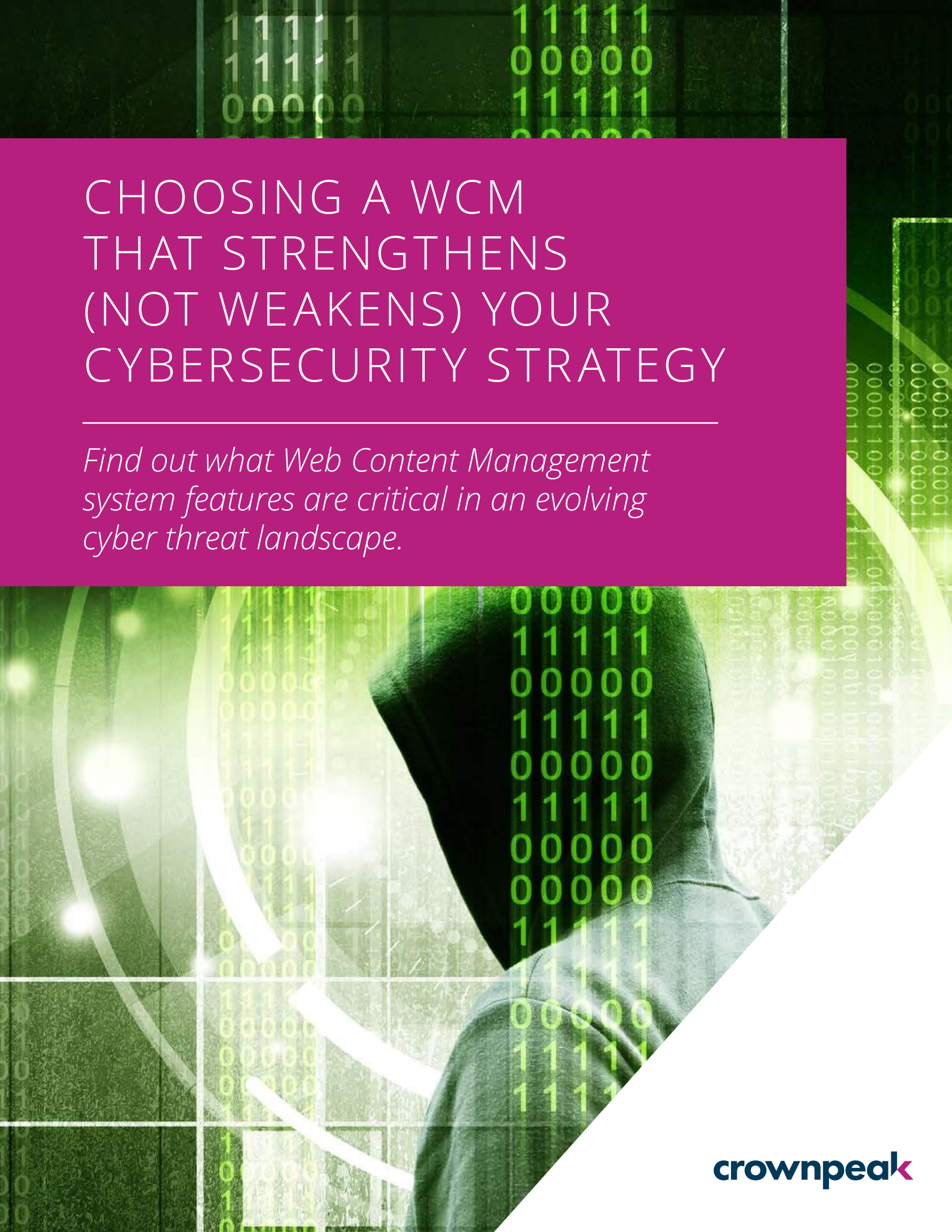
CHOOSING A WCM THAT STRENGTHENS (NOT WEAKENS) YOUR CYBERSECURITY STRATEGY

Find out what Web Content Management system features are critical in an evolving cyber threat landscape.



crownpeak

CONTENTS

INTRODUCTION: A NEW WORLD OF CYBERCRIME

On Friday, May 12, 2017, the WannaCry ransomware cryptoworm first reared its ugly head, and within 24 hours had infected over 230,000 computers in over 150 countries. Britain's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, as well as many other nations and companies around the world, in what became one of the biggest cybercrime exploits in history.

WannaCry is only the latest tip of the cyber threat iceberg to break the surface. According to just one cybersecurity firm, ThreatMetrix, they detected 130 million online fraud attacks alone in the first quarter of 2017, up 23% from the same period the year before. (Source: "Cybercrime: US Tops Priority, Europe Tops Production" Security Intelligence)

The sophistication and proliferation of cyber threats – viruses, ransomware, DDoS attacks and more – has grown startlingly, fueled by malice, political machinations or greed, with actual "cybercriminal web stores" sprouting up where criminals buy and sell credit card data and other stolen personal information, according to security researchers. (Source: Palmer, Danny, "Super-expensive Ransomware Linked to Online Cybercrime Market, Say Security Researchers" ZDNet)

Other sobering stats about the rise of various types of cybercrime?

- **97% of web applications** contain at least one vulnerability. (Source:" The 2016 Trustwave Global Security Report" Trustwave)
- DDoS attacks have **increased at a rate of 75%** year over year. (Source: "Q4 2016 DDoS Trends Report" Verisign Blog)
- The financial impact of a DDoS attack **can range from $100K - $1M**. (Source: "The Corporate IT Security Risks 2016 study" Kaspersky Lab -

Organizations of every type are now at risk, not just those reliant on transactional websites. DDoS attacks persist, but now vulnerability exploits (which we'll get into later) are the new "silent assassins" taking advantage of the increased opportunities presented by the expanding online footprints of global enterprises.

What are some of the outcomes for enterprises victimized by cybercrime?

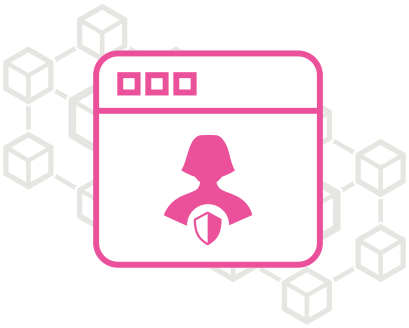
- The loss and exposure of customer data
- Financial losses to the organization
- The cost of litigation and liabilities if they're sued by customers
- Impersonation of the brand for nefarious purposes by criminals
- Reputational and brand damage that can be difficult to repair, if repairable at all (just ask **AshleyMadison.com** and **Yahoo!**)

In this threat landscape, **choosing the right Web Content Management (WCM) platform** is crucial to protecting an enterprise against attacks and their consequences. In this guide, we'll examine those threats in detail, and explain the standards to follow in picking a WCM that will help defend against them as part of an overall cybersecurity strategy.

> *One pair of enterprising hackers advertised a Mirai botnet of 400,000 bots, available for rent for DDoS attacks*
>
> **Source: Bleeding Computer**

THE ROLE OF YOUR WCM WHEN IT COMES TO SECURITY

Today's rising cyber threat level comes as the result of a "perfect storm" of factors. Large companies now offer a huge array of digital touchpoints, increasing the "attack surface area" to be far larger than just a few years ago. They also deploy heterogeneous platforms and technologies that are often safeguarded by varying and inconsistent levels of security.



Another contributor? Many companies have **mistakenly relied on their hosting providers** to insulate them against cyber crime. While Amazon AWS, for example, supply robust controls to maintain security and data protection, those only extend to the services it delivers as a host.

Simply assuming that your cloud-based sites and touchpoints are receiving ironclad 360° protection from your hosting provider is a mistake, because your operating systems, apps and proprietary platforms are your responsibility to secure.

Many of the enterprises targeted by WannaCry may have utilized rock-solid hosting services, but it was Windows vulnerabilities that opened the door to the bad guys. The same thing can happen to your WCM, simply by not fully understanding what aspects of security your WCM provider is responsible for managing.

When selecting a Web Content Management (WCM) platform, look for stringent security capabilities that A) bolster your overall security strategy, and B) work in tandem with the protections delivered by your hosting provider.

The key to building a holistic security management infrastructure that delivers the greatest possible defense against threats, starts with gaining a clear understanding of which security aspects your vendor is responsible for, and which ones rest on your shoulders.

THE THREAT OF CRIPPLING DDOS ATTACKS

A Distributed Denial of Service (DDoS) attack is an attempt to exhaust the resources available to a site or application in order to impair its ability to serve legitimate traffic.

These are considered ***distributed*** attacks because they're launched from diverse network locations, making them harder to neutralize. And like most cybercrime, they are on the rise, in various forms:

- DDoS attack frequency **exploded by 380%** in the first quarter of 2017 versus the prior year, according to analysts.
- TCP DDoS attacks grew from slightly over **10%** to **over 26%**, while UDP attacks grew from slightly over 2% to nearly 9%, and ICMP attacks rose from 1% to over 8%. (Source: Advisory, Nexusguard Threat. "Threat Advisories" Q1 2017 DDoS Threat Report)
- In 2017, "DDoS of Things" (DoT) attacks burgeoned, as they were increasingly launched using millions of compromised IoT devices now connected to the Internet.

A common goal of DDoS attack perpetrators is to make money, which is why banks, stockbrokers, and other financial services companies tend to be the most attractive targets. These attacks can inflict such serious material and reputational damage that many enterprises prefer to pay the cyber crooks' ransom demands.

500,000 IoT devices will suffer from at least one security compromise in 2017
Source: Forrester

Varieties of DDoS Threats

There many different types of DDoS attacks, and they typically target different layers of the infrastructure serving a site or application.

They can be broadly divided into two separate areas:

- The first is the **Application Layer**, also known as **Layer 7**. This is where the perpetrator interacts with the website functionality to attack it.

- The second type takes place at the **Network Layer**, often referred to as **Layer 3**. In this case, the underlying transportation (not the website itself) is attacked.

Cyber criminals often amplify the destruction by targeting both layers.

The primary offenders?

- **Volumetric attacks** occur at the **Network Layer**, where the perpetrator floods the network interfaces with high volumes of traffic until it can't respond because it is overwhelmed.

- **Protocol/State Exhaustion attacks** exploit weaknesses in underlying network protocols to tie up resources. One example might be opening a connection, keeping it open, then opening another connection and so on, until there are no more connections available.

- **Application attacks** exploit application protocols by issuing multiple requests to a website in order to tie it up, so that it can't respond to legitimate requests.

> *During the first quarter of 2017, **93%** of DDoS attacks used **a mixture of volumetric and application attacks**, so enterprises that lacked multi-layer security safeguards were vulnerable.*
>
> Source: Alexander Khalimonenko, Oleg Kupreev, "DDOS Attacks in Q1 2017" Securelist

VULNERABILITY EXPLOITS

A **vulnerability** is any flaw, glitch, or weakness found in software or an OS that can lead to the compromise of a system. One common example is a buffer overflow, where specially crafted data intentionally exceeds the space allocated by the system, sometimes permitting the execution of malicious code and access to restricted areas of the system.

Exploits that target software vulnerabilities are often the **"silent killers"** because organizations often don't notice they've been attacked until after the damage has been done, or is well underway.

Unauthorized access and the covert gathering of data can sometimes go undetected for weeks, months, or years (as was the case with the Yahoo data breach, where it took almost two years to discover that 500 million email accounts had been compromised).

Once discovered, software companies often issue patches for vulnerabilities. Unpatched vulnerabilities are known as "**zero-day vulnerabilities**."

These unpatched vulnerabilities can be discovered in various ways by cybercriminals, who deploy bots or scanners to crawl sites and applications, looking for security chinks to exploit.

Whether for the purposes of theft, espionage, or as a spring-board to other systems, attackers who gain admin control over a web content management system can then infect it with malware, access confidential data, or invade an entire network.

The RAND Corporation released a study in early 2017 that laid out a few eye-opening facts about zero-days, including:

- Zero-day vulnerabilities have an average life expectancy of nearly **seven years**, with as many as a quarter of them surviving for over nine years.

- The median time it takes to create an exploit for a known vulnerability is **22 days**.

- "Zombie" vulnerabilities exist: due to code revisions, they can be exploited in older versions of a software product, though not in the latest versions.

One example of how hard it is to kill off an exploit?

In 2016, the most popular zero-day exploit was the one used to spread the StuxNet virus. Even though a patch was provided in **2010**, the vulnerability still exists on countless copies of multiple Microsoft operating systems. (Source: "2016's Most Popular Exploit Was the Vulnerability Used for the Stuxnet Attacks" BleepingComputer)

In 2016, there was a 300% increase in daily ransomware attacks over 2015, when there were 1,000 attacks per day.

Source: CCIPS

RAISING YOUR WCM DEFENSES

An organization can't rely on its web hosting service for the entirety of its online security. It needs to deploy multiple layers of defense in front of its websites and digital touchpoints. That's why a WCM environment should perform just as ably at protection as the most bulletproof hosting service.

Unfortunately, WCMs are often overlooked when hardware, software, and operating systems get patched for security threats. That leaves a susceptibility that allows hackers to potentially uncover an entry point to an otherwise secure environment.

That's especially true for on-premise WCM systems, where companies don't often anticipate the need for a holistic security patch management program that upholds the highest possible security standards.

Another problem? Typically, users of many WCM systems, especially open-source ones, lack expert knowledge of the technology itself, let alone the security issues involved, spawning even more vulnerabilities.

Fortunately, an increasing number of organizations, particularly those that function on a global scale, are now making security a key yardstick in their WCM selection processes.

WHAT TO LOOK FOR IN A SECURE WCM

1. Compliance with industry & regulatory standards

A WCM provider seeking to service a global company needs to be able to prove it meets the recognized best practice standards for security and compliance, whether they're industry benchmarks or regulatory mandates.

In a best-case scenario, the WCM follows a "shared responsibility" principal, where it's already built atop a standards-compliant hosting service such as Amazon Web Services (AWS), and in addition the same standards are built into the WCM itself, offering layered compliance and protection.

> **Regardless of where they deploy content via their WCM, whether from a data center in their home market or half-way around the world, an organization needs assurances that their operations continually comply with applicable standards.**

Independent audits should confirm your platform-of-choice's alignment with guidelines and regulatory structures that can include FISMA, HIPAA, SSAE 16, ISAE 3402, US-EU Safe Harbor, TRUSTe Cloud Privacy and others, depending on the industry.

2. TLS & Encryption standards

TLS certificates prove the integrity and confidentiality of data as it passes between a user's browser and a site. Organizations like PCI, NIST & Mozilla document recognized industry standards and best practices.

Certificates require careful management and should be renewed on a regular basis to reduce the chance of compromise. The longer a certificate has been in existence, the greater the risk of compromise or accidental exposure of a private key, so it is strongly recommended that they be updated often.

Traditionally, an organization's IT department will provision certificates every 2-3 years, but a superior WCM provider will take on the burden and see to it that TLS certificates are renewed much more frequently. This diligence significantly lowers the probability of personal data being exposed for unethical use.

What do best of breed TLS and encryption standards look like in the context of a WCM platform:

- They provide continually **up-to-date standards** for encryption of data at rest and in transit.

- They ensure that HTTPS-enabled sites and applications meet **Qualys Grade A security benchmark**. Depending on an organization's use-case they many need to go beyond this, for example complying with NIST government standards.

- **Auto generation and renewal of TLS certificates** on a frequent basis (in the case of Crownpeak, every 3 months) with no noticeable loss of service, human intervention, or the need to share sensitive information (like private keys between parties.

- An automated **managed process for HTTPS certificates**, without any need for customer intervention.

3. Advanced security layering

Your WCM should aggregate multi-layered protections like those in the example below, extending all the way into the application layer, and feature real-time analytics and intelligence to detect and act on perceived threats.

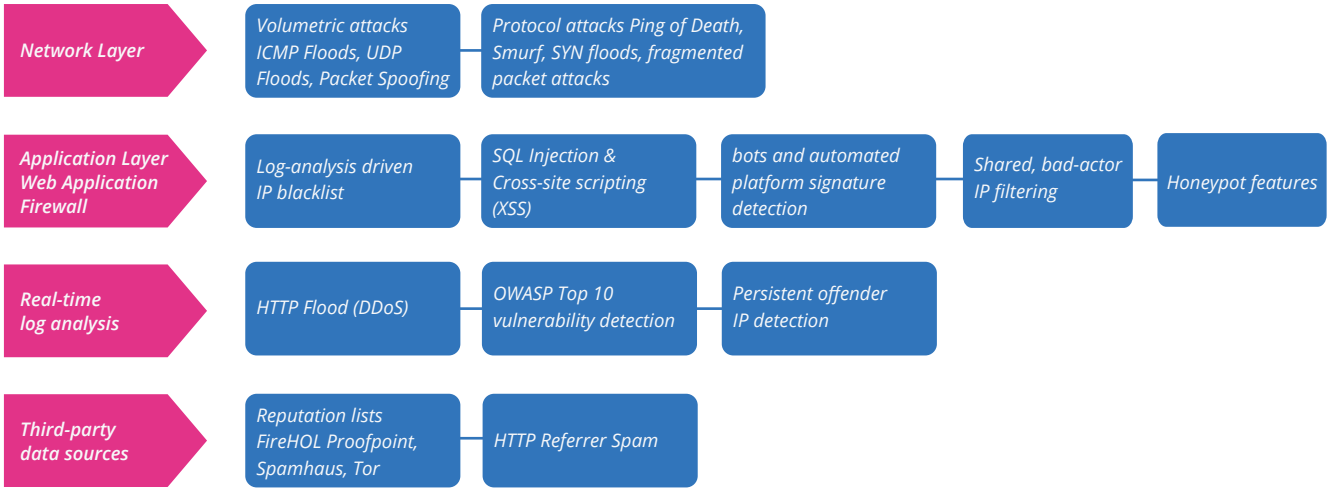
Some specific offerings to look for when evaluating WCMs:

- **Log analysis:** A WCM provider should monitor traffic coming into the website in order to spot patterns and block attacks. Log files should be analyzed after the fact to identify potential attempters and hacks, and block future requests from sources that pose a threat.

- **Threat intelligence:** IP reputation lists should be updated every day based on third-party threat intelligence providers, and traffic should be blocked from known criminal and spam organizations.

- **Gathering insights:** A WCM provider should provide intelligence to customers based on what their applications are doing so they can determine if the application is being used in a way that it shouldn't be used.

One example of a thorough WCM defense plan that covers all layers:



4. Other considerations

- The WCM provider should supply **shared threat intelligence and response**, so if one customer is attacked, the same effective defense is extended to other customers automatically.
- The WCM should integrate efficiently with your own **identity management platform**, whether it utilizes federated identity (FID) authentication or single sign-on (SSO).
- Choose a WCM that has sophisticated controls for **managing users** including defining roles, setting user access levels and more, since threats can originate from within.

SUMMARY

It's not quite a lawless melee on the web, but any enterprise wanting to operate digital touchpoints in an omnichannel engagement age needs to mount across-the-board protections.

Those should include choosing the right WCM system, one that offers full-featured, multi-layered defenses that are part of a holistic, integrated security scheme.

But no matter how advanced it may be, **a WCM can only do so much**. A huge responsibility for its own security still lies in the hands of the enterprise, which can't afford to entirely abdicate its role to automated platforms.

That would only put another advantage in the hands of hackers and cybercriminals, who are always poised to take advantage of a potential victim's moment of inattention.

crownpeak

crownpeak.com

Founded in January 2001, Crownpeak was the first company to offer web content management through a SaaS solution. Today, leading brands trust Crownpeak's cloud-first Digital Experience Management (DXM) platform to quickly and easily create, deploy and optimize customer experiences across digital touchpoints at scale.

Crownpeak provides a complete solution for DXM featuring content management, personalization, search and hosting, in addition to fully integrated Digital Quality Management (DQM) to ensure brand integrity and meet compliance requirements. More than 200 customers rely on Crownpeak to deliver engaging experiences that delight customers, promote loyalty and deliver results.