users can access data and applications.
- **Continuous monitoring** automates processes for compliance with security rules and requirements.
- **Collection and analysis** implements robust security analytics with efficient, scalable data storage and analysis.
- **Secure software supply chain** automates processes for ensuring the integrity of software.

Modern technologies offer agencies numerous opportunities to cut operating costs, improve service delivery, strengthen national security capabilities, and enhance mission performance, but only if agencies have an infrastructure that is secure and can withstand attacks against government networks and data. By establishing these mutually reinforcing security pillars, agencies can create a resilient foundation that supports their constantly evolving security requirements for today and tomorrow.

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

redhat.com

BUILDING A SECURE ORGANIZATION

Modern technologies have transformed how government agencies and workers carry out their mission responsibilities, enabling civilian and defense agencies to operate more efficiently, innovate faster, and use data to enhance mission capabilities. But the increased reliance on technology has also expanded the attack potential for malicious actors, whose relentless attacks on government systems are proliferating (search "Presidential Policy Directive—United States Cyber Incident Coordination"). Federal cybersecurity professionals want to be enablers of new technologies and capabilities, but they worry about the potential security risks. Among their concerns are:

- How do I protect data in a multilevel security environment?
- How can I efficiently carry out continuous diagnostics and mitigation (CDM)—that are both compliant and effective—in today's complex environment?
- How can I respond and recover quickly when my data and applications reside in so many different locations?
- How can I take advantage of data analytics to strengthen security?
- How do I ensure that new software is secure and free from malware, without slowing deployment, especially as my organization adopts DevOps and other innovative methods to rapidly develop and deploy new software and applications?

Across all of these concerns is the desire to comply with federal security laws and mandates, such as the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the White House Cybersecurity Strategy and Implementation Plan.

Red Hat, a secure and trusted provider of open source solutions to government, is helping federal agencies address these and other security challenges. The goal is to create a secure, resilient IT environment. This means defending against, and preventing, malicious intrusions. It means identifying unauthorized intruders and then responding quickly to mitigate the damage and expel the attackers. And it means having the resiliency to continue operations while under attack and to quickly return to normal operations.

How can agencies create resilient organizations? Equally important, how can they build a secure infrastructure that supports current needs for data analytics and other innovative security solutions, while also providing a foundation to extend security protections into new virtual, cloud, mobile, and emerging digital environments?

"An agency's IT environment is like a house that you continually renovate and expand," said Major Gen. (Ret.) Conrad Ponder, former chief integration officer in the Army's CIO Office, and now president at CP Consulting. "There is no such thing as a new house in IT. It's always a renovation. And so, in order to upgrade and add onto your environment, you need a solid security infrastructure that can also provide the most rigorous protections to your legacy systems—bring them up to code, so to speak—as you modernize."

In working closely with our government partners to secure their data and networks, Red Hat has found that a resilient organization requires a foundation built on five fundamental security pillars. These pillars are essential for all agencies, not just those moving to cloud and mobile environments. They provide the sturdy footings required for a secure and resilient infrastructure that can adapt and expand with ever-changing IT environments to meet evolving threats and vulnerabilities.

The five security pillars are:

1. **Secure multitenancy.** When organizations are providing secure access to users and data that have different levels of classification, they must ensure that only users with appropriate security clearances access classified data. A cloud environment complicates this challenge when multiple organizations—or tenants—share a cloud infrastructure in which they also share applications and hardware, including data storage. The ability to run multiple workloads, users, and classifications of data on a shared infrastructure creates numerous opportunities for cost savings and efficiencies. The potential benefits include centralized IT management, network consolidation, streamlined delivery of Software-as-a-Service (SaaS), and the ability to more easily customize and upgrade solutions for individual customers. But multitenancy can also create security risks, such as malicious attackers exploiting a vulnerability in one tenant to access the data or networks of other tenants in the shared network. Government organizations need assurance that a multitenancy environment won't increase security risks.

   Red Hat® solutions deliver secure multitenancy by isolating users, applications, and data. Red Hat Security-Enhanced Linux® (SELinux) is the default standard for Red Hat Enterprise Linux, as well as Red Hat's entire portfolio that builds on the Red Hat Enterprise Linux foundation. Originally developed by the National Security Agency (NSA), SELinux allows administrators to enforce mandatory access controls (MAC) by applying labels to every user, application, process, and file, automatically enforcing policies. Red Hat Enterprise Linux with Smart Virtualization and Red Hat OpenStack® Platform let agencies apply SELinux policies to virtual and cloud environments, while Red Hat Enterprise Atomic Host and Red Hat OpenShift enable application of SELinux policies to Linux containers.

   Network labeling ensures that only approved networks can communicate with each other, while data labeling ensures that only approved applications and users can access different types of data.

   There are two main types of data that must be protected—data at rest and data in motion. Red Hat Enterprise Linux offers protection for both. Data at rest can be encrypted via the Linux unified key setup-on-disk-format (or LUKS), whereas data in transit may be encrypted via virtual private networks (VPNs), which provide encrypted tunnels between computers or networks of computers across all ports. With a VPN in place, all network traffic from the client is forwarded to the server through the encrypted tunnel. Data in motion may also be encrypted via secure shell (SSH). SSH is a powerful network protocol used to communicate with another system over a secure channel. The transmissions over SSH are encrypted and protected from interception. Cryptographic login can also be utilized to provide a better authentication method over traditional usernames and passwords.

These capabilities not only protect data in multitenancy environments, but also in noncloud environments in which users and data have multiple levels of security.

2. **Identity management.** Securing data and applications requires strict authentication and authorization controls, but managing multiplying numbers of users and user groups, as well as the many policies and roles governing their access to data and services, can grow increasing costly and complex. Simply managing passwords can be cumbersome if users have to create and enter new passwords for each application they access, and then administrators have to manually replicate constantly changing passwords across multiple users and applications. Multifactor authentication complicates management even more. Consequently, agencies need centralized identity management and access control to efficiently manage the entire life cycle of identity management from provisioning to de-provisioning of users, including the automation of processes.

   Red Hat provides strict identity management through Red Hat Enterprise Linux identity management (IdM), Red Hat Certificate System (PKI), Red Hat Directory Server, and OpenStack Keystone.

   Red Hat Enterprise Linux identity management lets you centrally manage identities and define access-control policies for users, machines, and services within large Linux and UNIX enterprise environments. IdM also supports integration with Microsoft Active Directory, enabling you to use Active Directory as your identity hub across your Windows and Linux environments.
   Red Hat Certificate System provides a scalable, secure framework to establish and maintain trusted identities and keep communications private. It offers certificate life-cycle management for single and dual-key X.509v3 certificates needed to handle strong authentication, single sign-on, and secure communications. Red Hat Directory Server is a Lightweight Directory Access Protocol (LDAP)-compliant server that centralizes user identity and application information. And OpenStack Keystone, which provides a central directory of users mapped to the OpenStack services they can access, can also act as a common authentication system supporting multiple forms of authentication across a cloud operating system.

   Overall, Red Hat identity management solutions reduce the administrative overhead to manage users, user groups, systems, and services, while streamlining provisioning and improving security.

3. **Continuous monitoring.** Agencies continuously monitor their networks and systems for indications of intrusion, vulnerabilities, misconfigurations, and other anomalous or potentially malicious activity. Continuous monitoring also supports analytics that can help agencies anticipate and prioritize risks based on their potential impact, so cybersecurity staff can focus resources on the most significant problems. It also provides a foundation for fused intelligence for physical and cybersecurity. Continuous monitoring is essential in today's complex IT environment, particularly as cyber attacks on government networks continue to grow in sophistication and frequency.

   An effective continuous monitoring system requires a supporting infrastructure to securely and efficiently manage the rapid collection, analysis, and transmission of data. Red Hat solutions efficiently collect and integrate telemetry from many diverse endpoints on agency networks, rapidly transmit that data to the analytics platforms, and keep the data secure throughout. They also scale easily to support most rigorous CDM requirements to ensure compliance with current and planned federal CDM mandates—all within agency budget constraints.

Red Hat solutions for powering robust CDM include:

- Red Hat Satellite provides configuration and policy management.
- Red Hat CloudForms delivers ITIL-styled service catalogs for advanced life-cycle management of hybrid clouds, including monitoring and tracking, capacity management and planning, and resource usage and optimization.
- Red Hat Open Security Content Automation Protocol (SCAP)/Satellite provides agencies with centralized security scanning that automatically scans Red Hat technology for security gaps, vulnerabilities, and unauthorized changes in security configurations—and then remediates problems to restore security controls to an organization's established security configuration.

You can use Red Hat JBoss® BRMS as a common interface to multiple monitoring and analytic tools, such as Splunk, to create a centralized rapid incident response system that will quickly identify all instances of compromise. Working with existing security solutions using one application programming interface (API), an organization can isolate the attack and prevent its spread, eliminate the malware and fix the vulnerability, and minimize disruption. Continuous logging and advanced automation for all impacted networks allows for fast and efficient remediation, getting your systems up and running as quickly as possible.

4. **Collect and analyze.** Agency networks and systems generate enormous amounts of security-related data that, if effectively collected and analyzed, can significantly enhance an agency's CDM, incident response, and other security activities. For example, security analytics can collect data from multiple sources in near real time for event detection and remediation. It can also compare possible attacks across the enterprise from multiple locations and applications, such as Splunk, Tripwire, and Elastic. And it can deploy elastic monitoring so that the system expands in response to an incident and then contracts as the spike recedes. Agencies can also use analytic services to create rules that can flag specific conditions—occurring in a certain order or concurrently—and take automatic action to remediate the situation.

   Red Hat provides federal agencies with powerful analytic security capabilities and services. For example, Red Hat Enterprise Linux comes with a FedRAMP/FISMA-ready reference architecture that provides elastic and ephemeral compute and storage resources. Red Hat Ceph Storage and Red Hat Gluster Storage deliver scalable storage systems that support, in concert with JBoss, data integration and fusion necessary for collecting and analyzing large data sets in real time. Red Hat JBoss BPM Suite provides business rules management, business resource optimization, and complex event processing (CEP), while Red Hat JBoss Fuse serves as a critical component to securely and reliably ingest all continuous monitoring data and then route that data to the appropriate disparate parties. These processes can all be deployed as containerized services.

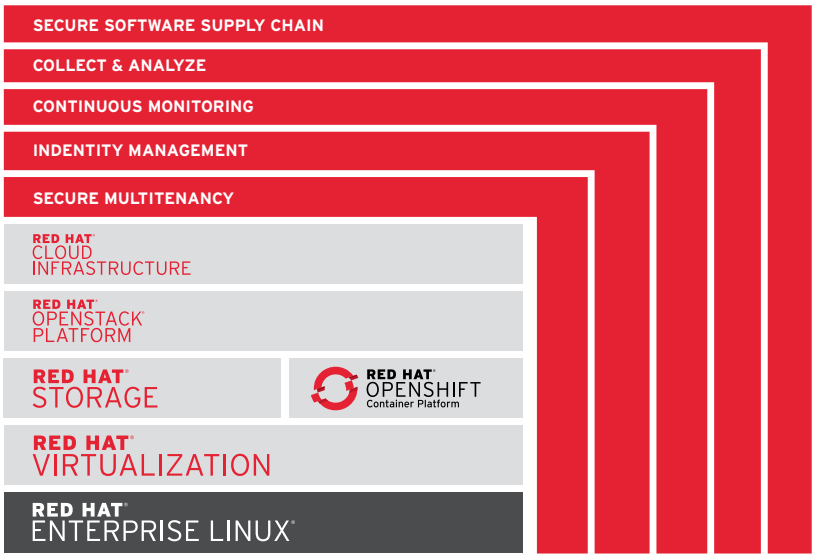
Agencies can implement cyber analytic capabilities as a service.
Red Hat OpenShift Container Platform can be used to architect an on-premise, in-the-cloud, or a mixed (hybrid) environment solution for storage and analytics. These would include things like Event Detection-as-a-Service, Identity Management Auditing-as-a-Service, and Logging-as-a-Service (rsyslog), among others. Analytic services can be provided for specific products such as Elasticsearch, Logstash, Kibana, and Apache Spark.

5. **Software supply chain security.** Software supply chains can pose serious security risks for civilian, defense, and intelligence agencies. As government agencies increasingly rely on outsourcing and commercial-off-the-shelf (COTS) products, they become susceptible to vulnerabilities that could be inserted—purposefully or accidentally—into software that has been developed outside an agency's supervision or control. Software may be delivered via email, CD, or File Transfer Protocol (FTP) and installed directly on a device without proper vetting. Employees can also reconfigure products in ways that introduce vulnerabilities. The technical challenge is how to attest and ensure that:

   - The software running in production matches the software that went through acceptance testing.
   - No malware was introduced.
   - Software versions match.
   - No new or undocumented attack surfaces were introduced.
   - File permissions, network accesses, etc. are properly configured.

   Red Hat gives federal IT administrators the tools to create an automatic, repeatable auditing process for ensuring software integrity. Security administrators can implement Satellite Open SCAP-Security Technical Implementation Guide (STIG) automation in
   Red Hat OpenShift Container Platform with Red Hat Cloudforms to automate the auditing of software. This capability provides software catalogs that compare the developer's trusted registries of software components with the deployed software. Audits of all components—from the OS-hypervisor through the containerized applications—are automatically created. (Containers inherit security parameters from the SELinux implementation.) OpenShift with CloudForms uses Auditing-as-a-Service to monitor software and ensure its integrity on an ongoing basis.

5 PILLARS



Red Hat SELinux provides the foundation for solutions and tools that support the five essential pillars for robust cybersecurity in the modern government organization.

YOUR PARTNER IN SECURITY

Red Hat technologies are used for secure government operations, from processing Medicare claims at the Centers for Medicare and Medicaid Services and handling air traffic at the Federal Aviation Administration to enhancing every tactical vehicle in the Department of Defense (DOD). We provide secure tagging of classified data for a major intelligence agency, and at DOD, we support the world's largest PKI user base and infrastructure. Our solutions are used throughout the federal government and in all 50 states.

With Red Hat solutions:

Security is written into the software. Because we co-develop software with our customers, you can build in the security capabilities you need, rather than trying to add them after the software's release.

Compliance is made easy. Red Hat solutions are delivered with preconfigured baselines that have already been tested and accredited as compliant with the government's most rigorous security requirements, including the Common Criteria, FIPS 140-2, FedRAMP, the Department of Defense STIG, FISMA, Section 508 accessibility standards, the Army Certificate of Networthiness, and the U.S. Government Configuration Baseline (USGCB).

Security exceeds traditional standards. Red Hat Enterprise Linux 5 and 6 received Common Criteria certification at Enterprise Assurance Level 4 under the Controlled Access Protection Profile (CAPP), Label Security Protection Profile (LSPP), and the Role-Based Access Control Protection Profile (RBACPP)—paving the way for you to create secure, open virtualized IT environments and move securely into the cloud.

Vulnerability updates are delivered automatically and rapidly. With Red Hat, 98% of critical vulnerabilities have had updates available the same day or the next calendar day.

MEETING GOVERNMENT'S HIGHEST SECURITY STANDARDS

For federal agencies striving to follow NIST's rigorous cybersecurity guidelines and standards, Red Hat security solutions provide a platform for implementing major portions of the NIST Cybersecurity Framework's technical requirements (see "Red Hat Solutions Align Directly with the NIST Cybersecurity Framework"). The NIST framework provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

Red Hat solutions align directly with the NIST Cybersecurity Framework

	NIST CYBERSECURITY FRAMEWORK				
RED HAT SOLUTIONS	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Red Hat Enterprise Linux	√	√	√		
Red Hat Virtualization	√	√	√		
Red Hat OpenStack Platform	√	√			
Red Hat Satellite	√	√			√
Ansible Tower by Red Hat	√	√	√	√	√
Red Hat JBoss BRMS	√	√	√	√	√
Red Hat Ceph Storage	√		√		
Red Hat JBoss Fuse	√		√	√	√
Red Hat JBoss Data Virtualization	√	√	√	√	√
Red Hat JBoss BPM Suite	√			√	√
Red Hat JBoss Data Grid	√			√	√
Red Hat OpenShift Container Platform	√	√	√	√	√
Red Hat CloudForms	√	√	√	√	√

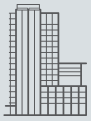
U.S PUBLIC SECTOR CYBER PRACTICE

Red Hat has a proven, 20-year track record of building Red Hat Enterprise Linux, the world's most secure operating system. And Red Hat Enterprise Linux security is inherited upwards as your agency's IT environment and mission requirements grow. As virtual servers evolve and support new applications and services, the security properties of the underlying infrastructure of Red Hat Enterprise Linux remain in place. All of the certification and accreditation built into the OS are passed to the virtual machines—the configuration, deployment of releases, patches, and new environments are scrubbed, controlled, and audited. Red Hat is recognized as a secure and trusted choice for open source solutions in government.

A FOUNDATION OF RESILIENCY

Government agencies are constantly striving to take advantage of both existing and new technologies to streamline operations and enhance performance. Hackers, criminals, and malicious state actors are equally relentless in their efforts to exploit vulnerabilities in the digital landscape. Cyber incidents in the federal government are not only growing in numbers but also in their ability to disrupt operations and mission activities. And herein lies the dilemma for federal organizations: How can we take advantage of our IT capabilities while also building the resilient security pillars needed to defend, protect, and quickly recover from the onslaught of cyber attacks?

The five cybersecurity pillars are essential to securing the modern enterprise. These are multitenancy security, identity management, continuous monitoring, collection and analysis, and software supply chain security. Of course, these are not the only cybersecurity pillars that agencies need. Whether your agency is seeking to strengthen its existing IT environment or adopt cloud and other new technologies, these five pillars provide a foundation for building a multilayered cyber defense that can reduce agency risk and strengthen the resiliency of your organization in a constantly changing threat landscape.



ABOUT RED HAT

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide 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
INC0399727_0716