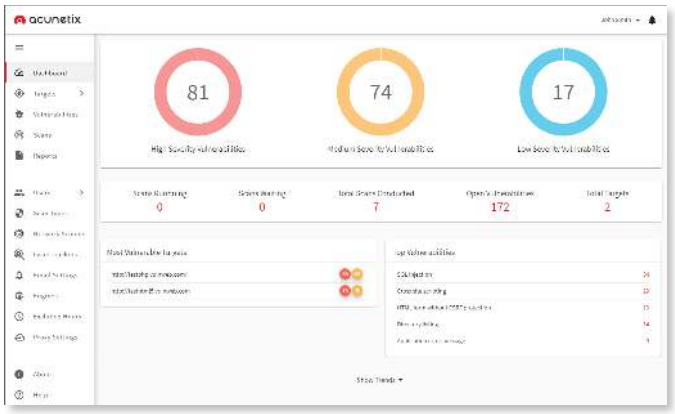
acunetix

All-in-One

Web Application Security Scanner

As the first company to build a fully dedicated and fully automated web vulnerability scanner, Acunetix carries unparalleled experience in the field and offers a trustworthy all-in-one solution for all your web application security needs.



Acunetix specializes in delivering leading-edge speed and accuracy when it comes to web application security thanks to its unique features, built into the product, so the process of securing your assets falls into the following three steps: **FIND. FIX. PREVENT.**

End–to–end web security for your organization: FIND. FIX. PREVENT.

1 FIND

- All web vulnerabilities
- All network vulnerabilities
- All web malware

2 FIX

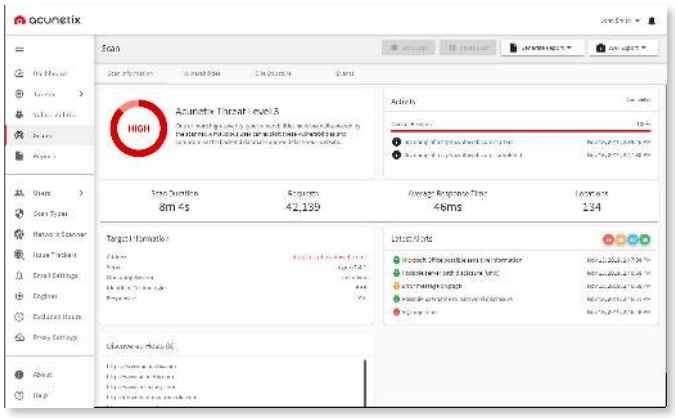
- Get detailed reports for developers
- Track progress internally and externally
- Confirm resolution

3 PREVENT

- Integrate into the SDLC
- Export to WAFs
- Prevent vulnerabilities from ever making it to production

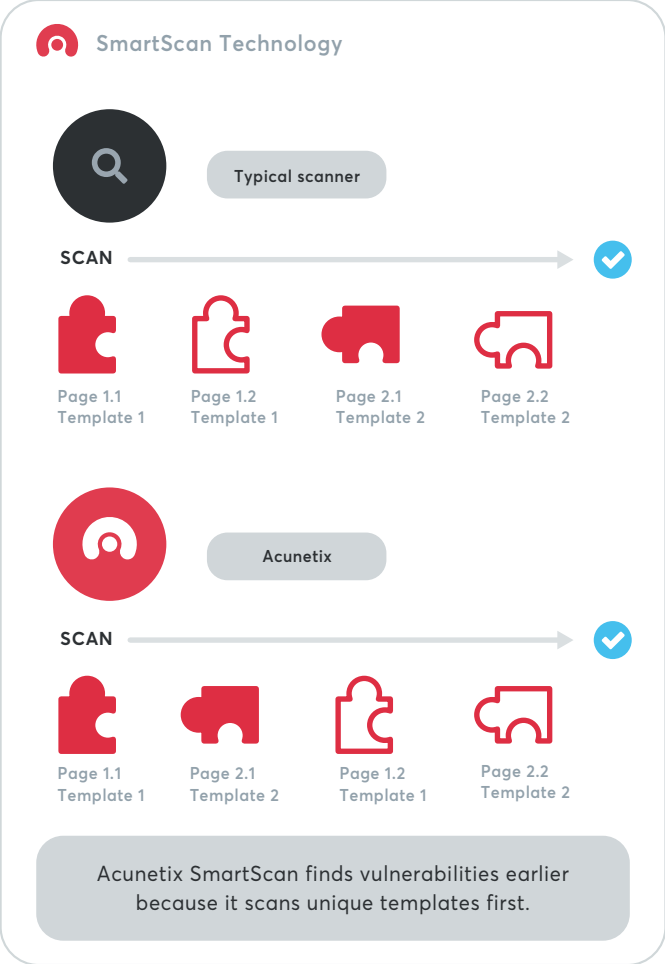
Fastest scanning engine

The Acunetix engine is written in C++. This makes it work much faster than scanners written in high-level languages. Scans use a minimum number of requests. This reduces network and server load and speeds up testing. Acunetix focuses on performance. With every version, we introduce new performance-related features.



SmartScan technology

Many websites and web applications have a lot of pages/interfaces that are based on the same or similar templates. The same templates usually mean the same potential vulnerabilities. Acunetix scans unique pages and interfaces first to give you 80% vulnerabilities in the first 20% of the scan.

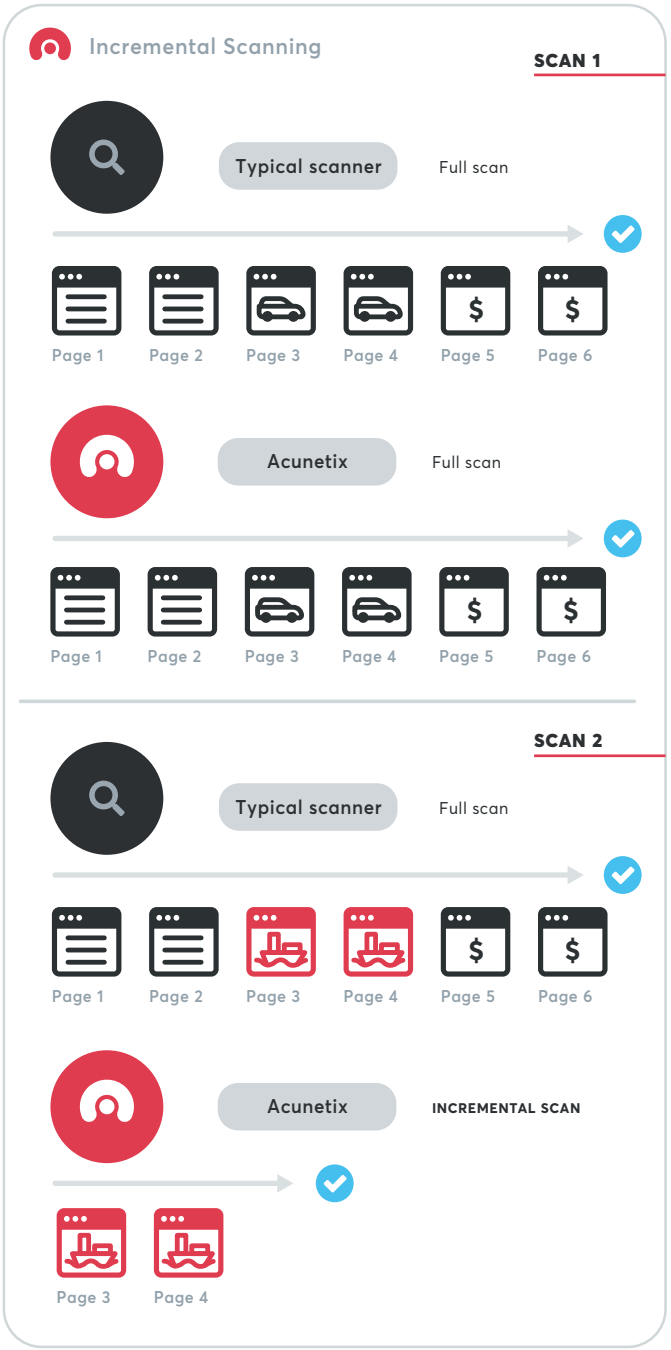


DeepScan technology

Modern web applications are written using complex HTML5 and JavaScript. The DeepScan technology based on the Chromium engine lets Acunetix crawl such pages more effectively than other scanners. DeepScan can automatically discover the most popular JavaScript frameworks: Angular, Vue, and React and adjust the crawl to their specific structures. DeepScan works together with the Acunetix Login Sequence Recorder to crawl even password-protected areas.

Incremental scanning

After the first full scan, you can configure Acunetix to scan only parts of the website or web application that have changed since the last scan. Incremental scanning can reduce scan times by more than 90%. It is especially useful in CI/CD pipelines. To maintain full security, you can perform full scans less frequently with frequent incremental scans in-between.



End-to-end web security for your organization

Minimum false positives

Acunetix attempts to exploit potential vulnerabilities and indicates the confidence level, so you know whether a vulnerability may require further penetration testing. For critical vulnerabilities, Acunetix provides proof-of-exploit. For example, it may display information that should not be accessible from the outside proving that the vulnerability exists.

Acunetix uses the AcuMonitor technology to fully confirm out-of-band vulnerabilities and the AcuSensor technology to obtain additional back-end information that helps to confirm more vulnerabilities.

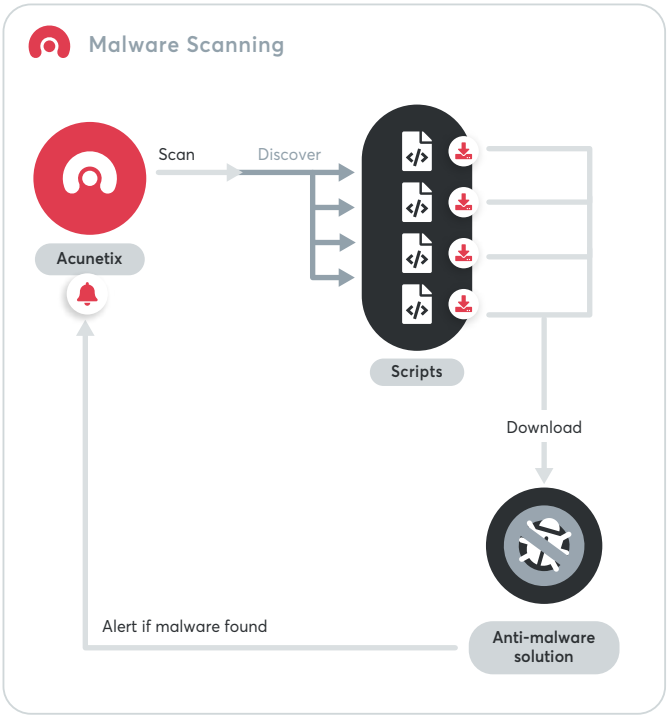
Network scanning

Acunetix is integrated with the market-leading OpenVAS network scanner and able to detect more than 50,000 network vulnerabilities. Network scan results and web scans results are managed together using the same interface, the same functions, and the same integrations.

Acunetix network scanning is available both in the cloud and on-premise so you can scan both your internal and external resources.

Malware detection

Acunetix uses safe browsing databases from Google and Yandex to identify malicious links. On Windows, Acunetix uses Windows Defender to scan all downloaded scripts for malware. On Linux, Acunetix uses ClamAV to scan all downloaded scripts.



Assess vulnerabilities

Acunetix automatically assesses all vulnerabilities based on their potential impact. When assessing, Acunetix automatically considers the configured importance of the scanned asset. You can improve the security of your web applications by using Continuous Scanning to frequently scan for high-threat vulnerabilities only.

*Discover up to **80% of vulnerabilities** in the first 20% of the scan thanks to unique scanning algorithms*

Manage vulnerabilities

Acunetix has built-in vulnerability management functionality where you can assign remediation to users and monitor remediation status, including automatic confirmation scans. You can use your current issue tracker with Acunetix. Acunetix will create issues according to your configuration.

Acunetix manages network and web vulnerabilities together, both using its own interface and external trackers.

Integrate in the SDLC

You can integrate Acunetix with your CI/CD tool to include web and network vulnerability scans in pipelines. Acunetix can automatically assign discovered vulnerabilities to the right teams using your current issue tracking software.

If you need a custom integration, you can use the Acunetix API. For enterprise customers, Acunetix can help develop custom integration solutions.

Work with other tools

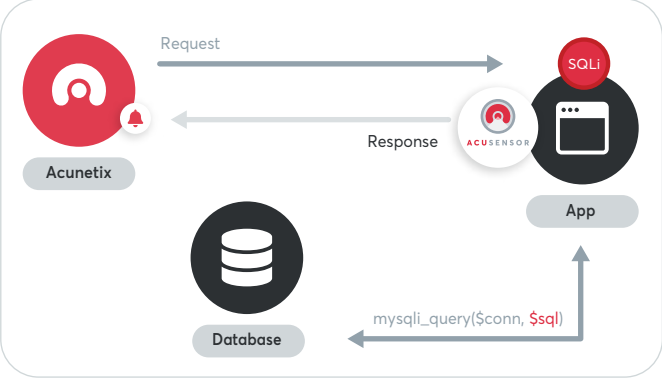
You can import data into Acunetix from many applications and formats, including Selenium, Telerik Fiddler, Postman, Burp, Swagger 2.0 and 3.0, WADL, WSDL, and more. You can export Acunetix scan results as web application firewall (WAF) rules for Imperva SecureSphere, F5 BIG-IP Application Security Manager, and Fortinet FortiWeb. All Acunetix capabilities are available using a RESTful API.

Out-of-band scanning

Unlike most competing products, Acunetix can discover dangerous out-of-band (blind) vulnerabilities by using unique AcuMonitor technology. AcuMonitor technology proves the existence of out-of-band vulnerabilities by receiving data from test payloads. AcuMonitor is completely safe to use and automatically activated for specific vulnerability checks.

Interactive scanning

Acunetix can be configured to become an Interactive Application Security Testing (IAST) scanner. This is achieved using the AcuSensor technology. AcuSensor is an optional component for PHP, Java, and ASP.NET that you install on the server and that communicates with the interpreter/compiler. AcuSensor can help you pinpoint the exact location of vulnerability in source code or byte code, greatly speeding up remediation.



Extensive reporting

Acunetix creates detailed developer reports with additional links that explain how to remediate the vulnerability. Acunetix creates management and executive reports and shows current trends. You can evaluate your PCI DSS, HIPAA, and ISO 27001 compliance with specially tailored reports.

Available on Windows, Linux, and online

Acunetix is available on Windows and in the cloud, and it is the only business-class scanner available also on Linux.

GET A DEMO AT **WWW.ACUNETIX.COM**

Customer testimonials

"Acunetix has played a very important role in the identification and mitigation of web application vulnerabilities. Acunetix has proven itself and is worth the cost. Thank you Acunetix team."

U.S. AIR FORCE

M. Rodgersk
US Air Force

"With Acunetix WVS we were able to perform our tasks better, thus improving the quality, stability and security of Joomla! We would like to thank Acunetix for supporting the Joomla! project and giving us the opportunity to use its tool. Thank you Acunetix team."

Joomla!™

Robin Muilwijk
Joomla!

Acunetix clients

Coca-Cola · American Express · HSBC · Honda The Power of Dreams · National Geographic · Ryanair · L'Oréal · NASA · National Security Agency · Lufthansa · Virgin · Expedia · easyJet · adidas · pwc

acunetix

WHERE TO FIND US

Stay up to date with the latest web security news.

Website. **www.acunetix.com**

Acunetix Web Security Blog. **www.acunetix.com/blog**

Facebook. **www.facebook.com/acunetix**

Twitter. **twitter.com/acunetix**

CONTACT INFORMATION

Acunetix (Europe and ROW)
Tel. +44 (0) 330 202 0190
Fax. +44 (0) 330 202 0191
Email. sales@acunetix.com

Acunetix (USA)
Tel. +1 737 2418773
Fax. +1 737 6008810
Email. salesusa@acunetix.com