DARKREADING

Report August 2024

Why Multi-Layered Defense is Critical in Application Security

Commissioned by OPSWAT. | F5

Introduction

In an increasingly digital work environment, cybersecurity gaps are an ever-present concern among IT and cybersecurity leaders within organizations. These leaders have been sounding the alarm on possible vulnerabilities for years, and the recent surge in cyberattacks validates their concerns.

According to the World Economic Forum's 2024 Global Risks Report, cyberattacks are a top-three concern for government and private-sector respondents. The financial impact of cybercrime is substantial and growing, with Statista's Market Insights estimating the global cost of cybercrime to rise from $9.22 trillion in 2024 to $13.82 trillion by 2028.

To better understand the security challenges organizations are facing, cybersecurity leaders OPSWAT and F5 worked together with Dark Reading to survey IT and corporate leadership on a wide range of cybersecurity topics. This report, filled with statistics and direct quotes from IT leaders, reveals surprising insights into the frustrations and challenges experienced by cybersecurity professionals.

The survey highlights significant concerns, including the lack of preparedness for escalating DDoS attacks, noncompliance with regulatory requirements, and a perceived lack of support (both in attention and resources) from organizational leadership. The answers make it clear that industry best practices help - but not every organization is following them closely.

Even with shift-left approaches moving testing earlier in the development lifecycle, CISOs see a need for a mindset change in the organization. To quote one respondent who works as an engineer, "Integrating security practices throughout the entire software development lifecycle, from requirements gathering to deployment and maintenance, can be challenging. Ensuring that security is a core consideration at every stage and not an afterthought requires a significant cultural shift and buy-in from all stakeholders involved."

In this comprehensive report you will find:

An analysis of the current state of cybersecurity, highlighting the most common types of attacks such as denial of service, data theft, and ransomware.

A review of existing best practices that some organizations are following.

Identification of gaps in cybersecurity measures and their impact.

The consequences of failing to meet compliance standards.

Insights into how cybersecurity practices are evolving in response to emerging threats.

This report aims to provide a clear and actionable understanding of the cybersecurity landscape, helping organizations fortify their defenses and mitigate the risks associated with cyber threats.

"Ensuring that security is a core consideration at every stage and not an afterthought requires a significant cultural shift and buy-in from all stakeholders involved."

- ENGINEER

Key Challenges

Complexity of Web Application Security

Web application security is a complex endeavor. The rising migration and deployment of cloud-hosted web applications pose continuous challenges for security teams. In fact, as of 2023, 60% of all corporate data is stored in the cloud. In highly regulated industries, the issue may be even more pronounced, as those industries are migrating to the public cloud four times faster than less regulated industries. All this complexity leads to added stress for security leaders. Failing a penetration test due to non-compliance with cybersecurity guidelines (like OWASP) can lead to legal penalties, financial losses, reputational damage, operational disruptions, and a competitive disadvantage.

Additional elements combine to make web application security even more involved, including a lack of experienced personnel across the cybersecurity world and a complex web of interconnected tools, including in-house solutions and useful but potentially vulnerable open-source options.

Regulatory Compliance and Best Practices

Maintaining regulatory compliance and adhering to OWASP requirements before and during production is a significant challenge for organizations. Only 27% of respondents in this survey regularly reference OWASP for web application security best practices. NIST is the highest-referenced organization, with 53% of respondents citing it as their primary guide, followed by CISA at 37%. Other frameworks such as CIS, SANS, and STIG are referenced by only 24%, 19%, and 9% of respondents, respectively. This disparity in adherence to best practices highlights the difficulties organizations face in navigating the complex landscape of web application security standards.

Implementation Challenges

Survey respondents noted how challenging it can be to implement end-to-end application security in their organization's current environment. There seems to be a disconnect between what security leaders believe they need and the support organizations give them. Budget constraints, limited resources, and reactive attitudes were common complaints.

- One IT executive respondent explained, "Tech folks are stretched extraordinarily thin and are responsible for far more disparate systems than anyone in the enterprise can fathom. Combine that with a budget that is extraordinarily tight - and often shrinking - and you have a situation where it is impossible to 'check all the boxes' that CISA and NIST, etc. come up with."
- A developer highlighted that "Organizations are reactive, not proactive" and pointed out a "lack of proactive evaluation of future risks across the organization."

These comments highlight the real struggles of maintaining strong security measures with limited resources and emphasize the need for a cultural shift towards more proactive security practices.

"Educational tech folks are stretched extraordinarily thin and are responsible for far more disparate systems than anyone in the enterprise can fathom. Combine that with a budget that is extraordinarily tight - and often shrinking - and you have a situation where it is impossible to 'check all the boxes' that CISA and NIST, etc. come up with."

- IT EXECUTIVE

Leaders Feel Unprepared and Under-Resourced

Overall, the top three concerns preventing leaders from feeling adequately prepared for security threats are budget shortages, staff training inadequacies, and lack of attention (Figure 1). This data mirrors a recent IANS survey where more than one-third of CISOs reported flat or shrinking cybersecurity budgets in 2023. Many of the other obstacles to improving security flow from this fundamental issue, as leaders are finding it difficult to implement or improve multi-layered security without the resources to make it happen.

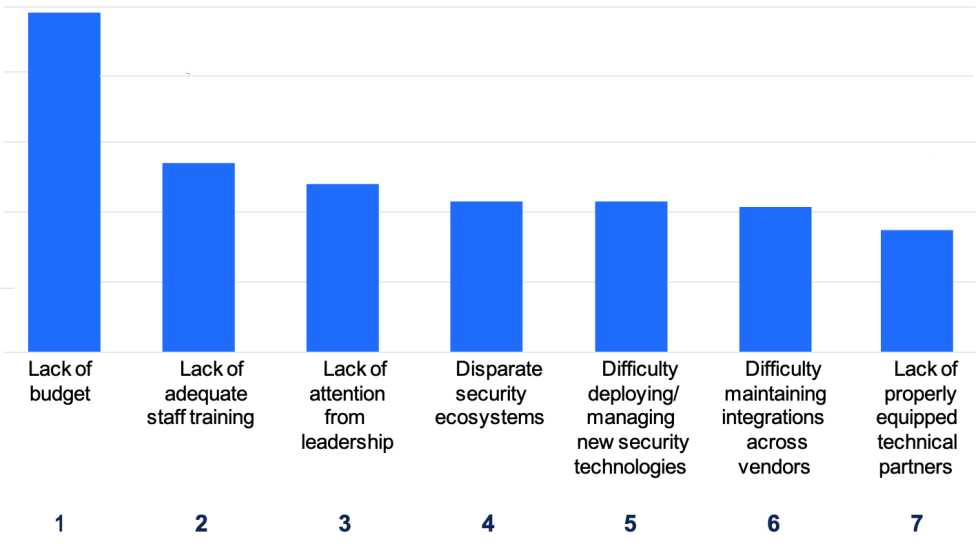
Beyond budgets, "disparate security ecosystems" and "difficulty deploying/managing new security technologies" were identified as significant issues. One IT Manager respondent noted their biggest challenge as "Executive leadership's basic lack of understanding or caring for anything IT related." There's clear frustration here, and these challenges highlight the complex and multifaceted nature of maintaining robust cybersecurity defenses in today's rapidly evolving digital landscape.

The security leaders surveyed are facing these challenges at a time when threats to their systems are more prevalent and sophisticated than ever.

FIGURE 1

Reasons Not Prepared for Security Threats

Please rank the reasons your organization may not be adequately prepared for security threats from the most to least significant factor.



Note: Rank is based on a weighted score. Items ranked first are valued higher than subsequent items, and the score is based on the sum of all weighted counts.

Data: Dark Reading survey of 131 cybersecurity and IT professionals, May 2024.

Evolving Threats Landscape

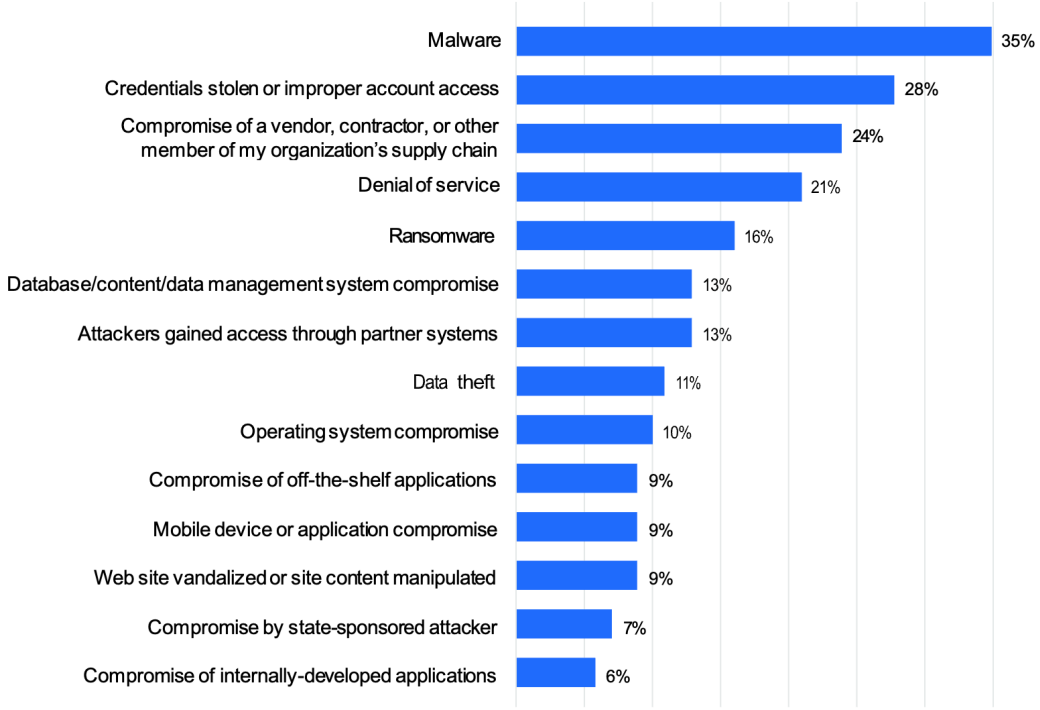
Cybercriminals already deploy a wide variety of attacks on organizations, and many are successful. Among those surveyed, 35% reported suffering a malware breach in the last year (such as the UnitedHealth ransomware attack that will cost the company $1.4-$1.6 billion), 28% experienced credential theft or improper account access, and 24% faced a compromise involving a vendor, contractor, or other member (Figure 2). While no single type of breach affected the majority of organizations, the survey results indicate significant breaches across various attack vectors.

In addition to common threats, malicious actors are continually innovating their attack strategies. Evolving threats such as file-borne malware, including Botnets, Zero-Days, and Advanced Persistent Threats (APTs), present a blind spot in web application security.

FIGURE 2

Cybersecurity Breaches in Past Year

Which types of cybersecurity breaches have occurred in your organization in the past year?



Note: Multiple responses allowed

Data: Dark Reading survey of 131 cybersecurity and IT professionals, May 2024

Types of File-Borne Malware and Examples:

Botnets

Description

Networks of infected computers controlled remotely by attackers, often used to launch large-scale attacks such as DDoS.

Example

Volt Typhoon: A court-authorized operation in December 2023 disrupted the “Volt Typhoon” botnet, which used hijacked SOHO routers for China state-sponsored hacking activities.

Zero-Days

Description

Vulnerabilities in software that are unknown to the vendor and for which no patch exists, exploited by attackers before the vendor can address them.

Example

In February 2024, Microsoft disclosed critical Exchange Zero-Day vulnerabilities and an Azure breach compromising executive accounts, leading to cloud account takeovers, phishing attempts, and NTLM credential impersonation.

Advanced Persistent Threats (APTs)

Description

Prolonged and targeted cyberattacks where attackers gain and maintain unauthorized access to a network, often remaining undetected for an extended period.

Example

Lazarus attacks: The Lazarus group, linked to North Korea, has conducted cyberattacks for years, attacked supply chains and critical infrastructure in 2023.

While many organizations have some level of preparedness for these threats, most acknowledge there is still work to be done.

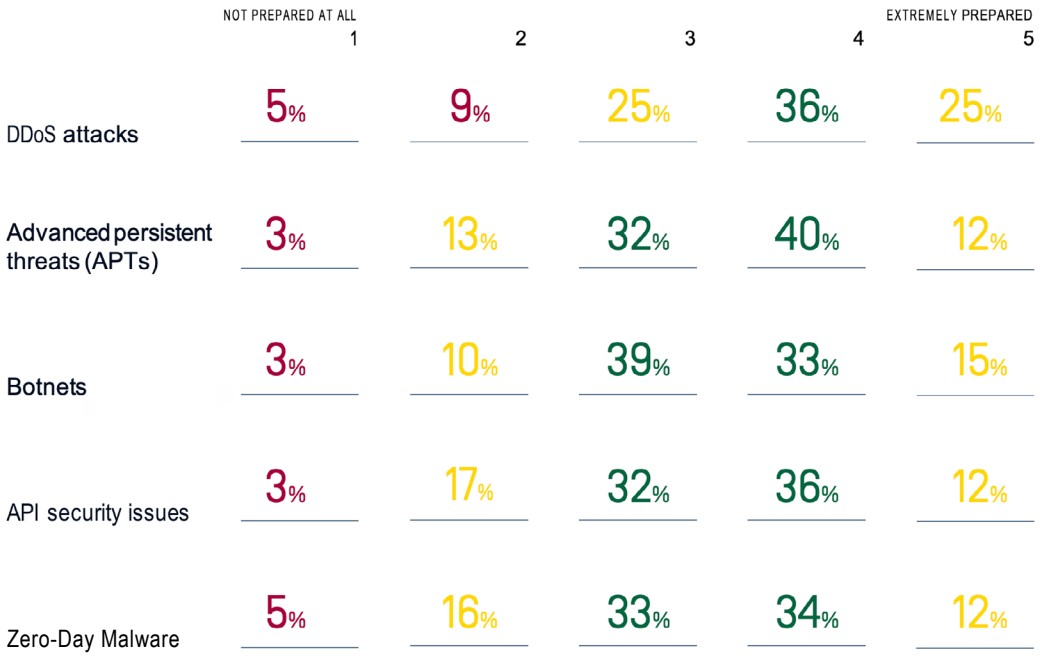
Only 25% of respondents described their organization as "extremely prepared" for DDoS attacks (Figure 3). Preparedness for other threats, such as APTs, Botnets, API security issues, and Zero-Day malware, was even lower, with only 12% to 15% of respondents feeling extremely prepared. OWASP regularly updates its Application Security Verification Standard and its Top 10 Application Security Risks to give organizations clear guidelines on how they can prepare their environments to thwart attacks. Yet, as noted previously, a lack of resources limits the ability to adhere to guidelines.

Organizations are currently deploying various methods to combat DDoS threats.

FIGURE 3

Preparedness Against Emerging Threats

How would you evaluate your organization's preparedness against each of the following emerging threats?



Data: Dark Reading survey of 131 cybersecurity and IT professionals, May 2024

Common Defense Strategies

Sandboxing

A security method that runs programs or code in a restricted environment to isolate them from the main system, ensuring they cannot cause harm if they are malicious.

Content Disarm and Reconstruction (CDR)

A technique that analyzes and removes potentially harmful elements from files, reconstructing them to ensure safety while preserving the original content.

Behavioral Analysis

The practice of observing and analyzing the actions of users and systems to detect abnormal behavior that might indicate a security threat.

Vulnerability Scanning and Management

The use of automated tools to find, assess, and manage security weaknesses in systems, helping organizations to prioritize and mitigate potential threats effectively.

Security Testing

Processes used to evaluate the security of applications, including methods like penetration testing and code reviews, to identify and fix vulnerabilities before they can be exploited.

User Education and Awareness

Programs aimed at teaching employees about cybersecurity practices, helping them to identify threats like phishing and understand the importance of secure behavior.

The most commonly used strategies among those surveyed include:

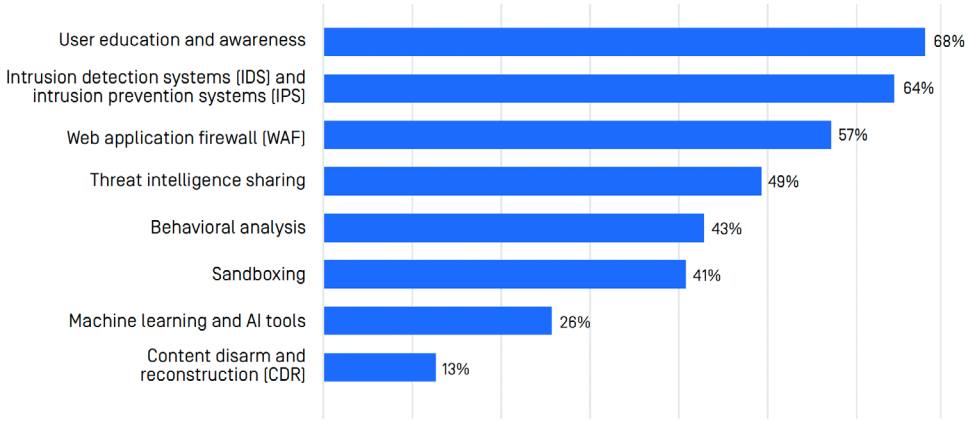
- User education and awareness (68%) to defend against Zero-Day malware
- Security testing (58%) to secure the software development lifecycle
- Vulnerability scanning and management (73%) for automating application and API security (Figures 4, 5, and 6)

Despite these efforts, many organizations struggle with application security stacks that are too diverse and difficult to integrate. They often lack the capability, flexibility, or manageability necessary to provide cohesive and effective security. This highlights the ongoing challenge of adapting to an evolving threat landscape and the need for continuous improvement in cybersecurity. One area of improvement is implementing defense-in-depth strategies.

FIGURE 4

Defending Against Zero-Day Malware

What methods does your organization use to defend against zero-day malware?



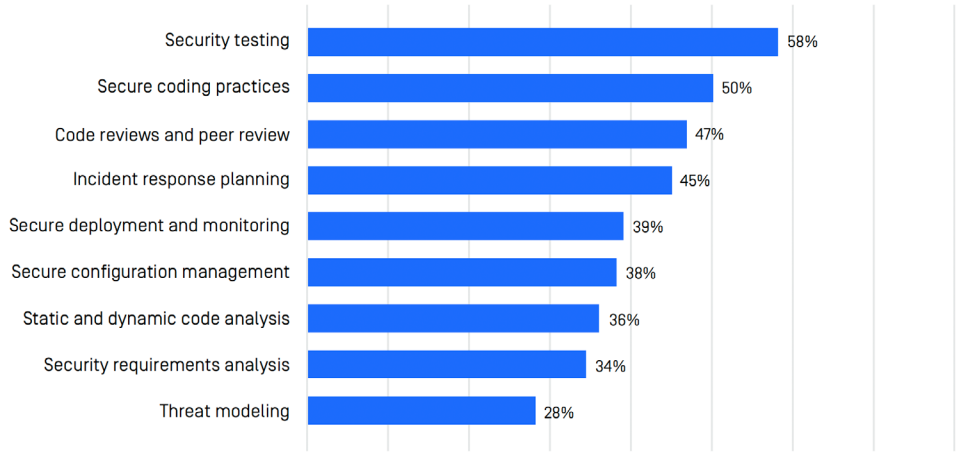
Note: Multiple responses allowed

Data: Dark Reading survey of 131 cybersecurity and IT professionals, May 2024

FIGURE 5

Securing Software Development Lifecycle

What methods does your organization use in its secure software development lifecycle?



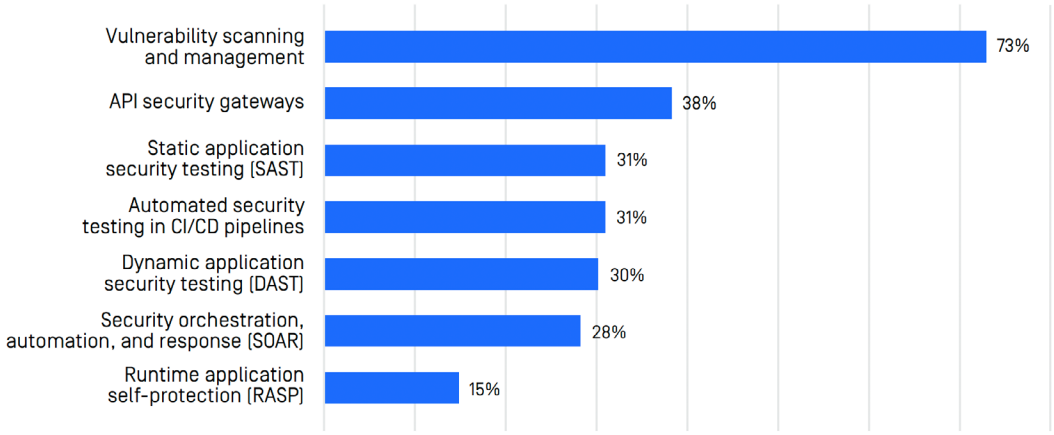
Note: Multiple responses allowed

Data: Dark Reading survey of 131 cybersecurity and IT professionals, May 2024

FIGURE 6

Automating Application and API Security

Which methods does your organization use for automating application and API security?



Note: Multiple responses allowed

Data: Dark Reading survey of 131 cybersecurity and IT professionals, May 2024

Defense-in-Depth Strategies

CISA recommends that organizations develop defense-in-depth strategies, which involve applying multiple countermeasures in a layered manner to achieve security objectives. This holistic approach uses specific countermeasures implemented in layers to create a comprehensive, risk-based security posture. The core idea is that if one countermeasure proves vulnerable to attack, the combined security of multiple countermeasures will still protect the organization effectively. Despite the awareness of these strategies, the survey shows that most organizations are lagging in their implementation.

While almost all respondents (94%) have at least "slightly implemented" defense-in-depth strategies, only 17% have "fully implemented" them (Figure 7). This gap indicates a need for organizations to strengthen their commitment to a multi-layered security approach.

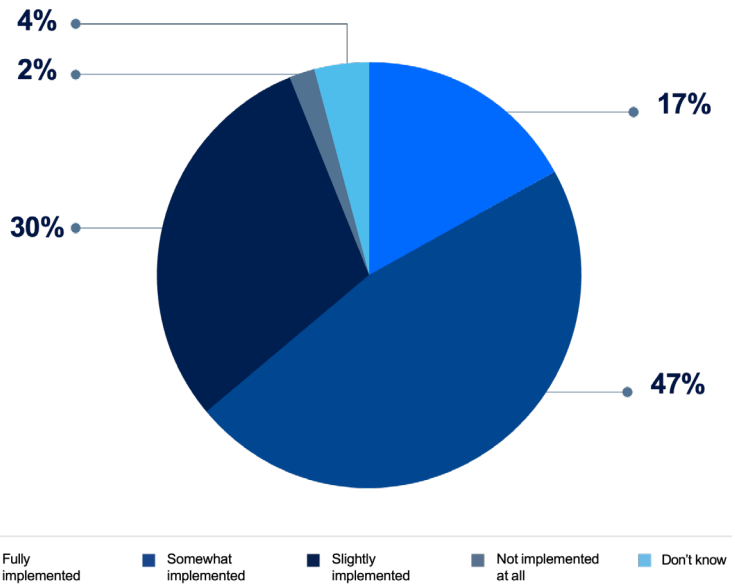
To combat the evolving threat landscape, organizations need a comprehensive end-to-end solution — one that covers network-based attacks and file-based malware. By fully implementing defense-in-depth strategies, organizations can create a robust security posture that minimizes risks and ensures that multiple layers of defense protect their assets from potential threats.

83% of companies have not fully implemented defense-in-depth strategies

FIGURE 7

Implementing Defense in Depth Strategies

To what degree do you believe your organization has implemented Defense in Depth strategies in application security as described above?



Data: Dark Reading survey of 131 cybersecurity and IT professionals, May 2024

Shared Responsibilities in Web Application Security

The shared responsibility model, popularized by organizations like AWS and Microsoft Azure, provides a framework for how customers and security vendors should approach comprehensive application security. This concept is highly relevant for web application security, which must encompass a range of protection capabilities including malware prevention, application firewalling, bot management, and API security.

Somewhat surprisingly, the survey results revealed that only 49% of respondents indicated familiarity with the shared responsibility model. This lack of awareness could be contributing to gaps or inefficiencies in organizations' web application security postures.

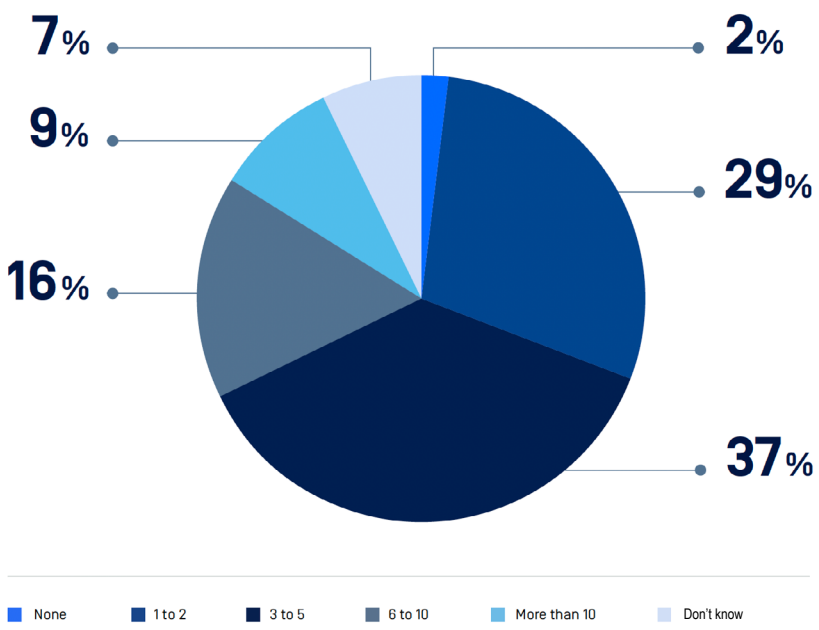
The skills gaps plaguing cybersecurity teams may also be a factor, with soft skills, cloud computing, and security controls emerging as key deficiencies according to ISACA's annual State of Cybersecurity 2023 report.

The complex vendor arrangements at many organizations can further complicate efforts to achieve robust web application security. A significant 62% of survey respondents stated that their organization works with at least three different external security vendors, and, in some cases, more than ten (Figure 8).

FIGURE 8

External Security Vendors

How many different external security vendors does your organization work with?



Data: Dark Reading survey of 131 cybersecurity and IT professionals, May 2024

The sheer number of security vendors involved is not the only complicating factor. As one IT executive respondent put it, "Complexities in internal and external systems (hardware and software), especially 3rd party systems," represent a primary challenge to effective cybersecurity. A cybersecurity executive said, "In today's world of leveraging best-of-breed solutions from multiple partners, it has become much more challenging to derive and present a comprehensive dashboard across all the tech." This sentiment was echoed by many other responses that cited complexity as a key hurdle.

The added complexity introduced by utilizing multiple security vendors can exacerbate common challenges that organizations already face, such as lacking sufficient trained staff — The ISACA report highlights that 59% of cybersecurity leaders say their teams are understaffed — or struggling to obtain leadership attention and buy-in for cybersecurity initiatives.

"In today's world of leveraging best-of-breed solutions from multiple partners, it has become much more challenging to derive and present a comprehensive dashboard across all the tech."

-CYBERSECURITY EXECUTIVE

Bringing Simplicity to Chaos

Confronting the complexities organizations face in securing their applications and data, an integrated platform approach can bring much-needed simplicity. F5 and OPSWAT have partnered to provide a comprehensive, multi-layered security solution that provides reliable end-to-end web application security.

F5 focuses on securing web applications and traffic through robust application firewalling, API security, bot management, and secure access capabilities. OPSWAT complements this by specializing in securing files as they traverse networks. Its MetaDefender platform inspects all files using proprietary technologies to detect and remove known and unknown malware threats while also safeguarding sensitive data.

By consolidating web application security, secure access, and advanced file security into a unified solution, security teams gain centralized control while eliminating the management overhead of disparate vendor prod- ucts. Additionally, F5 and OPSWAT provide consistent security policy. Learning security for AWS, Azure, Google, and On-prem is unnecessary with F5 and OPSWAT, as they support multi-cloud and hybrid cloud environments in addition to traditional on-premises deployments, ensuring consistent security policies and operations while addressing skill gap and cost challenges.

In contrast to patchworked stacks built from multiple vendors, this streamlined approach provides holistic protection against data breaches, malware, and other cyber threats targeting applications and files. The simplified administration and incident response workflows allow lean security teams to optimize their resources and enhance their overall security posture.

AI Threats

Threats constantly evolve. When asked to identify the most concerning future threat, many respondents mentioned evolving technology, specifically AI. To counter AI/ML-powered strikes, organizations require a holistic, integrated security posture. Those prioritizing unified platforms like the combined F5 and OPSWAT solution will be well-positioned to adapt. Consolidating app security, secure access, and file threat prevention into one streamlined architecture provides 360-degree resilience.

Simplicity, integration, and innovative shared responsibility practices will separate the secure from the vulnerable when facing this AI/ML-driven future.

"As someone who worries about keeping our company's applications secure, a few things really keep me up at night when I think about the future threat landscape: Artificial intelligence and machine learning are becoming more sophisticated, and that means attackers are going to be using them too. Imagine a future where attackers can automate their attacks, launching them at lightning speed and constantly evolving their tactics. We'll need to be even more vigilant and have even smarter defenses in place to keep up."

-IT MANAGER

Conclusion

Complexity of Web Application Security

The findings from the OPSWAT and F5 survey underline the pressing need for a paradigm shift in cybersecurity approaches across organizations. Despite some adherence to industry best practices, the persistent gaps in preparedness, regulatory compliance, and the integration of security measures indicate a significant struggle among cybersecurity leaders. The complexities introduced by the migration to cloud environments and the use of multiple security vendors exacerbate these challenges, making a unified, multi-layered security approach more critical than ever. Leaders are particularly hindered by budget constraints, inadequate staff training, and insufficient attention from executive leadership, contributing to an overall sense of unpreparedness for evolving cyberthreats.

To address these challenges, organizations must prioritize the adoption of comprehensive defense-in-depth strategies, integrating security at every stage of the software development lifecycle. By leveraging unified platforms like the combined F5 and OPSWAT solution, organizations can streamline their security efforts, reduce administrative overhead, and enhance their overall security posture. This holistic approach, coupled with a cultural shift towards proactive security practices and continuous improvement, is essential to fortify defenses against sophisticated threats, including those powered by AI and machine learning. Ensuring robust cybersecurity requires commitment, collaboration, and innovation to protect against the ever-evolving threat landscape.

Survey Methodology

OPSWAT commissioned a Dark Reading survey designed to better understand how organizations are addressing evolving cyberthreats and the ways in which security practices fulfill shared responsibilities relating to data protection. The survey collected responses from 131 qualified IT and cybersecurity professionals.

The survey was conducted online in May 2024. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Dark Reading's qualified database. Dark Reading was responsible for all survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

The final data set includes job titles from executive level to staff, predominantly located in North America. Twenty-six percent held IT and cybersecurity executive job titles (CIO/CTO, CSO/CISO, or VP of IT/cybersecurity). Other titles included IT head/director/manager (20%), cybersecurity head/director/manager (14%), and IT or cybersecurity staff (14%). Other titles included corporate management (8%), network/system administrator (5%), engineer (4%), and software developer (4%).

Respondents come from companies of all sizes representing more than 21 vertical industries, including technology, consulting, government, education, healthcare, manufacturing, and banking/financial services. A majority of respondents (52%) work at large companies with 1,000 or more employees; 30% at companies with 100 to 999 employees; and 18% from organizations with fewer than 100 employees.

OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, Zero-Day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com