radware

Guide

Overcoming Staff and Skill Shortages in Application Protection

Cybersecurity staff and skill shortages affect organizations worldwide, and nearly no company is immune to their effects. This is particularly a problem when it comes to application protection. While finding and retaining trained cybersecurity experts will likely remain a challenge in the years ahead, there are a number of key measures that organizations can begin taking today. These will go a long way in alleviating the impact of these staff shortages, and help organizations improve the quality of their web application protection programs.

Adjusting to a Reality of Staff Shortages

Combine this complexity with tightened budgets and the shortage of security expertise worldwide and thoughts of securing your applications becomes even more stressful. Trying to cobble together a security plan with different vendors only serves to muddy the waters. It results in poor security and higher costs. It creates security siloes that can spell disaster.

Cybersecurity staff and skill shortages have been consistent trends over the past few years. According to the (ISC2) 2022 Cybersecurity Workforce Study, the 2022 global cybersecurity workforce gap stood at 3.4 million people, an increase of 26.2% from 2021. This means that not only are cybersecurity staff shortages continuing, but they're getting worse and impacting organizations' ability to fight cybersecurity incidents.

Indeed, according to the report, 70% of organizations believe they do not have sufficient cybersecurity staff to be effective. Moreover, over half of employees at organizations with cybersecurity staff shortages rated the risk of cyberattack—as a result of these shortages—as "moderate" to "extreme." For organizations with "significant" staff shortages, 20% of employees rated the risk of cyberattack in their organization as "extreme."

Looking at the reasons for cybersecurity staff shortages, the leading causes were an inability to find enough qualified talent (43% of organizations), employee turnover (33%), inability to offer competitive wages (31%) and low budgets for cybersecurity programs (28%).

These findings are indicators of a prevalent, far-reaching, and persistent reality: organizations can't find enough people, and those that they can find—they can't keep.

This reality means that organizations must adjust their approach and adopt new measures which are not as heavily reliant on internal staff to maintain their cybersecurity programs and tools.

Web Application Security Becoming a Dedicated Discipline

One of the areas where the shortage in cybersecurity staff and skills is most pronounced is the domain of web application protection.

As web applications become the core of business functions, application protection takes an ever-more important role in protecting those applications, their availability and customer data that is processed through them.

However, as its importance grows, application protection is also growing in depth and complexity, with a unique set of attacks, tools and mechanisms for mitigation attacks. As a consequence, it is becoming a dedicated discipline within cybersecurity, distinct from other domains or specializations.

The implications of this development is that successful web application security programs require not just dedicated tools to protect against all types of various attacks, but also dedicated people, who specialize in application security and hold sufficient knowledge and expertise to properly protect applications.

Below are some of the top reasons why web application protection is now a dedicated discipline within cybersecurity, along with the proficiencies required by application security professionals in order to provide high levels of protection.

Reason #1: Greater Domain Expertise

One of the great challenges of web application protection is that application security is not a standalone topic. It's one that straddles multiple domains within cybersecurity and computing. To understand application security, one must understand applications. And to understand applications, ones must possess a deep understanding across computing and IT. Some of these topics include:

- Networks: How they are designed, built, configured and protected
- Applications development: How applications are developed, how they are architected, what technologies are used in building it, what is the development process and which stakeholders are involved it, and how they are rolled out
- Application capabilities: What is the business function of the application, what are its key capabilities, and how users interact with it
- Cloud computing: As most web applications are now deployed in the cloud, understanding public cloud, private cloud and hybrid clouds is paramount
- Kubernetes and microservices: How microservices (and specifically Kubernetes) work, how they are managed, their deployment lifecycle, and how they differ from traditional application design

It is no surprise, therefore, that finding qualified staff which possesses all of this knowledge is no easy task.

Reason #2: A Bigger, More Complex Attack Landscape

Apart from topic related to how applications are built and implemented, a key requirement in application security is understanding the threats facing modern applications today. As a result, it is crucial to hold a deep understand of application attacks, attack vectors and emerging threats.

This includes an understand of web application attacks, bot attacks, API attacks and vulnerabilities, application-layer (L7) DDoS attacks, and—increasingly—supply-chain and client-side attacks.

For each such vectors, it is required to understand how they are planned, how they are executed, how they are distinct from other attack vectors and their potential impact on application security

Reason #3: Broader Set of Tools

As the list of application threats has expanded, so has the list of tools available—and required—for application defense. Therefore, it is necessary for application security professionals to hold an in-depth understanding of security tools and mechanisms.

Application security today is more than just web application firewall (WAF). Itincludes bot protection, application-layer (L7) DDoS protection, API security, client-side protection and more. Application security professionals must know all these tools, how they work, what they cover (and what they don't cover), and how to use all these tools together to create a comprehensive protective armor around modern applications.

Since applications are a core part of the business, application security professionals need to understand more than how to deploy these tools and

implement security policies.They also need to know how to tailor them to the legitimate user behavior patterns of the application's users, eliminate false-positives, and review logs and analytics to identify potential security vulnerabilities.

Reason #4: Impact Across the Business

Finally, since applications are a core focus of the business, a key requirement in application protection is to understand how application security impacts the greater organizations—and it's bottom line.

While application security is recognized as essential, there is an inherent tension between security and agility. Many business teams want to be as agile and flexible as possible, working without any constraints. But security, by definition, is about imposing constraints so that malicious activity does not get through. So while security is recognized as essential, web application security can also be an inhibitor or showstopper for certain organizational business units such as DevOps, marketing, cloud operations and more.

The challenge is how to maintain state-of-the-art application protection, while remaining as frictionless as possible and not imposing operational or technical challenges, which may impact the company's bottom line.

Therefore, it is essential for web application security professionals to have that acumen and be cognizant of how application security impacts existing business and technology processes. They must knowhow to minimize the friction, while maintaining a high level of web application protection.

Overcoming AppSec Staff and Skill Shortages

There are three primary measures that organizations can start taking today in order to reduce reliance--and load--on internal cybersecurity staff: consolidation, automation and fully managed security services.

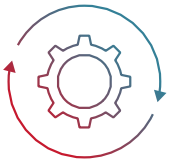
Measure #1: Consolidation

The first measure to address cybersecurity staff shortages is consolidation of security tools. The mathematics are simple: the fewer tools to manage and maintain, the less time and energy you spend switching between systems and management consoles—and the ower the load on the cybersecurity staff.

The solution is to consolidate individual tools and defenses providing piecemeal protections into one-stop-shop, best-of-suite tools. These provide coverage across a wide range of attacks and threat vectors from within a single tool—and a single management and reporting dashboard.

This approach enables security teams to maintain the same level of protection while speeding-up processes with centralized management and reporting. They can also spend less time switching between systems and integrating separate products.

One thing to note: Make sure that security is not degraded in the process of consolidation. This requires selecting a best-of-suite tool, which is also best-of-breed security-wise, in order to make sure that your maximize your cybersecurity protections.



Measure #2: Automation

The next measure to reduce the load on cybersecurity staff is to automate as many processes as possible, thereby replacing slow and labor-intensive manual configurations.

When it comes to cybersecurity, automation can fall into two categories:

- **Security automation** - automation of actual cyber defense activities such as policy configuration, rule configuration, signature creation, etc.
- **Deployment automation** - automation of the deployment of cybersecurity mechanisms in a way which does not interrupt existing business or technical processes.

As attacks grow increasingly larger and more sophisticated, security automation is essential in order to provide constant protection against attack. Any type of security process which is based on manual processes is inherently vulnerable to shifting attack patterns and new, zero-day attacks for which there are currently no protection signatures.

This is a particularly difficult problem in a staff-constrained world, where there aren't enough qualified people who have the time and skills to quickly respond and perform these activities when an attack occurs.

By combining these two types of security automation measures, organizations can reduce both the direct load on cybersecurity teams (such as those involved with creating new rules, defining security policies, etc.), as well as mitigate the broader impact of cybersecurity measures on the organization at large. They can do this by lowering the impact and interruption caused to other teams such as DevOps, IT, operations, marketing and more.

Measure #3: Fully Managed Security Services

Finally, the third measure is outsourcing your cybersecurity functions and relying on expert, fully managed security services to do the heavy lifting for you.

The term “cybersecurity” refers to a massive domain, which encapsulates within it many dedicated sub-disciplines. Examples of such sub-domains include network security (firewalls, VPNs, secure web gateways, etc.), application protection (WAF, bot protection, DDoS protection, and more), endpoint security (anti-virus, EDR, etc.), email security, public cloud security (workload protection, CSPM, IAM security, and more), and many, many others.

Each such subdomain is distinct in its scope of protection, attack vectors, threat surfaces and tools. And as the threat landscape becomes more complex, these domains are only growing further apart and becoming more dedicated and specialized.

As a result, it is virtually impossible to find cybersecurity staff who possess knowledge and expertise of each of those domains and the tools required to defend them. This means that even if your organization has the enough people, in many cases they won’t have the right skills to cover all your bases.

Therefore, it makes sense to rely on fully managed security services and effectively outsource certain security functions to dedicated teams of experts for whom these activities are their daily routine.

It is important to make sure that managed-security teams have a proven track record within their industry or domain, and that they are properly staffed and trained. However, this approach can greatly help alleviate the burden on internal cybersecurity teams, while simultaneously enhancing the level of protection.

How Radware Helps Organizations Overcome AppSec Staff Shortages

As a leader in web application protection, Radware provides a comprehensive set of measures to help organizations streamline and simplify their web application security mechanisms, thereby reducing reliance on manual configurations and helping overcome the shortage of cybersecurity staff and skills:

Measure #1: Automation:

As cyberattacks--and cyberattackers—become more sophisticated, it is increasingly more difficult to rely on any type of security measure which is dependent on manual configuration. In an attempt to test cyber defenses, attackers have learned to constantly shift their attack vectors. As a result, defenses based on any type of manual configurations, rules, or policies will be quickly exposed, as they will not be able to keep up with morphing attack characteristics.

Moreover, as applications constantly change, and user behavior patterns also shift over time, security rules and policies must constantly adapt in order to allow legitimate user traffic to pass through, while still blocking malicious requests.

Radware’s application protection tools provide a number of key automation features to help with improving security efficacy while reducing the risk of false positives:

- **Automatic traffic learning:** Radware's application protection tools are based on a positive security model, which allows only legitimate user request while blocking traffic that falls outside of legitimate user behavior. This approach is predicated on automated traffic learning capabilities, which learn the behavior of legitimate users and create a baseline of legitimate user behavior. They then blocks everything which falls outside these behavioral patterns.
- **Automatic policy optimization**: After Radware generates security policies which are custom-tailored to these customer behavior patterns, it begins a process of continuous policy optimization, using machine-learning algorithms to review ongoing security logs and automatically suggest security policy refinements, thereby producing more accurate security protection with less work for security teams.
- **Automated false positive correction:** In an attempt to remove barriers to legitimate user activity, Radware's WAF engine automatically scans for potential false-positives and alerts on them, so that security administrators can allow them as needed.

Measure #2: Comprehensive, Centralized Application Protection

Another key measure in narrowing staffing gaps is eliminating any unnecessary friction in managing security tools. This is done by combining multiple disparate tools into a single, best-of-suite, unified platform which covers all the required bases.

Radware's cloud security platform provides a comprehensive, one-stop shop for web application protection, covering all the key attack vectors and threat surfaces:

- **Web application firewall** – for protection against web attacks such as SQL injection, cross-site scripting (XSS), server-side request forgery (SSRF), and other OWASP Top 10 threats (and more).
- **Bot manager** – to discern between human and non-human web traffic and differentiate between good bots (such as search engine crawlers) and bad bots (such as web scrapers, DDoS botnets, etc.).
- **API protection** – with built-in, fully automated API discovery, to identify any undocumented APIs or API calls, and enforce protection of all of the organization's APIs.
- **DDoS protection** – for behavioral-based protection against DDoS attacks both at the network layer (L3/4) and the application layer (L7)
- **Client-side protection** – for protection of client endpoints against supply-chain attacks such as formjacking (Magecart) or DOM XSS attacks.

Radware's platform also provides a centralized management console, with unified dashboards, reporting and management for all these capabilities.

Measure #3: Frictionless integration

In today's modern environment, application protection is no longer a standalone discipline of its own; it is inherently intertwined with application development, deployment, delivery, DevOps and even marketing and social media. This is why frictionless integration is so important to application security: web application protection in the modern era isn't supposed to get in the way.

Radware offers a unique ability for frictionless integration in the form of the Radware SecurePath architecture. Unlike traditional application protection mechanisms,

which are inline, the Radware SecurePath architecture operates out-of-band, thereby providing seamless application protection without requiring changes to existing architecture or processes.

Traditional application protection tools all operate inline: either as an appliance (for local deployments), or via DNS redirection (for cloud-based deployments). While this approach allows for inspecting all traffic, it also induces interruptions to existing deployment methods and adds extra hops and latency in cloud deployments. This is particularly a problem in multi-cloud and hybrid cloud deployments. Although out-of-path deployment options existed, they were usually limited to alerting-only tools.

The Radware SecurePath architecture, on the other hand, provides full protection from the first packet via an API-based, out-of-path approach. By integrating with the application server, whenever a request comes in, an API call will be sent to the nearest Radware PoP with the request details, where it will be analyzed for suspicious activity, and malicious requests will be blocked. This allows full protection without requiring any changes to the data path, without adding extra traffic hops, without adding latency, and even without requiring the SSL/TLS certificate of the application.

Measure #4: Managed Security Services

Finally, Radware helps organizations overcome cybersecurity staff shortages with its managed security services, spearheaded by its Emergency Response Team (ERT).

As application protection becomes more and more of a dedicated discipline, many organizations find themselves in shortages of qualified staff who have the adequate knowledge, skills and experience to identify and protect against web application attacks.

Radware's cloud application protection services are, by default, a managed service, with Radware's SOC and support staff taking responsibility for helping customers with onboarding, configuration, ongoing monitoring, 24/7 support and attack-time protection.

This approach helps organizations both to improve the quality of their web application protection programs with experienced AppSec experts, who work easily with application protection day-in and day out, while simultaneously reducing the burden on internal staff by allowing them to focus on their organization's core responsibilities.

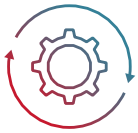
Overcoming Staff Shortages as a Practice in Reducing TCO

In today stressed economic environment, many organizations are looking for ways to cut costs and reduce total cost of ownership (TCO) on their cybersecurity tools. What many organizations don't realize is that many of the measures outlined in this paper will not only improve the quality of security protections, but will also aid them in reducing costs.

Some of the key measures to reducing TCO include:

Consolidation of solutions and vendors

Reduce the number of vendors and consolidate to a smaller number of tools which will cover more ground



Automation of resource-heavy processes

Improve the quality of protection while simultaneously speeding-up processes and reducing the amount of manual work required for them

Integrated, centralized management & visibility

Spend less time switching between tools and dashboards with single, centralized management and visibility console

Use a fully-managed security service

Take the burden of web application protection off of the shoulders of your team, improve the quality of protection and spend less resources doing it

Summary

The long-lasting impact of the COVID-19 epidemic, together with expanding threat surfaces and the growing complexity of attacks, has made staff shortages an enduring reality in many organizations. This is particularly true in web application protection, which is increasingly becoming a dedicated discipline within cybersecurity.

Overcoming these gaps requires a combination of elements centered around consolidation, automation, and expert managed security services.

As a leader in web application protection, Radware provides a comprehensive set of measures to help organizations streamline and simplify their web application security mechanisms. It helps organizations reduce reliance on manual configurations and overcome the shortage of cybersecurity staff and skills.