WHITE PAPER

Web Application Security OR Network Security

DO YOU HAVE TO CHOOSE?

Netsparker

Invicti

Contents

Executive summary

In a cloud-first world, the traditional line between network security and application security is becoming blurred. Until relatively recently, IT infrastructures were dominated by hardware, and IT security was generally taken to mean network and system security. However, with many organizations moving to the cloud during the past decade, physical infrastructure can now be hidden behind layers of virtualization, and web applications are frequently designed, developed, tested, and deployed entirely in the cloud.

Established organizations often have a mature network and infrastructure security program that accounts for the majority of their IT security budget. As a relative newcomer, web application security tends to receive far less spending there. At the same time, web applications have become the main target for cybercriminals and now account for 3 out of 4 data breaches worldwide. Web application security has never been more important – and yet there is still some confusion as to its place in the overall security posture.

This white paper examines the role of web application security, shows how it differs from network and infrastructure security, and explains why any mature cybersecurity program needs both application security and network security.

Introduction:
Cybersecurity in an application-first world

Internal and external web applications are now a major part of modern business. Some of the world's largest companies started from a single web application (Facebook and Google spring to mind), and web platforms are crucial for commerce, finance, and government. Any organization that wants to reach a wide user base is going to use web applications – often hundreds if not thousands of them.

Organizations continue to shift ever more data and business logic onto cloud platforms and become reliant on web technologies to do business. In fact, **94% of enterprises** already use at least one web platform. The traditional division into private and public networks is now often logical rather than physical, and all business assets accessible from the web are now in the front line of cyberattacks.

Business and personal data is a prized commodity, so cybercriminals are following the money and focusing on web assets. Studies confirm that **3 out of 4 data breaches worldwide are now related to web applications**. Traditional perimeter defense is no longer enough to secure business data.

Modern web assets include not just websites and web applications but also countless services and APIs (Application Programming Interfaces) that are used to exchange data between systems. With the mobile revolution, web APIs and web services have become a vital backend to deliver content and functionality to millions of mobile application users.

For many users, the application is the network. We are living in an application-first world, so application security is a vital part of overall cybersecurity.

Network security:
The roots of cybersecurity

Before the era of web, cloud, and mobile, cybersecurity was mainly about systems and network security. This is the traditional, more physical approach to IT security, focused on hardware and infrastructure – servers, workstations, routers, switches, firewalls, wired and wireless connectivity, and so on. In terms of communications protocols, this covers everything below the application layer. In terms of architecture, typical network security strategies were based around perimeter defense, with a physically secured internal network that could be protected from external intrusions.

In cloud computing and virtualized environments, network security is also virtualized but still exists and still covers everything below the application layer. Routers, switches, interconnects, firewalls – all these components can be partly or completely software-defined. While this can complicate the security architecture, the aim remains the same: to secure connections and systems. Network security tools are not designed to check application traffic, so they have limited effectiveness for web application security, where attackers usually send malicious payloads within legitimate HTTP traffic.

What are CVEs:

Finding known vulnerabilities

Common Vulnerabilities and Exposures, or CVEs, are publicly known hardware and software security vulnerabilities listed and classified at **https://cve.mitre.org/**. Every vulnerability in a specific product that is discovered and disclosed receives a CVE number. Network and systems security scanners focus on finding targets with vulnerabilities corresponding to known CVEs, such as outdated software versions or unpatched device firmware.

Examples:
CVE-2017-5715 (Spectre),
CVE-2014-0160 (Heartbleed)

The goal of network security is to secure access to devices, systems, and services. This starts with preparing an inventory of hardware and software assets to be secured, followed by a scan to find known vulnerabilities identified by CVE numbers. Armed with scan results and security best practices, security professionals can patch identified vulnerabilities and lock down services to ensure that no known security flaws remain in the network. Once set up and configured, network environments change relatively slowly, so network security focuses on patching and maintenance rather than finding new vulnerabilities.

Network security also means maintaining a solid defense that involves physical and software-based firewalls, intrusion prevention systems (IPS), and similar solutions. To ensure effective security, these must be deployed in the right locations within the network and configured with suitable rules to block intrusions while allowing legitimate traffic. The perimeter defense approach goes back to the pre-cloud days when users and business systems were restricted to a secure internal network and all communication with the Internet could be filtered and gated.

Vulnerability Scanning and Resolution in Network Security

1. Use a network scanner to discover hardware and software assets.
2. List identified devices, systems, and exposed ports and services.
3. Check assets for known vulnerabilities (CVEs), configuration errors, out-of-date releases, policy compliance etc.
4. List scan results for verification.
5. Engineers fix, update or patch vulnerable assets.

Understanding web application security

With the advent of cloud computing, whole application environments could be built using web technologies and operate entirely using HTTP(S) traffic on default ports. Anything going on within this traffic was beyond the scope of traditional network scanning tools. As web applications gained traction, more and more organizations started moving their business and data into the cloud. Cybercriminals were quick to follow and web application security became a major global concern.

The vast majority of IT security staff are familiar with network and systems security because that has been around for a long time. However, web application security is often less well understood, even though it requires a very different approach. Administrators with a network security background might scan web application environments with a network scanner to find and patch vulnerable servers, frameworks, and libraries. While this is definitely good practice, it is just the starting point for securing a web application, since there is no way of checking if the application code itself is secure. What's more, even if all the known components are up to date, they may still contain unreported vulnerabilities.

Modern web applications are not monoliths but rather patchworks made up of many products and technologies. Development usually starts with choosing a web application framework that provides the design backbone and takes care of vital but mundane tasks such as rendering the user interface or ensuring cross-browser support. Developers then work within the framework to code the application logic, bringing in external libraries (often open-source) to provide specific features. Coupled with other external resources such as styles, fonts, and icons, the resulting web application is a complex network of dependencies. Each external component can have its own development history and its own vulnerabilities, making security testing a complicated task.

What are CWEs:

Finding new vulnerabilities

Common Weakness Enumerations, or CWEs, make up a community-developed list of common software and hardware security weaknesses stored at **https://cwe.mitre.org/**. Unlike CVEs, they do not correspond to vulnerabilities in specific products but describe more general weaknesses that may lead to vulnerabilities. Web vulnerability scanners focus on finding new vulnerabilities that correspond to common CWEs.

Web application security is based on finding and fixing new vulnerabilities that correspond to known weaknesses, or CWEs. While checking for CVEs is also important, especially for popular web applications that make attractive targets, it is relatively easy to identify and patch vulnerable versions. The main value of a dedicated web application security scanner lies in accurately identifying new vulnerabilities.

Web application environments tend to be highly dynamic. Rapid development and deployment is the norm, made possible by the widespread use of ready frameworks and libraries. Even in the largest applications with millions of users, new and updated code can be committed into production environments on a daily basis. Web technologies evolve quickly and last year's security tools might no longer be enough for today's web. What's more, the web threat landscape changes rapidly and it takes dedicated specialists to keep up with the latest developments. All this means that even if a web application was tested and secured last year or last month, changes in the application, underlying libraries or attack techniques may make it vulnerable again.

In traditional IT security, the local network was treated as safe and secured home base, while the Internet was a dangerous minefield accessed only with the greatest care. Well, this minefield is where web applications live and web security professionals work. Unlike an internal system, every publicly accessible web application can potentially be attacked at any time and from anywhere in the world. Modern web applications make lucrative targets for cybercriminals, especially if they can yield confidential data. Worse still, the barrier to entry for cybercrime is extremely low – anyone with an Internet connection and a ready-made set of attack scripts can attack web applications.

Common web application security flaws

- **CWE-89** SQL Injection: User-controlled input (such as a query parameter or form field text) is inserted directly into an SQL query sent to a database without validation. Attackers can inject SQL instructions to extract data or modify database content.

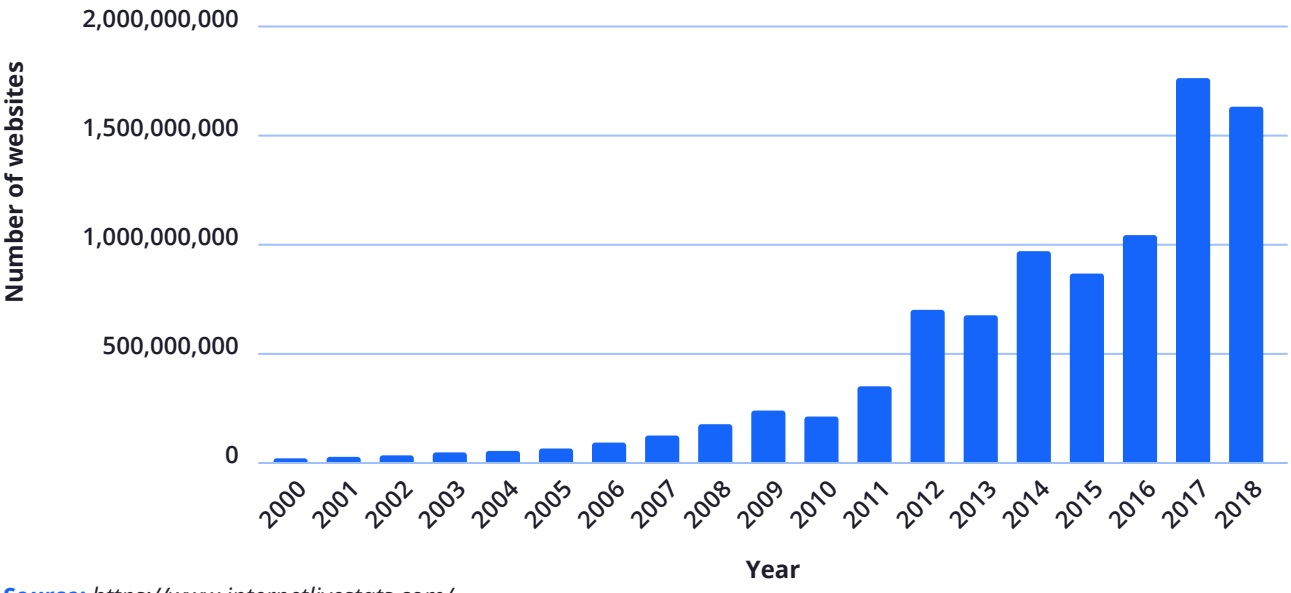
- **CWE-79** Cross-Site Scripting (XSS): Unvalidated user input is included in web page content. Attackers can inject JavaScript code to modify page content, hijack user sessions or redirect users to a malicious site.

- **CWE-611** XML External Entity (XXE) Injection: A weakly-configured XML parser is used that allows external entities in legacy document type definitions (DTDs). By supplying a specially-crafted XML document, attackers may be able to crash the server, access local files or execute code on an internal machine to perform further attacks.

As with network security, securing web applications started with manual testing. This worked well enough when websites and web applications were relatively few and far between, but the last decade has seen explosive growth in the number of websites. The web has gone from 50 million sites in 2005 to over 1.7 billion (and growing) in 2020. With the help of ready-made frameworks, libraries, templates, and content management systems, organizations world-wide are setting up hundreds of new sites every day.

> **The web has gone from 50 million sites in 2005 to over 1.7 billion (and growing) in 2020.**

Total number of websites



Source: *https://www.internetlivestats.com/*

To complicate the picture even further, the modern web is far more than just user-accessible websites and web applications. **Web traffic data from Akamai** shows that over 80% of all web traffic is related to web APIs (Application Programming Interfaces) used to exchange data between systems. With the rise of mobile, web APIs have become a vital backend to deliver content and functionality to millions of mobile application users. Adding web services into the mix, the total number of web assets becomes astronomical – and a large organization can have thousands of such assets, each with potential vulnerabilities. At that kind of scale, automated scanning is now the only practical approach to finding and eliminating vulnerabilities.

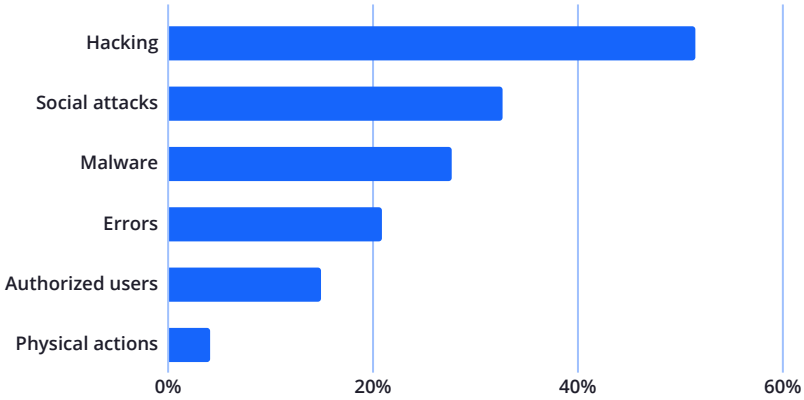
Current attack and risk trends

Cyberattacks and related risks are a leading global concern. In the **World Economic Forum's 2018 report**, cyberattacks are considered the most likely man-made threat. A year later, 79% of organizations **surveyed by Marsh** listed cyberattacks as one of the top 5 business risks overall, and 22% the #1 business risk. At the same time, confidence in the effectiveness of existing cybersecurity measures is slipping, with the proportion of organizations responding "Not at all confident" for their ability to understand, assess, and measure increasing from 9% in 2017 to 18% in 2019.

Among cyberattacks, data breaches are a major risk, as they can be extremely costly and have widespread consequences for organizations. **Verizon's 2019 Data Breach Investigations Report** makes for sobering reading. For example, in 2019, 2 out of 3 data breaches that involved an external hacking attack were related to web applications. Drilling down into the results, in some categories, as many as 3 out of 4 incidents involved web applications.

> **In 2019, 2 out of 3 data breaches that involved an external hacking attack were related to web applications.**

Origins of data breaches in 2019



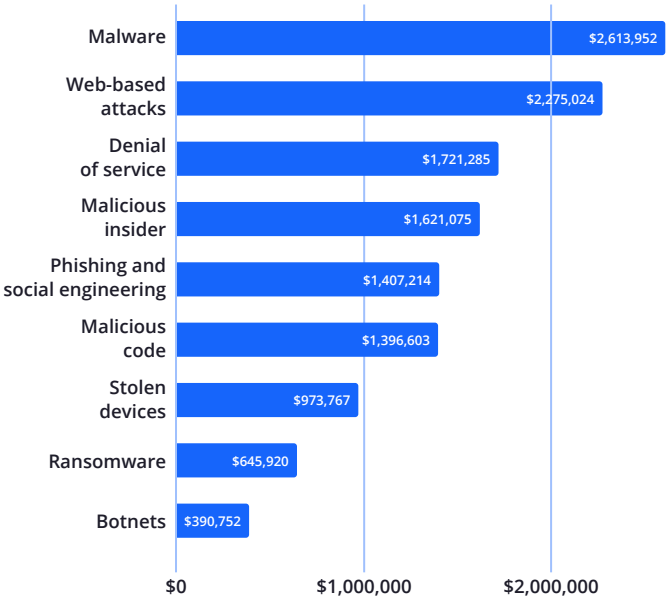
Source: *Verizon 2019 Data Breach Investigations Report*

The costs of cyberattacks

Cybersecurity is considered the biggest risk area for the global economy. Every year, studies confirm that the global cost of cyberattacks is enormous, with **some analysts putting the value at $1 trillion a year**. According to Accenture, **cybercrime cost the average organization $13 million in 2018** – a rise of 72% since 2013. Breaking this figure down, malware and web-based attacks are by far the most costly areas, together accounting for nearly $5 million of the total sum.

The same study found that by far the biggest contributor to the cost of a cyberattack is the cost of information loss, which in 2018 accounted for $5.9 million of the $13.0 million total cost per organization. Along with the cost of business disruption at $4.0 million, this makes up over 75% of the total financial cost of cybercrime.

Average cost of cybercrime for an organization in 2018



The consequences of a successful cyberattack can be long-reaching and go far beyond financial losses. Business disruption in the wake of a cyberattack can leave staff without the tools they need for everyday work. Existing orders can be lost due to downtime, while news of a cyberattack may cause some customers to take their business elsewhere. If personal data was leaked in the attack, this could mean regulatory liability, leading to fines, legal proceedings, and other problems. In the worst case scenario, a cyberattack can even threaten business continuity.

Risk factors

Organizations worldwide continue moving to the cloud, with **94% of enterprises** already using at least one cloud service. Analysts predict that **by 2025, cloud products will make up more than 50% of the software market**. By 2032, this figure may exceed 90%. In effect, all applications will be web applications or rely heavily on web technologies.

With the shift towards the cloud, web security has become a vital area of cybersecurity. As organizations move to cloud technology platforms, they also bring their data and business processes into web-based infrastructures. Valuable and confidential information, from industrial secrets and financial details to personal data, can now be accessed from anywhere in the world, often protected by nothing more than a login screen. As the financial, political, and business value of data continues to grow, web application security is becoming the first line of defense for organizations of all sizes, from small and medium businesses to enterprises and government institutions.

“ Valuable and confidential information, from industrial secrets and financial details to personal data, can now be accessed from anywhere in the world, often protected by nothing more than a login screen.

Facing the growing intensity and sophistication of cyberattacks are web security teams that are often underfunded and short of staff. In fact, in an **ESG survey from 2019**, 53% of organizations reported a problematic shortage of cybersecurity skills, with the issue becoming more pressing each year. The cybersecurity talent gap adds an additional risk factor to a wider issue facing organizations that need to secure their websites at scale.

While automated vulnerability scanning can help organizations to detect more vulnerabilities, the big challenge is actually resolving all the security issues that are found. Without a coordinated and fully integrated web application security process, security teams simply have no realistic way of fixing every single vulnerability across hundreds of websites, especially if they also have to manually weed out false positives from the scan results. This often means that only a handful of critical applications can be kept secure, while vulnerabilities in other assets are only fixed after many weeks or not fixed at all. In effect, it is outdated workflows that pose the biggest risk to enterprise web security.

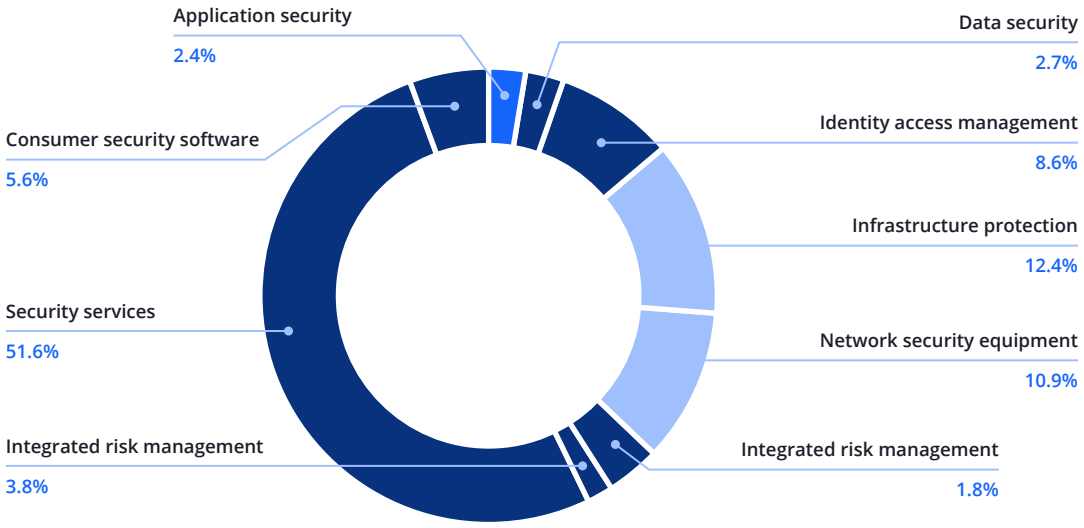
Current spending trends and technological maturity

Spending trends

Large, established organizations have mature IT security programs and many years or even decades of experience in network and systems security. Unsurprisingly, this is reflected in their cybersecurity budgets, with a large part of the money going on maintaining and upgrading existing devices, tools, and infrastructure. **According to Gartner**, worldwide security spending in 2018 exceeded $114 billion. Over $26 billion went on network security equipment and infrastructure protection, accounting for some 23% of the total spending. During the same period, just $2.7 billion, or 2.4% of the total, was spent on application security.

Gartner's report is a very high-level overview, so the categories used are too general to make detailed comparisons. For example, the security services category probably includes services from all areas of IT security, including web application security testing. However, the overall picture is all too clear: despite accounting for a clear majority of data breaches and cyberattacks, web application security is still not a high priority in IT security budgets. So why is that?

IT security spending in 2018



Source: *Gartner forecasts on worldwide information security spending (August 2018)*

One explanation is that organizations spend money on what they know and understand best. Being a relative newcomer to the IT security mix, web application security is frequently overlooked or underfunded, even though cyberattacks mostly target web applications and this is where most data breaches happen. Organizations might have large and experienced teams of network and systems security staff but just one small team tasked with securing business web applications on a limited budget. The good news for overworked security teams is that application security spending is growing and, according to **Forrester's global forecast for 2017–2023**, is expected to reach $7.1 billion by 2023, with double-digit annual growth.

Technological maturity

Network security has been around for several decades and is a mature and developed field, with established players in each segment offering comparable hardware and software products. For customers, this means that choosing a solution is often more a matter of price and compatibility with existing investments than of features or effectiveness.enterprises and government institutions.

In the field of web application security, the market is much younger and more fragmented. To start with, some network security vendors include web vulnerability scanning features in their network scanning solutions. There are also a handful of dedicated web application security vendors, including Invicti Security, the company behind industry-leading dynamic and interactive application security testing (DAST+IAST) solutions, Acunetix and Netsparker, as one of the pioneers and leaders of this industry with over a decade of experience. Unlike the more mature network security space, the scope and effectiveness of different products can vary significantly, making it harder for customers to choose a solution that's right for them.

> **To address web vulnerabilities at scale, you need specialized solutions that go beyond just scanning.**

As already discussed, securing a web application is a complex and multi-dimensional process. The vital requirements here are accuracy (to find vulnerabilities) and effectiveness (to address them). While a number of web application scanners exist, to actually address vulnerabilities at scale, you need specialized solutions, such as Acunetix or Netsparker, that go beyond just scanning. For example, Netsparker's unique value proposition is based on its laser-accurate Proof-Based Scanning™ technology that identifies and automatically verifies vulnerabilities. Thanks to extensive two-way integration with ticketing systems, confirmed vulnerabilities can go straight to the developers who fix them.

Why network security alone is not enough

Network security and web application security are two separate and complementary pieces of the cybersecurity puzzle. Each relates to different technologies and has to deal with different threats. To keep secure in the connected modern world, organizations need to maintain a solid cybersecurity posture in both areas, especially as the majority of cyberattacks and data breaches are related to web applications.

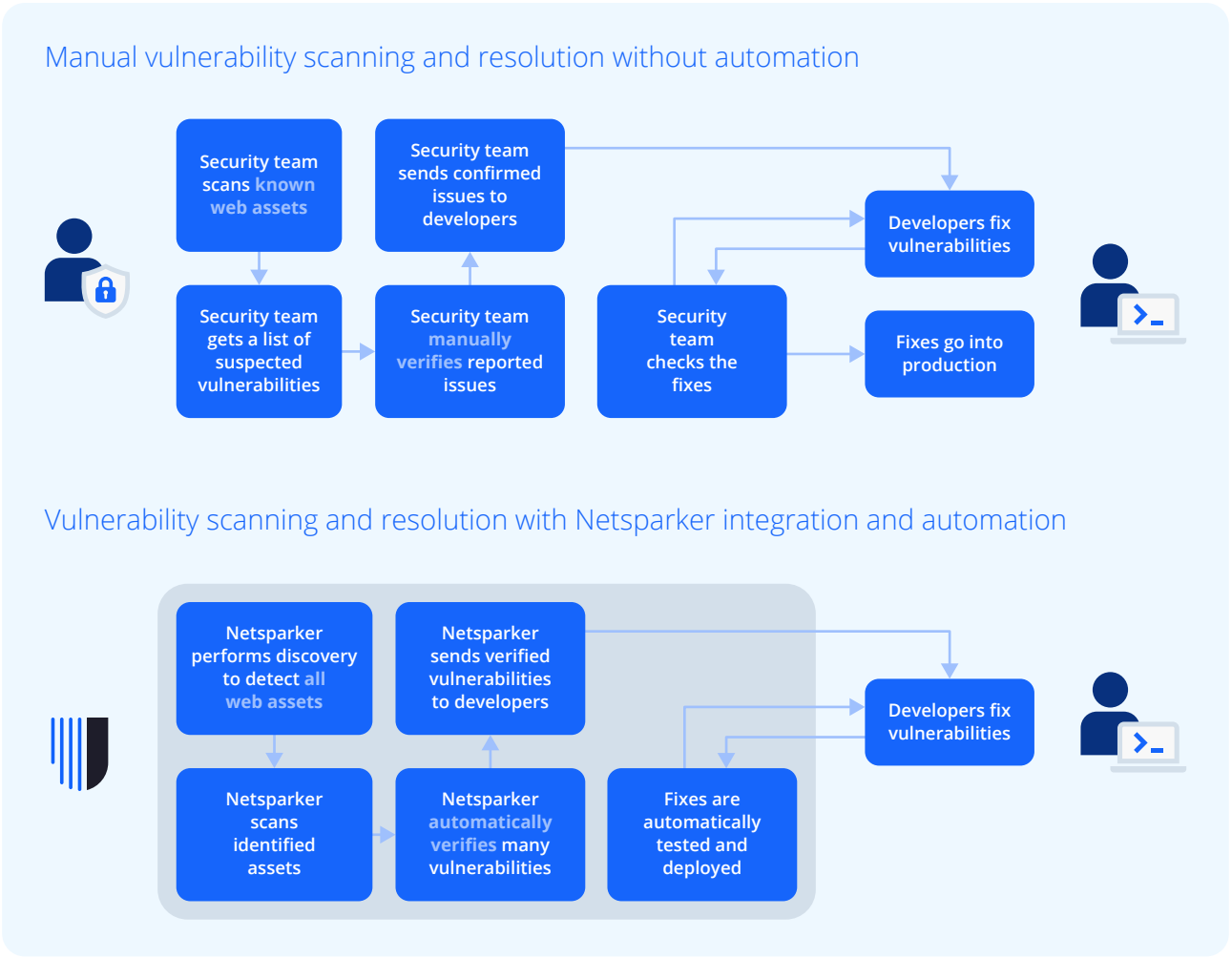
Established companies with mature cybersecurity programs centered around network and systems security might need to add web application security scanning into the mix. In the past, when most organizations had just a handful of websites, manual vulnerability testing may have been sufficient. Faced with the challenge of securing hundreds of assets, organizations can no longer afford to rely just on manual testing. Some look to their existing network security tools for a solution and while many network security products do offer web application scanning features, ensuring web application security goes far beyond just running an additional scan. In a large organization, a vulnerability scan can return several thousand results. So what's next?

To work at scale, web application security requires dedicated and accurate tools based on years of web security expertise, combined with deep integration to ensure that vulnerabilities are fixed, not just found. When dealing with hundreds or thousands of web assets, automation also becomes a necessity – and to automate, you must be confident that your scan results are not false positives. This is where you need one of Invicti's dedicated solutions like Netsparker with its proprietary Proof-Based Scanning™ technology to ensure that only verified issues are passed to developers to fix.

Unlike older organizations, many companies founded in the past decade rely mostly or exclusively on web technologies to do business. This is especially true for application-first companies built around a single web

application. With the central product and often also supporting business applications running entirely on cloud platforms, network security is delegated to the cloud infrastructure provider. For these organizations, IT security is all about securing business-critical web assets, including websites, applications, services, and APIs. And when the safety of your data and your entire business hinges on web application security, having specialized, accurate, and trustworthy tools is a must.

> **Scanning is just the first step in securing web applications.**



Moving application development to the cloud has removed much of the complexity from development workflows, allowing distributed teams to collaborate effectively on fast-moving projects. In agile approaches such as CI/CD, new code might even be deployed daily. However, each change to a web application can potentially introduce a vulnerability, so with frequent modifications, manual checks are not enough – and are not scalable. Integrated and automated security testing is vital for secure web application development. If you add to that the fast-changing cyberthreat landscape, only specialist tools backed by years of web security expertise can provide the accuracy and confidence necessary to truly automate the process.

Summary

As organizations continue the move to the cloud and web applications, the weight of cybersecurity is also shifting towards web security. A wealth of valuable data is now accessible to staff and consumers via web browsers and mobile applications – but cybercriminals, nation-state actors, and unscrupulous business rivals are also targeting it. Web applications and interfaces are in the first line of cyberattacks, so they must be well secured.

At the same time, even mature organizations with decades of experience and investment in network and systems security often overlook or underestimate the importance of web application security as a separate field. In a large organization, there can be thousands of web assets spread across multiple systems and geographies. At this scale, keeping them all secure is only possible with dedicated web application security solutions that deliver accurate and actionable results.

Maintaining a solid security posture in a cloud-based world requires the right tools and processes in all areas of IT security. Network and systems security is still an essential part of any comprehensive security program, but here and now, the front line of the battle against cybercrime has firmly moved towards web security. With so much at stake if a cyberattack succeeds, organizations cannot afford to leave any gaps.

Quite simply, if you have web applications, you need web application security.

Invicti

ABOUT INVICTI SECURITY

Invicti Security is changing the way web applications are secured. A global leader in web application security for more than 15 years, Invicti's dynamic and interactive application security products help organizations in every industry scale their overall security operations, make the best use of their security resources, and engage developers in helping to improve their overall security posture. Invicti's product **Netsparker** delivers industry-leading enterprise web application security, while **Acunetix** is designed for small and medium-sized companies.

Netsparker

ABOUT NETSPARKER

Scalable tech is fundamental for enterprises. Established by security expert Ferruh Mavituna in 2009, Netsparker can scan thousands of websites and web apps then prioritize and verify vulnerabilities with proprietary Proof-Based Scanning technology.