PROTECT YOUR APIs WITH RED HAT AND ELASTIC BEAM

PARTNER TECHNOLOGY BRIEF

APIs SUPPORT BUSINESS TRANSFORMATION

To gain a competitive edge, many organizations are transforming by aligning people, processes, and technologies. To support these efforts, application programming interfaces (APIs) are key to IT services that speed delivery of new projects and improve integration with business partners. Standardized, open source APIs are being used successfully across industries, from banking to healthcare. However, taking full advantage of innovative APIs require solutions that offer comprehensive traffic visibility and updated security capabilities that protect business assets from threats.

Learn how an integrated solution from Red Hat and Elastic Beam can help you protect your APIs—and your data.

API CYBERSECURITY REQUIREMENTS

Many organizations that have deployed APIs lack in-depth visibility into client or machine activity on each API service. Reporting on API access—including the user's identity, commands or methods executed, and traffic generated—is critically important to meeting compliance requirements and discovering any malicious or unauthorized use.

Exponential API growth has broadened hacking activities that target back-end data and systems. Major organizations—including the Internal Revenue Service (IRS), Apple, Snapchat, McDonald's, Paypal, and Instagram—have reported API breaches resulting in compromised user information. Many companies have also experienced API-level distributed denial of service (DDoS) attacks that affected the performance, cost, and availability of their user-facing applications and cloud computing environments.

To minimize these security breaches, automated API traffic inspection identifies and automatically blocks malicious activity, such as:

- Takeover of client, patient, and citizen accounts or industrial control systems.
- Data deletion or modification.
- Data breaches of customer or patient records, banking information, or business plans.
- Service disruption or shutdown.
- Financial fraud against banks, retailers, and payment processors.

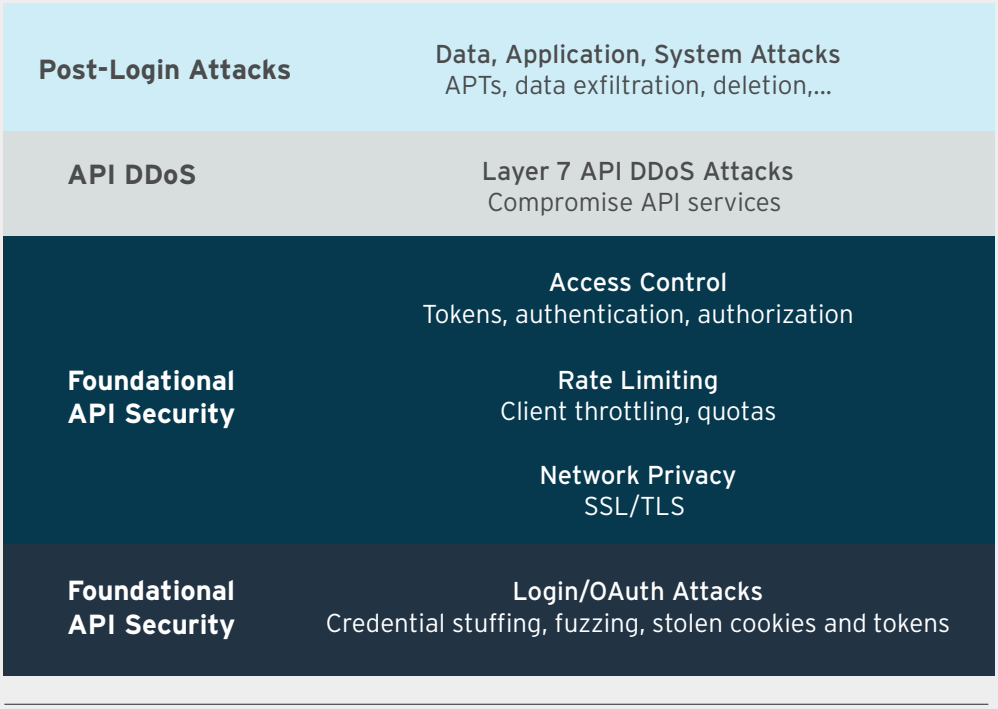


Figure 1. Types of cyberattacks affecting APIs

To protect API services from cyberattacks, organizations require comprehensive defense capabilities that automatically stop attacks on API services, including:

- **Attacks that defeat log-in systems:** Hackers probe for API vulnerabilities, attempt to use stolen credentials, or piggyback on valid sessions.
- **DoS and DDoS attacks**: These attacks are routinely undetected by existing DDoS defense products or content delivery networks (CDNs), as they are not traditional volumetric attacks that affect multiple systems. Instead, they target a specific set of API services with an attack that stays below single-client flow control limits to avoid detection—such as flooding API memory or session management services. However, the combined traffic can disrupt or shut down API services—or even use normal autoscaling cloud orchestration to generate unstoppable, extensive, and costly system resource use.
- **Attacks on data and systems**: Hackers who possess or have obtained valid credentials—by defeating the log-in environment successfully or piggybacking on valid sessions—use the API service to access data, line-of-business (LOB) applications, industrial systems, and other protected business assets. The intent is often to steal, delete, or manipulate information.
- **Internet API attacks (e.g. man-in-the-middle attacks)**: These attacks intercept internet API traffic and use the information for malicious activities.

COMPREHENSIVE API PROTECTION FROM RED HAT AND ELASTIC BEAM

Red Hat and Elastic Beam offer an integrated solution to help organizations protect their API environments from threats. This solution combines Red Hat® 3scale API Management and Elastic Beam API Behavioral Security to offer a robust API management solution that includes cyberattack protection and detailed traffic reporting for your API environment.

This integrated solution offers enterprise-ready capabilities, including:

- Flexible support for on-premise, cloud-based, or hybrid deployments, as well as containers.
- Comprehensive insight reporting.
- Seamless scalability based on traffic.
- Self-learning, AI-based protection.

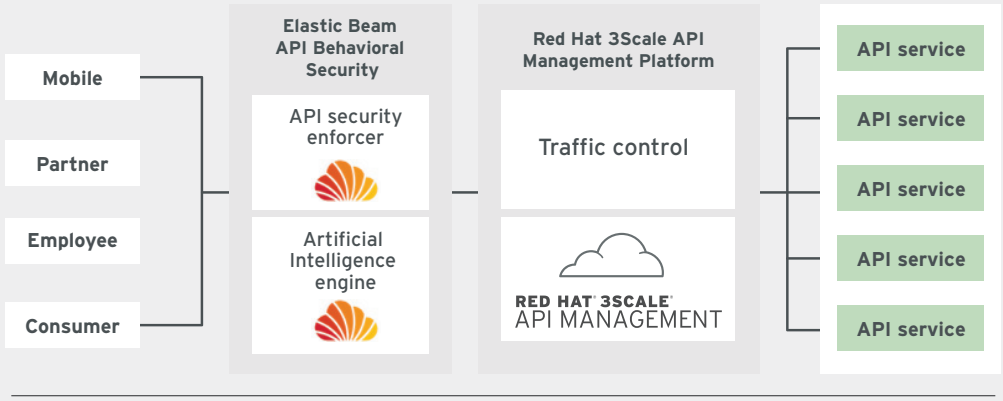


Figure 2. Red Hat and Elastic Beam API security solution

RED HAT 3SCALE API MANAGEMENT

- **Authentication**: Provides several options for API authentication that can be used alone or in combination to issue credentials and control access, including:
  - Standard API keys
  - Application ID and key pair
  - OAuth authorization protocol, versions 1 and 2
- **Access control**: Expands basic security and authentication with application and account plans that restrict access to specific endpoints, methods, and services and simplify access policy for user groups. Tiered access levels support monetizing your API with paid access plans.
- **Rate limits**: Set rate limits for API use—such as per-period limits for incoming APIs—and control traffic for groups of developers to protect your infrastructure and keep traffic flowing smoothly. Automatically trigger alerts and define responses for applications that reach or exceed rate limits.
- **Network privacy**: Enforce Transport Layer Security (TLS) version 1.2 encryption for strong API traffic protection.

ELASTIC BEAM API BEHAVIORAL SECURITY

Elastic Beam API Behavioral Security automates cyberattack detection, blocking, and reporting using live, AI-powered security. It is optimized for RESTful and WebSocket API environments.

- **Comprehensive threat protection**:
  - Prevent probing for vulnerabilities or attempts to defeat access controls.
  - Stop insiders or hackers from using stolen credentials for malicious activities.
  - Block attacks on data, apps, and systems—including data theft or destruction, host or account takeover, clients using stolen cookies or tokens, addition of code to the API infrastructure, or attacks targeting session management systems.
  - Protect against API-specific DoS and DDoS attacks with real-time overload protection to complement Red Hat 3Scale API Management rate limiting functionality. Attacking clients may further be identified by the AI engine and automatically blocked to stop the DDoS attack.
- **Rich traffic visibility and reporting**:
  - Easily gain insight with graphical dashboards.
  - Access detailed reporting of all activity for each API, including use trend analysis, debugging of complex applications, and every method or commands used.
  - Accelerate gathering of evidence after an attack to expose all activity.
  - Track compliance with optimized reports.
  - Access in-depth reports for forensic investigations and compliance. In addition, an API is provided to deliver information to any JavaScript Object Notation (JSON) enterprise reporting application.

Figure 3. Elastic Beam graphical attack activity dashboard

- Deliver information to other enterprise dashboards used to aggregate information or any JSON enterprise reporting application.

- **Instant, automated attack detection and response**:
  - Instantly trap hackers and attack patterns with API-based deception. Decoy API access is instantly recognized. The hacker is allowed to continue activity but blocked from accessing valid APIs. The attack footprint is logged, analyzed, and reported by the AI engine.
  - Terminate identified attacks automatically across environments.
  - Block API access based on real-time traffic validation.
  - Stop attacks without requiring signatures or programming security rules using self-learning capabilities. Elastic Beam API Behavioral Security can recognize multiple types of DoS and DDoS attacks that can only be identified with AI algorithms, and attack sources are usually identified and automatically blocked.

INDUSTRY USE CASES

HEALTHCARE

Hospitals, clinics, and other healthcare providers can protect their patient information accessed via online portals. Monitoring of inbound activity protects against:

- Unauthorized access to patient online accounts.
- Illegal extraction and anomalous changes to patient medical information, healthcare records, or private data.
- Service disruptions from excessive inbound activity on customer portals.
- Irregular activity or unauthorized, remote control of Internet of Things (IoT) devices.

Post-login activity is continuously monitored to detect malicious activity that violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Extensive reporting provides visibility into all API use to demonstrate compliance.

FINANCE AND INSURANCE

Financial institutions using Open Bank Project APIs or those that must meet Revised Payment Service Directive (PSD2) requirements need complete visibility into API sessions to show compliance. They can also protect APIs from malicious actions, including data injection or extraction. Log-in service traffic is controlled to stop access disruption or credential stuffing to compromise accounts. Security analysts can use detailed reports for forensic investigations.

In addition, banks and other financial institutions can protect against:

- Extraction of customer account data, banking data, or other sensitive information.
- Malicious customer account activity, such as unauthorized fund transfers.
- Abnormal internal user activity.
- Portal service downtime due to DDoS attacks.

GOVERNMENT

State and federal agencies can deploy API deception to instantly trap hackers and collect attack information. All inbound traffic to API services is monitored to prevent Layer 7 DDoS attacks. System logins are monitored for credential reuse, and all outbound API activity is analyzed to detect data access or manipulation. With API deception capabilities, attack information is automatically distributed across a hybrid cloud environment to block hackers across all locations.

In addition, agencies can protect against:

- Suspicious extraction or deletion of sensitive data, including classified records and private data.
- Probing for unauthorized system access.
- Illegal application access.
- Injection of code or other malicious content.
- Disruption of public services.

LEARN MORE

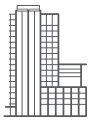
With the progression towards more connected, API-based technology, selecting the right API platform is crucial to business innovation and growth. Together, Red Hat 3scale API Management and Elastic Beam API Behavioral Security offer comprehensive API development, cybersecurity, and reporting capabilities, helping organizations to thrive in this new API environment.

Learn more about Red Hat 3scale API Management at redhat.com/en/technologies/jboss-middleware/3scale.

Learn more about Elastic Beam's solutions at elasticbeam.com.

ABOUT ELASTIC BEAM

Founded in 2014, Elastic Beam is headquartered in Redwood City, CA (Silicon Valley). The company delivers AI-powered cybersecurity for the API-based economy. Elastic Beam's flagship solution, API Behavioral Security, was built by Silicon Valley entrepreneurs with a history of success in the cloud infrastructure, API gateway, and security markets. To learn more about how Elastic Beam can bring intelligence and security to your API environment, email us at sales@elasticbeam.com.



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
#f10190_0118