CYBERSECURITY SERVICES
Application Security Testing

Expert Testing to Gain Confidence That Micro Services, Web Applications, APIs and In-house Applications Are Secure

Test Your Security Defenses

Organizations often lack the internal resources and expertise to keep up with an ever-changing security landscape, let alone test and assess their networks, applications and overall security programs. They need help elevating their security profile, reducing risk and achieving compliance with applicable laws and industry standards.

How Enfo Helps

Enfo Security Application Testing provides organizations with the knowledge, expertise and efficiency needed to conduct thorough security evaluations of their environment. We offer testing and assessments that address logical, physical, as well as technical and nontechnical threats to your assets and environment.

We can help you identify the gaps that expose you to risk and ultimately construct a stronger security posture.

Application Security Assessments provide assurance that your, micro services, web applications , APIs and in-house applications are secure.

Protect the value of and trust in your brand, while gaining peace of mind by leveraging our deep knowledge of the Tactics, Techniques and Procedures (TTP) used by threat actors.

Incorporate security checks in your DevOps development pipeline.

Web Application Security Assessment

External Applications

Web applications represent an organization's connection to the Internet and its customers, partners and suppliers. Web applications are critical assets that drive customer awareness, revenue and sales activity.

This makes web applications attractive targets for threat actors, and the source for a majority of reported security breaches.

Internal Applications

Applications that are accessible through an organization's internal network drive business processes and house sensitive information such as intellectual property, client data, employee information and sales data.

Our elite team exceeds the OWASP Top 10 and SANS Top25 to assess and test the state of your applications, and provide actionable recommendations to enhance their security using binary and dynamic code analysis.

With Enfo, you can:

- Assess your applications for known vulnerabilities

- Identify business logical flaws before attackers do

- Validate the effectiveness of your perimeter controls

- Evaluate the security controls in place for your applications

- Test to determine specific areas of weakness and their risk to your organization

Contact Enfo
Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

Micro Services Security Assessment

Businesses and public organizations are turning more and more to mobile-based applications to innovate and interact with their customers, employees and partners.

However, mobile devices and micro services can increase an organization's attack surface for cyber threat actors, or inadvertently risk unauthorized access and data loss. As a result, many organizations are grappling with the issue of micro services security for their customers, employees, and business partners.

The Enfo Mobile Application Security Assessment is a holistic security and risk assessment of your mobile application. Our assessment examines the security and compliance risks of your entire mobile application, its associated backend systems and the interaction and data flow between them. We will:

- Examine the application interfaces as well as the supporting infrastructure to determine possible attack vectors

- Analyze internal controls in an effort to expose vulnerabilities that are not apparent from end-user interface testing only

- Perform detailed manual technical testing with the goal of identifying potential risks, vulnerabilities and threats

Web Service or API Testing

Web service or APIs are typically used as connective tissue between applications (middleware) to connect systems and support business operations.

Examples include business to business (B2B) transactions and backend e-commerce functionality. Testing application web services or APIs requires advanced knowledge of the coding techniques and packages used in delivering applications and services

Other Adversarial Security Testing Services

No individual, stand-alone technique provides a comprehensive picture of an organization's security. Each adversarial test has its own objectives and acceptable levels of risk. Enfo can work with you to determine what combination of techniques you should use to evaluate your security posture and controls to identify your vulnerabilities.

- Penetration Testing of the applications

Customer Benefits

- Gain assurance that our mobile applications, web applications and APIs are secure

- Receive actionable recommendations to enhance security

- Reduce your risk and improve operational efficiency

- Maintain client, employee and business partner confidence

- Meet compliance

Solution Features

- Tests assess web applications, mobile applications, and APIs to identify known vulnerabilities

- Expert guidance and recommendations to improve security posture

- Testing includes, but is not limited to the OWASP Top10 and SANS Top25 most critical application security flaws

- Many supported Web Services and API frameworks

- Thorough review of not just the application but whether a hacker could gain access to the network or data behind it.

enfo

CYBERSECURIITY SERVICES

AWS Cloud Security Guardian

Automate and Continuously Monitor Security Configuration Across Your AWS Control Plane

The volume of events and changes to cloud workloads place significant demands on your staff to maintain security configuration settings. AWS Cloud Guardian by Enfo is an agentless SaaS solution that helps to eliminate the risk of human error and misconfigured control plane settings by automating the protection of your Amazon Web Services (AWS) environment.

Customer Benefits

- **Stay Secure:**
  Identifies gaps in security coverage that threat actors could exploit

- **Increase Visibility:**
  Always-on monitoring and visibility to keep up with dynamic cloud environments

- **Save Time:**
  Respond to alerts with 1-click repair mitigation

Solution Features

- **Agentless** solution with no performance impacts

- **Easy** provisioning,not hours or days

- **Customizable** security policies

- **Real-time** AWS configuration visibility and automated remediation

- **Security best practices** used from CIS benchmarks and Enfo Cybersecurity

Ensure Security Control

Your cloud workloads are inherently dynamic which makes them difficult to control on a daily basis. Recently publicized examples show that simply misconfiguring an AWS S3 bucket can lead to a devastating data breach.

You need constant visibility of your control plane settings to ensure gaps are shut down immediately before damage occurs and to avoid 'configuration drift'.

Security automation solves this cloud configuration challenge and provides continuous cloud workload protection to ensure you are maintaining good hygiene and security control in the cloud every day.

Contact Enfo
Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

How Enfo Cybersecurity Helps

Enfo offers a SaaS solution that provides the security configuration visibility needed and automates AWS control plane settings for your cloud environment.

Provisioned in minutes, the agentless SaaS solution alerts you to critical issues that need repair such as disabled multi-factor authentication settings, S3 Bucket gaps, and outdated EC2 instances.

AWS Cloud Guardian Portal

Real-time monitoring and visibility pinpoints security events that require your attention and helps you respond quickly to actual threats before damage or exfiltration can occur.

The solution helps to eliminate the risk of human error and misconfigured control plane settings by automating the protection of your AWS environment. 1-click remediation can be enabled as well as the ability to lock-down configurations against future vulnerabilities.

How It Works

AWS Cloud Guardian helps eliminate the risk of human error and misconfigured control plane settings by automating the protection of your AWS services, accounts, and availability zones.

The SaaS solution provides an early warning of potential security risks and guidance for areas of additional security focus. It also provides continuous configuration monitoring, validation across your AWS environment, real-time issue identification, and automated repair.

Configuration issues are escalated as alerts to enable rapid response either manually or by locking down 1-click repair mitigation.

Built From Security Best Practices

Cloud security best practices such as Center for Internet Security (CIS) Benchmarks were integrated into the development of the solution along with insights gained from Enfo Cybersecurity Incident Response engagements.

Logging Alert Examples

- Users without multifactor authentication

- S3 Bucket is publicly accessible, or S3 Bucket does not have logging enabled

- EC2 instance is inactive in region

- CloudTrail not enabled or CloudTrail log file is not encrypted

- CloudTrail not integrated with CloudWatch Logs

- Load balancer does not have access logging enabled

- Role policy allows manipulating EC2 Security Groups

enfo

CYBERSECURIITY SERVICES

Cloud Security Monitoring

Continuous Monitoring Combined with Advanced Analytics and Threat Intelligence to Protect Your Cloud and Hybrid IT Workloads

Cloud Security Monitoring by Enfo enables organizations to fortify their cloud defense posture while reducing costs and increasing response speed without adding new headcount. Powered by the Enfo Cybersecurity monitoring platform, our experts monitor, correlate, and analyze your cloud data sources to filter out false positives, identify true security events, and support remediation.

Customer Benefits

- Reduce cloud breach risk with continuous monitoring

- Save time by reducing false positives

- Close costly cloud compliance gaps related to log monitoring

- Free up your staff to focus on strategic responsibilities

- Gain insights and control of shadow IT usage

Solution Features

- Monitoring of applications, devices and servers in the cloud

- Powered by the Enfo monitoring platform for advanced analytics and event correlation

- Proactive escalations and alerting

- Single-pane view of your cloud and on-premises threats

- Simplifies compliance with easy reporting

Cloud Threat Visibility

Migrating valuable data and applications to the cloud comes with an increased need for protection against threat actors. Inadequate cloud security during this transition stage exposes you to compliance gaps and vulnerabilities.

However, your cloud environment provides a variety of new data sources that enhance threat visibility when monitored correctly with the right people, process, and technology in place.

The challenge is hiring and retaining cloud security experts and equipping them with a process and platform to make sense of the volumes of log data on a regular basis.

This is a complex task and can leave security gaps especially when neglecting advanced analytics and threat intelligence.

Contact Enfo

Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

Cloud Security Monitoring for Amazon Web Services

Enfo is an AWS Advanced Technology Partner and industry leading security services provider that monitors your AWS environment for threats.

Powered by the monitoring platform, we collect and analyze data from a variety of AWS log sources and services (e.g. CloudTrail, VPC, Flow Logs, Logical Devices, etc.) to ensure you remain protected as you scale up or down.

For advanced threat visibility, our Advanced Endpoint Threat Detection provides AWS server monitoring coverage.

Monitored Firewall and WAF on AWS

In today's cloud-first environment, virtual firewalls and web application firewalls (WAFs) are key controls to secure your data and applications. They also generate a substantial amount of log data.

Enterprises without the staff or expertise to evaluate and assess suspicious traffic can rely on Enfo for monitoring, threat correlation, and expertise.

Cloud Security Monitoring for Microsoft Azure

Receive security monitoring, event correlation, and advanced analytics of security logs from your Azure infrastructure including Azure Active Directory, Azure Activity, and Azure Security Center Alerts.

In addition, we can provide monitoring support for your Azure firewall and WAF devices.

For advanced threat visibility, our Advanced Endpoint Threat Detection provides Azure server monitoring coverage.

Cloud Security Monitoring for Office 365®

Enfo provides the threat visibility needed to transition your enterprise to Office 365 with confidence.

Robust data logging, monitoring, and reporting alert you to threats and unauthorized access to key services such as Exchange Online, SharePoint Online, and Azure Active Directory.

We help you achieve better data governance and detect unauthorized users or activity before damage occurs.

Supported Platforms

Azure   Office 365   aws

Enfo
Data-driven business transformation

enfo

CYBERSECURIITY SERVICES

Managed Security Detect

Identify Vulnerabilities and Reduce Risk

Vulnerabilities emerge every day within new networks, web applications and databases. They may occur due to software defects or misconfigurations of information systems. It is essential to protect your critical IT assets and safeguard sensitive information by eliminating these opportunities for potential cyber adversaries.

Customer Benefits

- Identify real, exploitable vulnerabilities

- Satisfy regulatory compliance requirements

- Supplement your team with dedicated vulnerability management experts

- Track remediation workflow easily

- Access information security experts 24x7
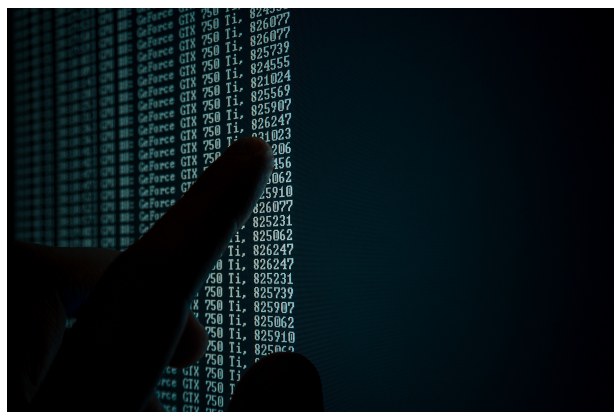
Solution Features

- Highly accurate internal and external vulnerability scanning

- Supports physical, cloud and virtual infrastructure

- Dedicated vulnerability management team provides expert guidance and support

- Flexible reporting and remediation workflow tools via

- on-demand portal

- Policy and compliance scanning to satisfy regulatory mandates

- 24x7 expert support by certified security analysts

Identify Security Threats and Reduce Risk

According to research conducted by Gartner, through 2020, 99 percent of vulnerabilities exploited by threat actors will continue to be ones known by security and IT professionals for at least one year.

One common thread in the dialogue of regulatory challenges and litigation has been, "Did the organization have a plan to address known vulnerabilities and did they execute on that plan?"

Additionally, IT organizations are commonly expected to explain how threat actors penetrated existing defenses in the event of a security breach.

Comprehensive vulnerability management, a foundational component of an organization's security posture, can be difficult to manage due to time and resource constraints. To lower business risk, meet compliance mandates and protect critical assets, organizations need complete visibility of the vulnerabilities that exist in their IT environment, context to determine their relative risk and a remediation plan.

Contact Enfo

Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

How Enfo Cybersecurity Helps

Enfo Vulnerability Management As a Service partners with leading security platform providers to perform highly accurate scan audits across internal and external network devices, servers, web applications, databases, and other assets on-premises and in cloud environments.

Provided as an on-demand service, Enfo VMaaS provides world-class vulnerability management without the hardware, software and maintenance requirements of most scanning products. The security platform technology is fully managed and maintained by our dedicated vulnerability management team, eliminating administration and maintenance burdens.

Taking It to a New Level

Enfo Vulnerability Management As a Service Platinum is a high-touch program managed solution designed for large enterprise Customers, which implements and manages powerful vulnerability scanning capabilities as well as the prioritization and tracking of remediation activities. VMS Platinum solves two problems: how to prioritize vulnerabilities identified by the scanner, and how to ensure timely remediation of the biggest threats.

Our Vulnerability Management solution reduces your exposure, ensures regulatory compliance, and safeguards your devices and data, allowing you to focus on your business priorities. There is no operational overhead with our solution, eliminating the demand on Customer personnel to chase false positives, false negatives and host crashes.

New signatures are delivered weekly, meaning the solution stays up to date on the ever-evolving global threat landscape.

Powerful, Effective Scanning

Our Vulnerability Scanning service delivers the largest and most up-to-date knowledge base of vulnerability checks, using internal and external scanners to accurately detect vulnerabilities across your network and supported cloud environments. Security platform modules provide the added value of:

- **Cloud agent:** Extends security across a Customer's enterprise by collecting vulnerability data on each host even if the host is not connected to the network. Provides faster and more accurate scan results.

- **Threat protection:** Cloud-based solution that prioritizes vulnerabilities posing the greatest risk by correlating active threats against vulnerabilities. Also includes a Live Threat Intelligence feed and dynamic dashboards to highlight areas of exposure.

- **Continuous monitoring:** Constantly monitors a Customer's perimeter, detecting changes in the network and providing alerts before they turn into breaches.

- **PCI compliance:** Provides scanning of in-scope PCI IP addresses, review of submitted false positive exceptions and reporting.

- **Policy compliance:** Automates the process of assessing server and application configuration compliance, which is useful for Customer's subject to compliance mandates (PCI, HIPAA).

- **Web application scanning:** Automated, self-service vulnerability scanning of internal- and external-web-based applications.

Contact Enfo
Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

CYBERSECURITY SERVICES

NexGen Endpoint Threat Protection

Reduces Time to Detect and Effort to Respond With Carbon Black Technology

How Endpoint Protection Works

Our NexGen Endpoint Threat Protection solution utilizes lightweight sensors to gather security specific telemetry from your servers, laptops and desktops. The sensors continuously monitor the registry, file system, process tables, memory and other areas for potential compromise.

The "always-on" nature of the solution with 24x7 protection gives you the earliest possible warning when threat indicators are detected, even when your endpoints are disconnected from the corporate network. Sensor telemetry is sent to powerful analytics systems that apply a combination of supervised machine learning and human intelligence to identify more threats faster.

Threat Intelligence from the Enfo Cybersecurity team helps eliminate time wasted on minor issues or false positives, so your security team can focus on what's important. If a threat is detected, an alert is automatically generated. Alerts and suspicious activity are investigated in more depth by Enfo.

Because sensors record a wide range of activity taking place on each endpoint, analysts are able to pinpoint threats and determine how and when they entered the environment.

The NexGen Endpoint Threat Protection can even identify threats that use no malware and threats that slip past security technology alone.

Our analysts use a variety of public and proprietary tools, combined with information from your environment to add enriched context to the alert, such as who may be behind the attack, which endpoints are impacted, what else to look for across your organization and what next steps are appropriate for remediation
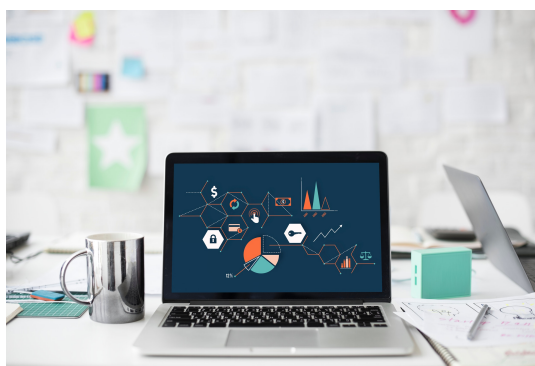
NexGen Endpoint Detection and Response

Security teams are increasingly aware of the risk posed by advanced threat actors bypassing existing security controls and threat prevention tools via phishing, social engineering and exploitation of unpatched vulnerabilities in servers, laptops and desktops.

As a result, your security strategy must include 24x7 endpoint protection to identify advanced threats and threat actors who may infiltrate your organization with little or no malware.

Employing strong technology, the Enfo Cybersecurity team and the NexGen Endpoint Threat Detection solution gives you the earliest possible warning that your endpoints may be hosting an advanced adversary.

The solution elevates your security situational awareness by warning you when endpoints may have been compromised and accelerates remediation efforts by identifying which systems are compromised, how they were compromised and how you can repair them.

Contact Enfo

Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

Carbon Black Cb Response

Cb Response is a highly scalable Endpoint Detection and Response (EDR) technology that provides visibility for top security operations centers and incident response teams. No prevention technology can stop all threats and an attacker only needs to breach one endpoint to infiltrate your organization so endpoint visibility is critical.

Cb Response captures detailed security related information from your Windows, macOS and Linux endpoints, giving analysts and incident responders a more complete understanding of the threat. Isolation of infected systems helps prevent lateral movement and enables removal of malicious files.

Cb Response allows you to see what happened with clear attack chain visualizations that help uncover the root cause, so you can quickly address gaps in your defenses.

Customer Benefits

Gain heightened visibility across your endpoints

- Detect threats that may be invisible to other security tools

- Accelerate response with critical event escalation including remediation guidance

- Fortify defenses and increase the value of your other security tools by helping to validate their output

- Minimize data loss and other damage by identifying affected systems quickly

- Increase confidence in system integrity and data confidentiality

Once we have determined the severity of the issue, critical alerts are promptly escalated to you.

Proven Intelligence and Enhanced Visibility

Advanced Endpoint Protection leverages strong EDR technology and Threat Intelligence developed by the Enfo Cybersecurity Team. This combination of supervised machine learning and human intelligence has proven to be effective in detecting advanced threats across hundreds of thousands of endpoints.

Sensors record all pertinent activity on your endpoints so our security analysts can pinpoint when a breach occurred, the cause and to where the threat actor and malware may have spread.

This precision means you can eradicate threats earlier in the kill chain with response efforts that are targeted, more effective and less costly. Detailed alerts with business context help reduce costs by allowing your security team to patch exploited vulnerabilities versus reimaging entire systems in hopes of evicting threat actors.

Insights from our experienced analysts help you see activity from the initial breach to lateral movement across your organization. We help eliminate time wasted on minor issues and false positives, so you can focus on what's important to your business.

This is how the Enfo Advanced Endpoint protection allows you to see more, know more and defend faster.

Contact Enfo
Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

CYBERSECURIITY SERVICES

Penetration Testing

Validate Security Defenses Against Real-World, Simulated Attack Methods

Identify vulnerabilities and validate security defenses utilizing independent expertise, experience and perspective to enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency.

Customer Benefits

- Gain assurance by testing internal and external security controls, including protections around high-value systems

- Gain actionable course of action for remediation

- Satisfy compliance requirements, including ISO27001, PCI DSS and HIPAA

- Confidence knowing the latest Threat Intelligence from Enfo Cybersecurity was utilized

- Determine your real-world risk of compromise.

Think Offensively to Secure Defenses

Unauthorized access to company resources using existing and new vulnerabilities is a serious security concern.

Verifying that new and existing applications, networks, and systems are not vulnerable to a security risk is key to addressing these vulnerabilities before they can be utilized by unauthorized users.

While vulnerability assessments are a "light touch" evaluation to identify gaps and vulnerabilities in your network, further testing is required to show how an attacker would gain access to your environment and use those systems as a base for attacks deeper into the network.

How Enfo Cybersecurity Helps

Enfo approaches every penetration test as unique to every organization. Our methodology is performed by the industry's top security testers, leveraging our proprietary tactics and intelligence from Enfo Cybersecurity Team.

Penetration Tests are designed to show how a cyber adversary would gain unauthorized access to your environment by using similar tactics and techniques.

During Internal Testing, Enfo can leverage your entire network in an effort to compromise a subset of target systems..

During External Testing, Enfo will leverage tactics such as OSINT and credential testing in an effort to compromise the target systems.

Enfo delivers the findings in a final report and provides a customized course of action for both leadership and technical audiences.

Contact Enfo

Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

What Does the Test Help You Answer

A Penetration Test identifies and demonstrates vulnerabilities, answering the question: could an attacker break into my network?

The results of the test empower your organization with a new understanding and strategy to strengthen your security posture against cyber threats that uniquely affect you.

Enfo Penetration Testing can be performed from the perspective of threats exploiting the network edge facing the Internet (**External**), as well as from inside the network environment (**Internal**).

Wireless Network Testing identifies what wireless devices are accessing your network, determines if there are any rogue access points, and evaluates the security of your Wi-Fi infrastructure.

Testing Your Security Awareness

Lack of security awareness of your personnel could also pose a risk to your business.

Phishing tests can identify if your employees need training to improve your security defense. For example, you may:

- Have a mature security program and want to test people as well as the network

- Need a more advanced threat simulation that more closely matches attack vectors seen in the wild (phishing + endpoint compromise)

- Need to mix phishing engagements with network penetration testing

Solution Features

- Tailored Rules of Engagement including review of target systems for business-critical data

- Final reports containing detailed findings and executive summary

- On-premise and remote testing options

- Option to mix External Penetration Testing, Internal Penetration Testing, and Phishing to create a blended threat scenario

- Tester-driven, manual process that includes tactics used by threat actors

- Goal-based methodology ensures that systems are tested in the greater context of their environment

What to Expect in Your Report

An **Executive Summary** is targeted toward a nontechnical audience — senior management, auditors, board of directors, and other concerned parties.

- **Engagement summary:** Briefly describes the results of the engagement

- **Summary of findings and recommendations:** Describes systemic issues and high-risk findings, and our recommendations to remedy issues or reduce risk

Detailed Findings are targeted toward technical staff and provides detailed findings and recommendations:

- **Engagement methodology:** Details of what was performed during the engagement

- **Narrative:** Describes the sequence of actions taken by the testers to achieve the goals of the engagement, to assist in understanding blended threats and/or dependent phases

- **Detailed findings and recommendations**: Describes any findings, web page links for further reading, and recommendations for remediation or risk reduction. Testers supply evidence of their findings where applicable and, if possible, sufficient information to replicate the findings using publicly available tools.

Contact Enfo
Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo

CYBERSECURIITY SERVICES

Vulnerability Management as a Service

Identify Vulnerabilities and Reduce Risk

Vulnerabilities emerge every day within networks, web applications and databases. They may occur due to software defects or misconfigurations of information systems. It is essential to protect your critical IT assets and safeguard sensitive information by eliminating these opportunities for potential cyber adversaries.

Customer Benefits

- Proactive in your security approach

- Identify real, exploitable vulnerabilities

- Satisfy regulatory compliance requirements

- Supplement your team with dedicated vulnerability management experts

- Track remediation workflow easily

- Access information security experts

Solution Features

- Highly accurate internal and external vulnerability scanning

- Supports physical, cloud and virtual infrastructure

- Dedicated vulnerability management team provides expert guidance and support

- Flexible reporting and remediation workflow tools via on-demand portal

- Policy and compliance scanning to satisfy regulatory mandates

- Expert support by certified security analysts

Identify Security Threats and Reduce Risk

According to research conducted by Gartner, through 2020, 99 percent of vulnerabilities exploited by threat actors will continue to be ones known by security and IT professionals for at least one year.

One common thread in the dialogue of regulatory challenges and litigation has been, "Did the organization have a plan to address known vulnerabilities and did they execute on that plan?"

Additionally, IT organizations are commonly expected to explain how threat actors penetrated existing defenses in the event of a security breach.

Comprehensive vulnerability management, a foundational component of an organization's security posture, can be difficult to manage due to time and resource constraints.

To lower business risk, meet compliance mandates and protect critical assets, organizations need complete visibility of the vulnerabilities that exist in their IT environment, context to determine their relative risk and a remediation plan.

Contact Enfo

Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

Enfo
Data-driven business transformation

Enfo is a Nordic IT service company enabling its customers' data-driven business transformation. With our niche expertise in hybrid platforms, information management and applications, we bring together relevant data for more intelligent operations. We both build and run digital solutions – supporting our customers with genuine care in mastering the complexity. We are 900 experts working for a more intelligent world, with technology empowering people, businesses and societies.

enfo

How Enfo Cybersecurity Helps

Enfo Vulnerability Management as a Service (VMaaS) partners with leading security platform providers to perform highly accurate scan audits across internal and external network devices, servers, web applications, databases, and other assets on-premises and in cloud environments.

Provided as a flexible scheduled service, Enfo VMaaS provides world-class vulnerability management without the hardware, software and maintenance requirements of most scanning products. The security platform technology is fully managed and maintained by our dedicated vulnerability management team, eliminating administration and maintenance burdens.

Taking It to a New Level

Enfo VMaaS can be delivered as a Platinum tier that is a fully managed solution designed for large enterprise Customers, which implements and manages powerful vulnerability scanning capabilities as well as the prioritization and tracking of remediation activities. VMaaS Platinum solves two problems: how to prioritize vulnerabilities identified by the scanner, and how to ensure timely remediation of the biggest threats.

Our Vulnerability Management solution reduces your exposure, ensures regulatory compliance, and safeguards your devices and data, allowing you to focus on your business priorities. There is no operational overhead with our solution, eliminating the demand on Customer personnel to chase false positives, false negatives and host crashes.

New signatures are delivered weekly, meaning the solution stays up to date on the ever-evolving global threat landscape.

Powerful, Effective Scanning

Our Vulnerability Scanning service delivers the largest and most up-to-date knowledge base of vulnerability checks, using internal and external scanners to accurately detect vulnerabilities across your network and supported cloud environments.

Security platform modules provide the added value of:

- **Cloud agent:** Extends security across a Customer's enterprise by collecting vulnerability data on each host even if the host is not connected to the network. Provides faster and more accurate scan results.

- **Threat protection:** Cloud-based solution that prioritizes vulnerabilities posing the greatest risk by correlating active threats against vulnerabilities. Also includes a Live Threat Intelligence feed and dynamic dashboards to highlight areas of exposure.

- **Continuous monitoring:** Constantly monitors a Customer's perimeter, detecting changes in the network and providing alerts before they turn into breaches.

- **PCI compliance:** Provides scanning of in-scope IP addresses, review of submitted false positive exceptions and reporting.

- **Policy compliance:** Automates the process of assessing server and application configuration compliance, which is useful for Customer's subject to compliance mandates (PCI DSS, HIPAA and ISO27001).

- **Web application scanning:** Automated, self-service vulnerability scanning of internal- and external-web-based applications.

enfo