Why Security Must Move to the Application Layer

The perimeter defense paradigm is broken

Most information security experts agree that the old paradigm of defending the perimeter, hosts, and endpoints is broken. They point to several trends:

1. Perimeters have become too porous. Hackers can take advantage of mobile devices, compromised web sites, social networking applications, and other poorly defended avenues into corporate networks.

2. Cybercriminals have become more sophisticated, more targeted, and more patient. They use spear phishing and social engineering to capture user credentials, and then extract confidential data using techniques that evade detection by traditional perimeter and host security products.
3. **Enterprises no longer control their complete infrastructure.** Most organizations now use software-as-a-service (SaaS) applications and cloud computing resources that they can’t monitor or control directly.

Many threats can be detected only with business-specific logic

There is also a fourth factor at play:

4. **Many of the most insidious information security threats can be understood only with reference to business context and business-specific logic.** Insider threats, fraud, and attacks from focused “adversaries” don’t have simple signatures that can be detected at the perimeter. They can be identified only by detecting patterns of behavior. Sometimes these patterns are meaningful only to a single industry or even a single organization.

Shift attention to application-level security

The logical response to these trends is to not only continue with a defense-in-depth strategy using traditional security tools, but to also shift more resources and attention to application-level security.

In fact, there are many advantages to enhancing security at the application level:

- **Better protection against cyberattacks and fraud.** Recent statistics show that a majority of security vulnerabilities are caused by security flaws in application and web software, yet most organizations invest only a small percentage of their security budgets to monitor and protect that software.

- **Simplified compliance.** Many government regulations and industry standards mandate the protection of specific types of business data (for example, customer account data, protected health information, and cardholder data). Application security is the most direct way to show compliance with many of these mandates.

- **An opportunity to enforce business rules and operational policies, as well as technical policies.** Application security can alert administrators to business policy violations.

In short, better monitoring and security at the application level should result in fewer data breaches, faster audits, and more predictable operations.

Three Components of Application Security

There are three key components of application security: Secure Application Development, Application Security Monitoring, and SIEM (Security Information and Event Management). These are illustrated in Figure 1.

In this paper, we will talk briefly about Secure Application Development, go into more depth about Application Security Monitoring, and then discuss how Application Security Monitoring and SIEM can work together to provide the highest levels of application monitoring and attack detection.
Secure Application Development

Best practices for the software development life cycle

Secure Application Development is the process of building security best practices into every step of the software development life cycle (SDLC) in order to minimize vulnerabilities in application code.

This includes analyzing security requirements and performing threat modeling in the requirements-gathering phase of the SDLC; following security design guidelines during the design phase; enforcing secure coding practices and conducting security-oriented code reviews during the development phase; performing static code analysis and dynamic web scanning tests during the test phase; and conducting security-oriented physical deployment reviews during the deployment phase.

Organizations can also take advantage of resources such as the OWASP Top 10 project, security publications from the Department of Defense and Defense Information Systems Agency, standards like PCI DSS and HIPAA, and other projects that identify common application vulnerabilities and define application security best practices.

The limitations of Secure Application Development

However, organizations also have to recognize limitations to Secure Application Development:

- **Slow adoption.** It takes years to train architects, developers, and testers, and to build security into all phases of the SDLC.

- **Code from outside parties.** There can be compelling economic and time-to-market reasons to utilize purchased applications, hosted SaaS applications, code from outsourcing partners, and open source software, but organizations cannot impose their own secure development practices on these suppliers.

Figure 1: The three components of application security: Secure Application Development, Application Security Monitoring, and SIEM.
Legacy applications. It is usually not feasible to retrofit existing applications with all required security features and secure coding practices.

Evolving threats. Newly emerging threats and attacks require new countermeasures, which often cannot be incorporated into existing applications.

For these reasons, prudent organizations must assume that at least some of their production applications are not fully secure against the latest threats, and must look toward additional defenses at the application level.

**Application Security Monitoring**

The second key component of application security is Application Security Monitoring (see Figure 1). This means observing applications as they execute and alerting administrators to anomalous behaviors, including:

- Evidence of scans and probes by hackers and unauthorized users.
- Indicators of known attack types, such as SQL injection attacks, cross-site scripting, and remote file inclusions.
- Attempts to access secure data by users who don’t normally use the data or requests for unusual quantities of data.

Such behaviors can be logged and used to trigger alerts to systems administrators and information security personnel.

There are two approaches to Application Security Monitoring: code it into each application, or deploy a third-party Application Security Monitoring tool.

**Monitoring in individual applications**

Some organizations code security monitoring into each application. The ability to tailor logging and monitoring to the organization’s industry and business practices appears to offer an advantage. However, in practice, there are major drawbacks to the code-it-yourself approach:

- Most application developers are accustomed to writing code to handle use cases, not abuse cases. They may not have the experience or knowledge to anticipate all likely attacks and abuses, or to write complex logic to detect probes, unauthorized access to data, and other kinds of attacks.
- Most application logging mechanisms implemented by developers collect too little information for comprehensive security monitoring. The log events they do record are usually non-standard and difficult to correlate with logs from other applications and systems.
- Most organizations utilize legacy applications and at least some packages from third parties, and it is rarely possible to retrofit application monitoring into these.

Finally, many sophisticated attacks and forms of fraud cannot be detected by monitoring individual applications. They can be identified only by correlating events across multiple applications, or across applications and firewalls, intrusion prevention systems, and other network and security devices.
Application Security Monitoring tools

Application Security Monitoring tools operate “inside” applications to observe application and user activities and to identify anomalous behaviors.

For example, an Application Security Monitoring tool might detect:

- SQL statements included in data entry fields on a web form.
- Private data being sent over the Internet.
- A user logging on at 3:00 a.m. from an IP address that is not from the user’s home country.
- A query to download an atypically large number of records from a customer account database.
- A user in sales accessing an engineering database containing confidential intellectual property.

While some of these suspicious behaviors can be understood in purely technical terms (evidence of a SQL injection attack), others are meaningful only because they violate business norms (salespeople rarely access engineering documents). This ability to utilize business context is not available to security tools that operate “outside” of applications.

Application Security Monitoring tools also have several key advantages over the approach of writing monitoring code into individual applications:

- They incorporate the extensive knowledge and experience of the software vendor and the vendor’s customers regarding attacks, abuses, and methods to detect suspicious activity.
- They can collect, normalize and log many types of application data, to compensate for limited logging built into the applications themselves.
- They can be deployed with legacy and purchased applications. There is no need to modify the applications or develop custom logs.
- They have well-designed methods for creating customized business rules.
- In some cases, they have out-of-the-box capabilities to interface with SIEM systems (discussed in the next section).

Combining Application Security Monitoring with SIEM

SIEM systems aggregate security and log data from many sources, including routers; gateways and other network devices; firewalls; intrusion protection systems and other security solutions; database, server and other system logs and directories; and identity management systems. SIEM systems can correlate these masses of data and alert operations and security personnel to probes, attacks, policy violations, unauthorized activities by insiders, and other indicators of security breaches.

Application Security Monitoring tools can feed event streams to SIEM systems, so application-related data can be correlated with network and security events and other systems data (see Figure 2).
In fact, Application Security Monitoring tools and SIEM systems are an extremely powerful combination, because together they can identify subtle patterns of behavior that neither technology by itself could pinpoint.

The combination can be particularly effective when it takes advantage of industry- and company-specific business logic.

**A Financial Industry Example**

Let's look at an industry-specific scenario.

An Application Security Monitoring tool is monitoring a customer account management application. It detects a SQL injection attack in the act of capturing a customer’s login credentials (Figure 3, top). Later it finds a user with those credentials querying the account database (Figure 3, bottom).

These events are streamed to the SIEM system. There, correlation rules determine that this user was behaving in an atypical fashion, and further that the accounts are being accessed in the sequential order of the account numbers. Custom rules in the SIEM system indicate that this is highly suspicious activity, because individual customers never have sequential account numbers. The SIEM system then puts the user on a suspicious actor list and notifies the financial institution’s fraud team. Administrators temporarily block fund transfers by that user, preventing the cybercriminal from wiring funds to an off-shore account.
This example shows how an Application Security Monitoring tool and a SIEM system can work together and use industry-specific business rules to detect complex, multipart attacks that would elude individual security technologies.

**Conclusion: The Case for Application Security Monitoring and SIEM**

The movement toward increased application monitoring is being driven by the limitations of traditional perimeter and host security products, by the increased sophistication of hacker and insider threats, and by the challenges of providing security when parts of the infrastructure are located at SaaS and cloud computing sites.

But it also reflects the increased value that can be provided by utilizing a new technology, Application Security Monitoring, particularly when combined with SIEM systems. The benefits include:

- Better protection against cyberattacks and insider security threats.
- Simplified compliance with government regulations and industry standards through better monitoring of application and user actions.
- The effective use of custom business logic and business context to detect fraud and sophisticated attacks targeting specific industries and companies.

**HP Enterprise Security: A Single Source for Advanced Application Monitoring**

Enterprises looking for the most advanced application monitoring tools should consider solutions from HP Enterprise Security.
HP Enterprise Security

HP Fortify RTA is an application security monitoring tool that is extremely easy to implement, provides data on a wide range of attacks, provides for the creation of sophisticated custom business rules, and allows for customized responses to attacks.

HP ArcSight ESM is an industry-leading SIEM platform that can correlate and analyze extremely high volumes of data from the widest variety of systems and devices.

Security events identified by HP Fortify RTA can be streamed to HP ArcSight ESM, where they can be correlated and analyzed with many other types of security and operational data, with no special integration work required from the enterprise.

And the HP Enterprise Security organization can provide a full range of implementation and support services so advanced application monitoring solutions can be deployed smoothly, integrated with other best-of-breed security systems, and configured for maximum effectiveness.

About HP

HP is a leading provider of security and compliance solutions for modern enterprises that want to mitigate risk in their hybrid environments and defend against advanced threats. Based on market leading products from ArcSight, Fortify, and TippingPoint, the HP Security Intelligence and Risk Management (SIRM) Platform uniquely delivers the advanced correlation, application protection, and network defense technology to protect today’s applications and IT infrastructures from sophisticated cyber threats. www.hpenterprisesecurity.com

Find Out More

For more information about application monitoring, HP Fortify RTA, HP ArcSight ESM, and other industry-leading enterprise security products from HP, please visit the HP Enterprise Security web site at: www.hpenterprisesecurity.com.

1 Gartner has stated that: “Over 70% of security vulnerabilities exist at the application layer, not the network layer.” Quoted in Computerworld, February 25, 2006 (http://www.computerworld.com/printthis/2005/0,4814,99981,00.html). A Microsoft survey found that application vulnerabilities were reported about four times as often as browser vulnerabilities and operating system vulnerabilities combined. Microsoft Security Intelligence Report, Vol. 9, January through June 2010 (http://www.microsoft.com/security/sir/keyfindings/default.aspx#section_3_1).