WithSecure™ Elements Vulnerability Management

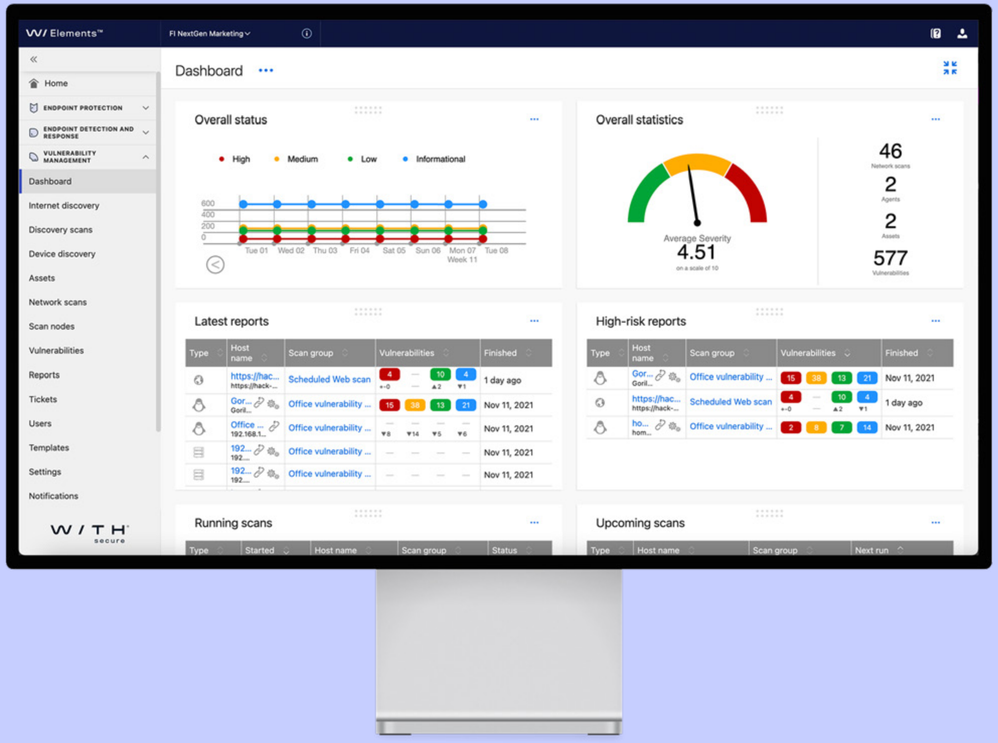
Know your attack surface to reduce risk.
Fix vulnerabilities with an end-to-end solution
designed for dynamic IT environments.

W / T H
secure

Expanding IT environments are more challenging to protect and need more emphasis on predictive cyber security measures. With automated scanning and continuous remediation of vulnerabilities you can minimize risks and tackle threats before they occur. With risk-based prioritization your efforts will have the biggest impact, and your productivity will soar.

As evident as the business benefits are, new solutions come with security drawbacks. Dynamic and complex IT environments lead to broad attack surfaces with more security challenges and vulnerabilities. Attackers are constantly looking for opportunities to exploit unpatched and flawed systems for unauthorized access to valuable data. They search for vulnerabilities for one simple reason - because it works. The more devices, systems and applications in the environment are left vulnerable, the more opportunities there are for the attacker. One loophole is enough.

Out of sight, out of mind is not the best play when it comes to cyber security. You want to know what it is that you are protecting, and how to make it more secure. Your attack surface is a living organism where new vulnerabilities emerge every day. Scanning for vulnerabilities every now and then is better than nothing - but it is not enough. By taking programmatic predictive and preventive measures you can considerably improve your odds of weathering cyber threats.



Say goodbye to flying blind and reduce your attack surface.

Strengthening your cyber security starts with knowing your assets and where they are vulnerable

Vulnerability management means proactively closing security gaps before attackers exploit them. It's a continuous process of discovering and monitoring your assets. It includes identifying, categorizing, prioritizing and remediating vulnerabilities in your operating systems, as well as software and applications in your IT environment. It's a vital element in any organization's cyber security strategy and in ensuring a healthy security posture by lowering the odds that cybercriminals will breach your systems.

Effective vulnerability management evolves with changing environments while remaining systematic. It is prioritized based on your level of risk and your business goals. Regular network and vulnerability scanning ensures that you will get the most out of your efforts. Continuous and cyclical vulnerability management helps you gain and maintain a thorough understanding of your environment, its new devices, services, and trends, and whether vulnerabilities have been acted on appropriately.

Gain situational awareness and get regular updates on your security status

WithSecure™ Elements Vulnerability Management identifies your organization's assets, pinpoints exactly where they are vulnerable, and determines where the most critical loopholes are. Instead of driving blind you can:

- Identify all hosts in your network range
- Scan your assets for open ports
- Detect current software and operating system versions
- Find vulnerable software versions by comparing your installed versions to a database of known vulnerabilities
- Identify configuration flaws
- Scan and thoroughly check target assets
- Leverage automated scans
- Respond fast to your biggest threats with risk-based prioritization.

Why WithSecure™ Elements Vulnerability Management?

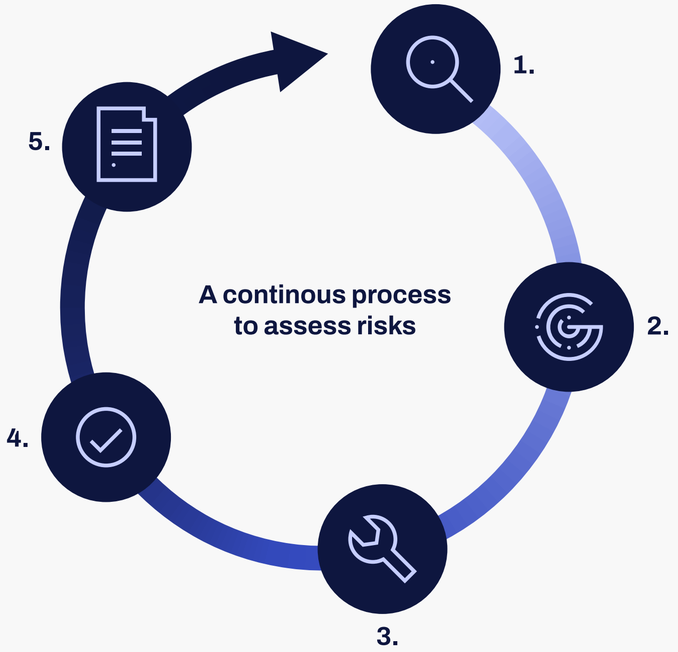
Know what you are protecting
Good security requires you to know what exactly it is you are securing.

Continuous visibility
Effective security mapping through precise discovery and mapping of all assets, systems, and applications on the network and beyond.

Find loopholes
Minimize your attack surface by fixing vulnerabilities before they are exploited

Predict risk
Know where your high-risk assets are and prioritize them.

Find your internal and external weak points before anyone else does with consistent and systematic operations.



Effective vulnerability management is a continuous process

There is a widespread but false belief that vulnerability management is cumbersome and extremely resource intensive. It does require a certain level of commitment and consistent effort when done well, but it is easier than you might think.

We have split the vulnerability management process into five straightforward steps. With this framework you can effectively stay in the know about your IT environment, understand its assets and vulnerabilities, fix the found vulnerabilities, track your progress and document the whole thing.

1. **Discover** all network assets
2. **Scan** assets and applications for vulnerabilities
3. **Remediate** effectively via a managed process
4. **Validate** that corrective actions were completed
5. **Document** all corrective actions taken for auditing

Benefits

- **Minimize risk**
  Predict and prevent threats stemming from your security architecture.
- **Prioritize for productivity**
  Focus on high-risk vulnerabilities instead of constant firefighting.
- **Streamline workflows**
  Build efficient management processes. Automate and reduce manual touch points.
- **Cost-efficient without compromises**
  Gain continuous visibility with unlimited vulnerability scans and scan nodes. The cost of predictive measures is extremely low compared to remediation costs or the cost of a breach.
- **Comply with regulations**
  Remain compliant with current and future regulations by performing regular vulnerability assessments.

1. Discover network assets

Collect information about your internet-facing systems and map your internal devices.

At first, you start by getting to know your environment. In practice, you map your internet-facing assets with Internet Discovery Scan and your internal assets with Discovery Scan. By doing this you can keep up with a modern and constantly changing IT environment and discover any unknown or forgotten assets (Shadow IT) with potentially missing security patches that pose a risk to your security posture. This first step is fairly simple, but important to the workflow, as it will help you fix flaws in your true attack surface at later stages in the process.

2. Scan assets and applications for vulnerabilities

Once you have mapped all assets in the network, you can scan them for vulnerabilities.

You can scan Windows computers with **agent-based scanning** for detailed vulnerability information including:

- List of installed software
- Vulnerable software versions
- And vulnerable OS versions

For a broader scan, you can use **System Scan** to scan all systems with an IP address in your network for:

- Open ports
- Known vulnerabilities
- Default passwords
- And misconfigurations.

For an in-depth investigation, you have **Authenticated Scan** that lets you remotely log into systems to gather more detailed and accurate vulnerability data.

With **Web Scan** you can find vulnerabilities in custom web applications. The same applies to custom modules on common platforms like WordPress.

3. Prioritize found vulnerabilities by risk level and remediate them

The solution scores found vulnerabilities based on risk and criticality. This enables prioritized workflows with emphasis on vulnerabilities with the greatest business impact and enables you and your team to spend your time on the most critical ones. You can assign and manage vulnerabilities with a built-in ticketing system.

4. Validate corrective actions

You can verify if vulnerabilities have been remediated with the built-in ticketing system. Rescanning a target will automatically indicate in ticketing if remediation was done.

The solution automatically documents any corrective actions taken for auditing.

5. Document corrective actions with standard and customized reports

With our built-in reporting tool, you can create customized reports that suit the needs of your manager, system administrator, or 3rd party service provider. You can easily report compliance with regulations and justify your value in risk management.

Reporting can be customized with tagging, target scan and in many other ways.

Next step: repeat. Continuously assessing your network and assets for potential vulnerabilities keeps you on top of your attack surface and minimizes loopholes for attackers.

Drive an efficient vulnerability management process with:

Risk-based assessment and prioritization
Prioritizing vulnerability remediation can be hard based on traditional metrics such as CVSS score alone.

By merging contextual information about the asset and its importance, such as how it's being used, with broad information about the vulnerability, you can understand the real risk behind identified vulnerabilities. This helps you make prioritized shortlists of the most urgent security issues. You can make informed decisions, optimize time spend and maintain healthy overall risk-levels and steady security hygiene.

Intuitive dashboards
Get the big picture at a glance from comprehensive visualizations. Easily create and edit widgets to fit your information needs.

Built-in ticketing system
Integrate to your existing IT ticketing system to reduce manual touchpoints.

Clear reports
Communicate risks, current status and what has been done to the right stakeholders with ready-made and custom reports.

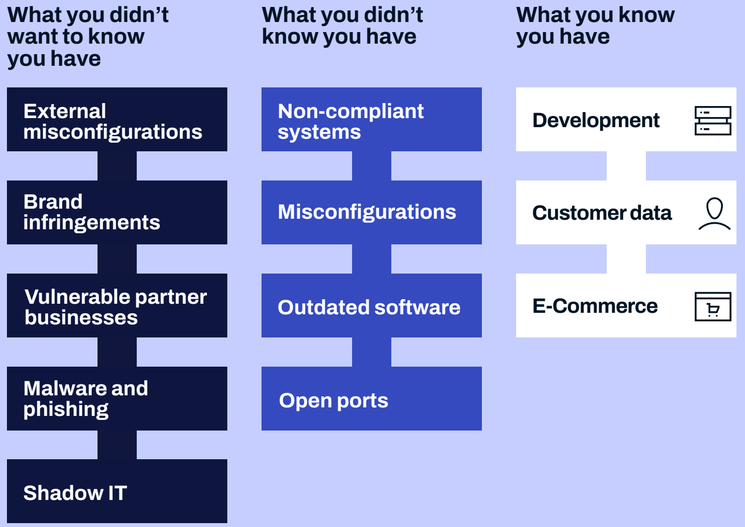
Automated scans
Keep up to date by continuously scanning your environment with unlimited automated scans.

Unlimited scan nodes
Only pay for the number of IP addresses you cover. Scan as many environments as you like.

Flexible deployment
Deploy rapidly as a cloud-delivered solution or on-site – even in closed offline environments.

Consolidated security
With the unified cloud-native WithSecure™ Elements cyber security platform, you can stay on top of your security state, and secure your endpoints and cloud collaboration, while managing your attack surface with network-based vulnerability management. By managing your security through a single pane of glass you can reduce risk, workload, and response time when threats emerge.

What is the attack surface?



What is a vulnerability?

In cyber security, a vulnerability is any means by which an attacker can gain unauthorized access to or control of an application, service, endpoint, or server.

Powerful scan arsenal to cover your attack surface

WithSecure™ Elements Vulnerability Management arms you with a broad range of scanning options. Get full visibility by combining node-based network scans, cloud scans, node scans for external threats and agent-based scans for agile remote scanning. Log into systems to get a detailed view.

Discovery scan
Discovery scan discovers and maps all assets, systems and devices on your network. The scan lets you create scan groups for efficient vulnerability management.

Agent-based scan
The agent-based scan leverages the single agent of the WithSecure™ Elements platform, and lets you scan remotely sprinkled Windows computers outside your network. This is especially handy in the remote working era, and means less open doors required to your most valuable devices when performing vulberability scans. The agent-based scan collects lists of hardware and software, and identifies open ports and vulnerabilities related to installed software and operating systems. The agent-based scan is a lightweight procedure – easy to perform frequently to maintain an up-to-date view of your assets.

Internet discovery scan
The Internet Discovery Scan identifies all internet-facing systems/services. The Internet Discovery Scan gives you a powerful search function by using DNS names to identify assets within the domain. It helps you gain awareness of what services actually reside within domains under your control. With an Internet Discovery Scan you can find shadow IT and potential brand infringements/breaches (e.g. a misleading domain name).

System scan
System Scan is a network-based vulnerability scanner that is able to scan any system with an IP for common vulnerabilities. It first identifies the system and its version number, and then checks it for open ports, known vulnerabilities (i.e. missing patches), default passwords and misconfigurations. It causes no disruption, so there's no fear of denial of service.

Authenticated Scan lets System Scan log into systems – improving accuracy and decreasing false positives and negatives – to find vulnerable system versions, missing patches and mis-configurations.

Web scan
The web scan – typically used as a complementary scan – allows you to scan and test custom web applications. You can use web scans during the development of new applications as part of the development life cycle, enabling you to catch vulnerabilities early in the process and saving considerable resources in the long run.

Web servers, Email servers, DMZ subnetworks (Cloud Scan Node)

Windows servers, Windows desktops (Endpoint Agent)

Servers, Computers, Network devices, Other devices (Local scan node)

Unifying vulnerability management with preventive and responsive cyber security measures for true situational awareness

Good cyber security can't live in a silo. First of all, when using a fragmented cyber security tool stack, you have to constantly jump from one portal to another. Alert fatigue is real, and managing multiple separate workflows is complex, making it challenging to prioritize.

Second, management is not the only inefficiency. Solutions in a set-up like this don't co-operate – and can be completely oblivious of one another. This means silos, missed detections, slow responses and eventually a weaker security posture.

To overcome the challenges of a siloed world, WithSecure™ Elements unifies core cyber security capabilities into one intelligent platform. More elements means more results, but you can build your own cloud-based cyber security suite with pick-and-choose technology modules. You can easily introduce new capabilities and ramp usage up and down as the time passes and your needs change.

When you power up your cyber security stack with a unified combination of vulnerability management, endpoint protection and endpoint detection and response and cloud application protection, you can fend off a full spectrum of cyber threats. Unified technologies work together as one – from back-end to front – and are easy and efficient to manage from a single portal.

What makes the unified set of vulnerability management and endpoint detection and response so powerful, is the situational awareness you gain. You get risk-based visibility into the threats you face from multiple fronts. You can see where the flaws in your security architecture are, what are the weak spots the attacker can exploit to get in and what is happening in your IT environment.

When you onboard WithSecure™ Elements Collaboration Protection, you'll be able to detect malicious content and activity across your business-critical Microsoft 365 collaboration applications. Besides vulnerabilities, email is still one of the most exploited attack vectors for cyber criminals to gain entry to target systems. In the hybrid work era, other collaboration applications such as SharePoint are also gaining traction.

Instead of siloed pointer solutions, WithSecure™ Elements gives you the means to protect your IT estate in a unified and efficient way. Intelligent technologies are powered by advanced AI and automation, lightening the load for you and your team. You can also offload your daily security management to our certified partners, and free up time to focus on more strategic activities.

WithSecure™ Elements – consolidate your cyber security

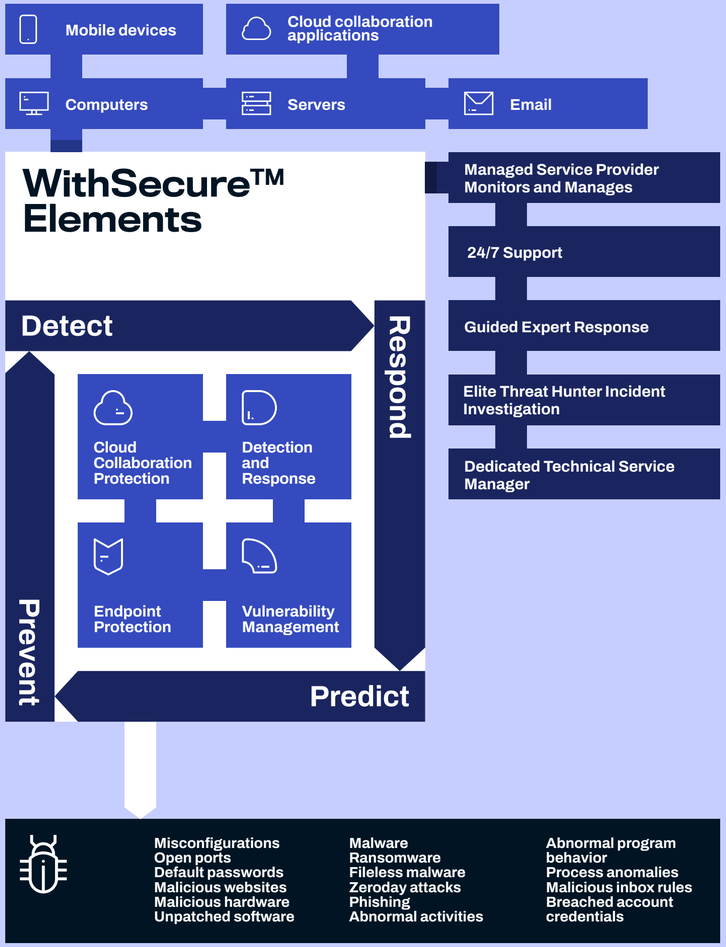
Unify your security technologies
security components work together seamlessly without loopholes using a shared data set, and are managed through a single security center

Be situationally aware
real-time visibility into your environment, including a complete picture of what is happening there, what your risks are, and how to prioritize them

Build your suite
customize your security palette with pick and choose modules

Integrate easily
connect security data easily with your third-party SIEM, SOAR, security management, monitoring or reporting systems

Adapt to changes
no strings attached, with flexible subscription options ranging from usage-based to annual



Supported operating systems:
Requirements

Supported browsers
Vulnerability Management supports the latest versions of the following browsers:

- Microsoft Internet Explorer (end of support 1st of May 2020)
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Supported languages
English, Finnish, French, German, Italian, Japanese, Polish, Portuguese (Brazil), Spanish (Latin America), and Swedish.

On-site installation
On-site installations of Vulnerability Management require one of the following Windows operating systems:

- Windows Server 2008 R2 or newer (full installation, not Server Core)

Reduce your attack surface by finding and fixing vulnerabilities across your IT environment.

Book a demo

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure