GUIDE TO VULNERABILITY MANAGEMENT

F-Secure Whitepaper

F-Secure

TABLE OF CONTENTS

MANAGEMENT SUMMARY

Complete Threat Management

F-Secure Radar is a comprehensive, easy-to-deploy, all-in-one vulnerability scanning and management platform that supports organizations' security programs with clear, actionable, and prioritized visibility into real risks. Radar is mainly designed to address the needs of small and medium-sized enterprises (SME), empowering them to protect their business continuity through effective vulnerability management. Unpatched and badly configured software is a key attack vector and breach enabler, especially when it comes to more advanced attacks. F-Secure Radar can significantly lower the cost of cyber security by being proactive and identifying potential security problems before they are exploited. Leveraging Radar's cloud resources allows organizations to reduce their expenses, which is a particularly important factor for SMEs that do not yet have dedicated security resources.

Additionally, F-Secure Radar is an optimal solution for managed service providers (MSP), enabling them to enter the cyber security service business, grow with F-Secure, and capture market opportunity. With Radar, managed service providers can expand their service offering to cloud-based vulnerability management, and deliver market-leading cyber security solutions and services in a scalable and cost-efficient manner.

End customers who lack the time or knowledge to manage their own vulnerability assessments are likely to execute their cyber security strategy with the help of an established, local managed service partner. The EU data and privacy laws (GDPR) incentivize customer companies to become compliant and seek help and services from a local managed service provider. Managed service partners are most influential among end-customer deployments of less than 1,000 seats.

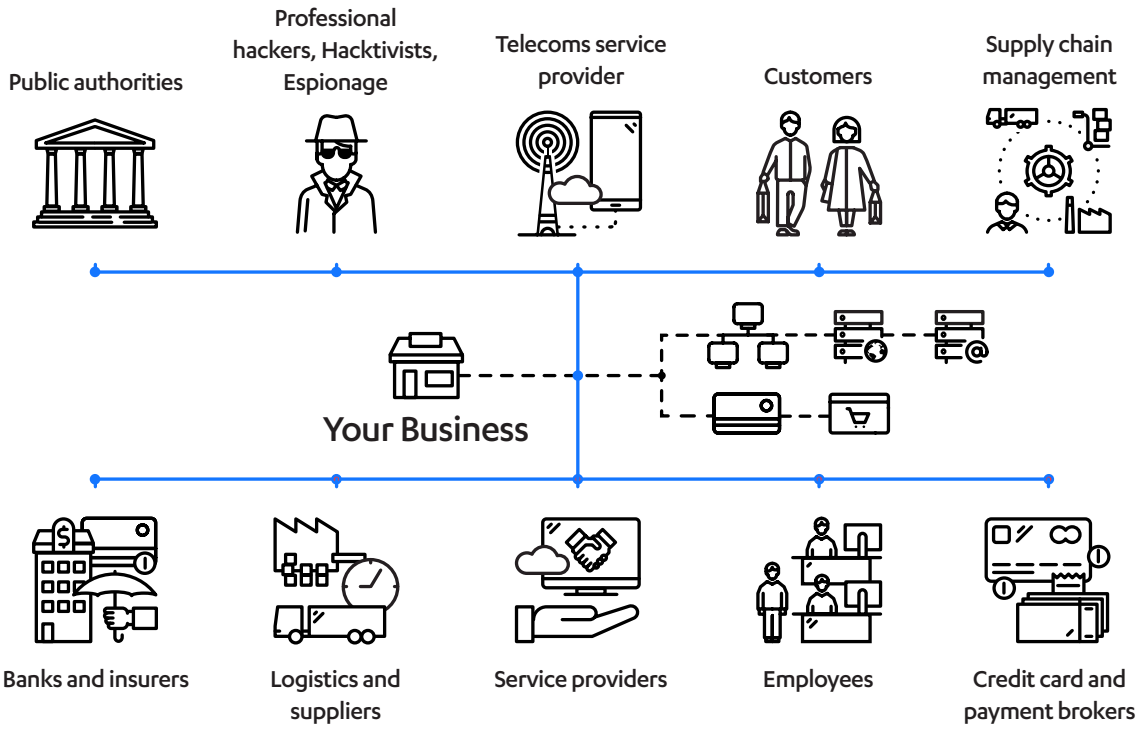
This document describes the high-level security controls F-Secure employs with Radar.

Identify and expose possible threats

Unlike many other vulnerability management solutions on the market today, F-Secure Radar features web crawling technology, called Internet Asset Discovery, that also covers the deep web. With this, you can fulfill a wide variety of tasks ranging from threat assessment to business intelligence. In essence, Radar allows you to easily browse through all targets to quickly identify risks and potentially vulnerable connections, and expand the analysis of your attack surface beyond your own network.

Successful intellectual property and brands often make companies the target for fraudulent or malicious activities. Such activities include brand violations, where third parties pose as your company, phishing sites intended to scam or infect visitors, and typo squatting – where someone registers domains using words resembling your brand to redirect traffic through links that look like yours. Many companies have little to no awareness of these sorts of activities.

THE MANY WAYS A BUSINESS CAN BE EXPOSED TO CYBER RISK



Payment Card Industry Data Security Standard (PCI DSS)

Ensure compliance with current and future regulations

As an approved service vendor, F-Secure has to perform the actions listed here to identify any scoping discrepancies that exist in the information provided by the scan customer. Information on any scoping discrepancies must be indicated on the Attestation of Scan Compliance in the "Scan Status". Although this information must be reported as noted, we then have to disregard this information in determining the PCI DSS compliance:

- Include any IP address or domain previously provided to F-Secure and still owned or used by the scan *customer that has been removed at the request of the scan customer.
- If the scan customer no longer owns or has custody of the IP address or domain, include that IP address or domain for at least one additional quarter after it was removed from scope or released by the scan customer.
- For each domain provided, look up the IP address of the domain to determine whether it was already provided by the scan customer.
- For each domain provided, perform DNS forward and reverse lookups of common host names—such as "www," "mail," etc.—that were not provided by the scan customer.
- Identify any IP addresses found during MX record DNS lookup.
- Identify any IP addresses outside the scope that are reached via web redirects from in-scope web servers (covers all forms of redirecting including: JavaScript, Meta redirect and HTTP 30x codes).
- Match domains found during crawling to user-supplied domains to find undocumented domains belonging to the scan customer.

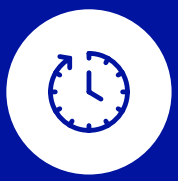
F-SECURE RADAR AT A GLANCE

Get the big picture

Map all system assets for a complete security overview. No system is too big— F-Secure Radar scales as you grow.

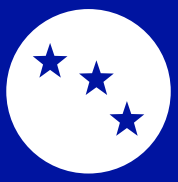
Continuous improvement

F-Secure Radar is automatically updated, improved, and ready for seamless third-party integration through F-Secure Radar API.



Streamlined security management

Monitor vulnerabilities efficiently with automated, scheduled scans. Assign, manage and track all security issues in coordination with system administrators, developers, auditors and more.



Compliant with EU regulations

F-Secure Radar meets EU regulations with PCI ASV vulnerability scanning compliance and helps customers to comply with GDPR.

Customized reporting made simple

Customize and automate standardized reports for all audiences in a variety of formats.

F-Secure Radar your way

Run vulnerability scans from a secure cloud-based SaaS or as an on-site solution behind your corporate firewall.

THE STORY OF EQUIFAX

On September 7th, 2017, Equifax, a consumer credit reporting agency, announced that they had been the victim of a cyber attack in which the personal data of as many as 145.5 million individuals was accessed. At the time of writing, this incident precipitated the early retirement of the company's CEO, two top security officials, Chief Information Officer and Chief Security Officer.

Forensic analysis into the incident indicated that the attackers leveraged an unpatched vulnerability in Equifax's web application software, Apache Struts. This vulnerability was initially discovered by Nike Zheng, a Chinese security researcher. Apache released a fix for the vulnerability on March 6th, 2017. By March 9th, 2017, attackers were already actively exploiting the vulnerability in the wild.

Equifax, like all other companies using the platform, was made aware of the patch on May 6th, 2017. A memo about the vulnerability was sent to IT staff on May 9th, 2017, but due to internal miscommunication and a series of unsuccessful investigations, Equifax did not patch all their vulnerable Apache Struts installations until July 29th, 2017, after they had discovered evidence of being breached.

As it turns out, attackers got into Equifax's systems on May 13th, 2017, exactly one week after the patch had been released. Closer investigation revealed that Equifax had a 48-hour policy for applying critical patches, but this policy wasn't followed. Had they followed their policy, they would have avoided this breach altogether.

Although close to three months sounds like a long time to patch a critical vulnerability, Equifax isn't even close to being the slowest company to patch systems against critical vulnerabilities. For instance, there are still plenty of systems in the wild that are susceptible to the EternalBlue exploits that enabled both NotPetya and WannaCry during the Summer of 2017. And while Equifax's story sounds like chaos, it's more often than not the reality for teams tasked with managing complex computing infrastructure.

Patching is not a given

Patching is not a given. Applying software updates is often the job of multiple individuals in an organization. Just as operating systems and software are highly diverse, so are the mechanisms used in applying updates and receiving notifications of available patches. Every vendor alerts their customers about the availability of updates in their own way. There is no single place to find all the information you need, and IT departments still rely heavily on email and RSS feeds to keep themselves on the map.

Updates and patches arrive on a frequent basis, and with dozens or even hundreds of separate applications to manage, most IT departments are flooded with different updates. For each of these, someone needs to understand not only what's changing in the software itself, but how it might affect the surrounding systems. For this reason, updates often need to be tested or piloted before being deployed across a whole organization. In the case of server updates, maintenance windows need to be scheduled, especially if patching causes downtime. This forces IT departments to prioritize patching activities, and to generally only patch when absolutely needed. But to make these prioritization decisions, they need to know if a vulnerability is being actively exploited, and whether that vulnerability is present in the organization's attack surface.

Known unknowns, and unknown unknowns

To properly secure computing infrastructure, IT personnel need to know what systems require patching. Obtaining this knowledge often involves collecting and maintaining an accurate inventory of all known systems and software in the organization. As companies grow, business functions commonly implement their own systems and applications without the involvement of the IT department. Those systems become part of what is commonly known as shadow IT, and can drastically increase an organization's attack surface. Shadow IT systems are difficult to find, and their impact is often grossly underestimated.

But if shadow IT systems represent a set of known unknowns, systems belonging to a company's supply chain represent an even larger set of unknown unknowns. Still, supply chain attacks are fairly common.

During Christmas 2013, criminals stole credit card details belonging to more than 60 million people from Target, a large US retail chain. The attackers breached Target's network by installing malware (via an email attachment) onto a system belonging to a company called Fazio Mechanical. At that time, Fazio Mechanical was supplying heating and air-conditioning services to Target. After the attackers breached Fazio Mechanical, they obtained the VPN credentials needed to remotely connect to Target's corporate network, and once inside, the attackers pushed malicious software onto cash registers at an estimated 1800 stores. Investigations into the incident revealed that there were no controls limiting the attackers' access to any of Target's systems, including devices within stores, such as point of sale (POS) registers and servers. In one instance, the attackers were able to communicate directly with cash registers in checkout lanes after compromising a deli meat scale located in a different store.

Don't forget your Intranet

While patching vulnerabilities in Internet-facing systems is generally taken seriously, the security of systems within a corporate network is often overlooked. Systems behind the corporate firewall are often considered "protected" from attacks, and it is assumed that there are no intruders on the network. These security shortcomings aren't always tied to software patch levels, though. Misconfigurations often provide attackers with access to easy lateral movement mechanisms.

Identifying software misconfigurations is a troublesome task. This is compounded by the fact that software isn't always secure straight out of the box, and it often takes research to figure out how to properly configure each piece of a company's IT infrastructure. Take, for example, an SSH server. Once installed, you probably want to configure it to not allow password logins, and you'll most likely want to disable the ability to remotely log into a system as root. A new admin setting up a system would need to know that these two configuration changes should be done, and would need to know how to do them. Now let's say you have a handful of SSH servers on your network, all of which were installed at different times, by different staff. To find out if any of those are misconfigured, you'd need to perform an audit of each one. Now apply that same logic to multiple other pieces of software installed across an organization, and to settings in the operating systems themselves. Not an easy task to perform once, let alone on a frequent basis. So, again, tasks like these are prioritized.

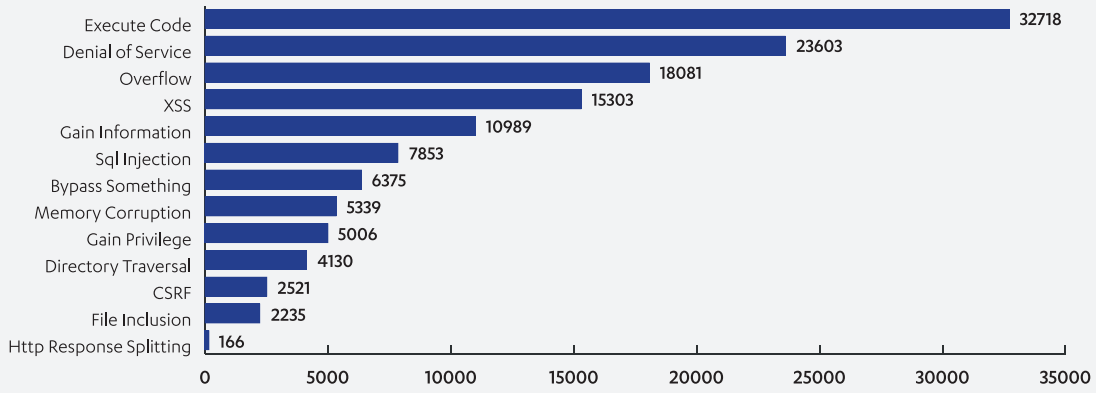
Visibility is key

Keeping systems secure is overwhelmingly complex and work-intensive. But ultimately, it's important to have a clear and accurate picture of your current situation. Only then can you start to approach the task of properly securing your infrastructure. And by then, you will you be able to answer questions such as:

- Is our risk level where it should be?
- What is the likelihood of a breach occurring?
- What would be the likely impact of a breach?
- Which of our assets are most exposed?
- What is our plan for reducing exposure of assets in the future?
- How much will it cost to bring our risk level to where it should be?
- How does that cost fit into current budget allocations?

These are the types of questions any leadership team will ask of an IT department if they're at all worried about cyber security (which they should be). So, by obtaining enough visibility into your organization's infrastructure (including the known unknowns and unknown unknowns), you'll not only be in a position to answer those questions in a proactive and confident manner, you'll sleep better at night.

OVERVIEW OF CURRENT VULNERABILITIES



Source: http://www.cvedetails.com/vulnerabilities-by-types.php

Prevent incidents proactively

With cyber threats growing more rapidly than ever, the issue of security has been brought to the forefront of every CIO's mind. Today, cybercrime is a billion dollar enterprise, and it's on the rise. According to data from Arbor Networks, the number and size of cyber attacks increased by 73% in 2017. With the incidents of cyber attacks growing year over year, no organization, regardless of size or industry, is free from the risk of a data breach. So it is no longer a question of if your company will be attacked, but when. For this reason, it is important now, more than ever, to implement a proactive approach to cybersecurity.

Due to the misconception that implementing security measures will cost businesses a lot of time and money, the default approach that companies take with cybersecurity is "reactive." A reactive approach means that companies wait until they are affected by a threat to implement a solution. Ironically, this method will likely cost your business considerably more time and money than implementing preventative measures. Statistics show that the ROI for businesses that implement preventative security measures is met in the face of an attack.

The Key to Preventing Cyber Attacks

The key to overcoming breaches caused by human error is to create an environment where all employees have a vested interest in security. Employees need to understand the value of protecting client and partner information, and their role in keeping it safe. They also need basic knowledge regarding the risk landscape, and a way to make good judgments regarding Internet safety on a consistent basis. To many people, security seems like common sense, but it is more like "out of sight and out of mind". Creating a secure foundation must begin with the training and education of employees.

Though advances in technology bring new and exciting security solutions to our industry, attackers continue to develop and launch new tactics, techniques, and procedures to outwit them. Security does not have to be a costly process, but doing nothing should not be an option. Whether or not a company can afford a new, high-tech security solution, taking a step back and focusing on security at a basic level should still be a priority. Being proactive about security is everyone's job, and requires constant vigilance. By making a conscious effort to adhere to standard processes, procedures, and policies for security and educating employees, companies can drastically reduce their vulnerability to attack.

ADVERSARIES DON'T NEED MANY VULNERABILITIES ONE IS ENOUGH

Every

90 **minutes**

a new security vunlnerability is identified

That is an average of

7 **vulnerabilities**

per asset across a typical IT environment

That is an average of

8000

known and disclosed vulnerabilities each year

50–300

critical vulnerabilities

exploitable depending on industry

It takes an average of

103 **days**

until known security vulnerabilities are remediated

It takes

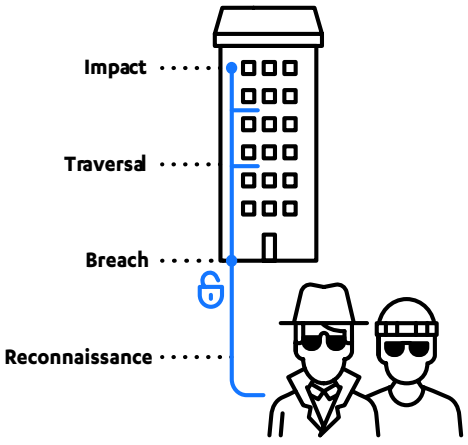
15 **days**

in the average that a vulnerability is exploited

THE USUAL TIMELINE OF AN INTRUSION

In computer security jargon, "Day Zero" is the day on which the interested party (presumably the vendor of the targeted system) learns of the vulnerability. Up until that day, the vulnerability is known as a zero-day vulnerability. Similarly, an exploitable bug that has been known for thirty days would be called a 30-day vulnerability. Once the vendor learns of the vulnerability, they will usually create patches or advise workarounds to mitigate it.

In general, there is too much hype surrounding zero-day vulnerabilities. The CVE Details website shows an average vulnerability score of 6.8, across all known vulnerabilities on all known platforms. Of the over 80,000 known vulnerabilities in their database, 12,000 (almost 15%) of those are classified as high-severity. However, it is good to remember that these vulnerabilities exist across plenty of different client and server-side applications (including, you guessed it, Adobe Flash).



From a company's point of view, handling high-severity vulnerabilities is the number-one priority. And they get handled in well-run organizations. High-severity vulnerabilities get a lot of visibility, and because of this, they're patched on the spot. But vulnerabilities alone don't make up your company's entire attack surface. Your CISO is probably more worried about phishing and upstream attacks than internal network misconfigurations and unpatched internal systems. As an IT admin, taking care of infrastructure is your biggest concern.

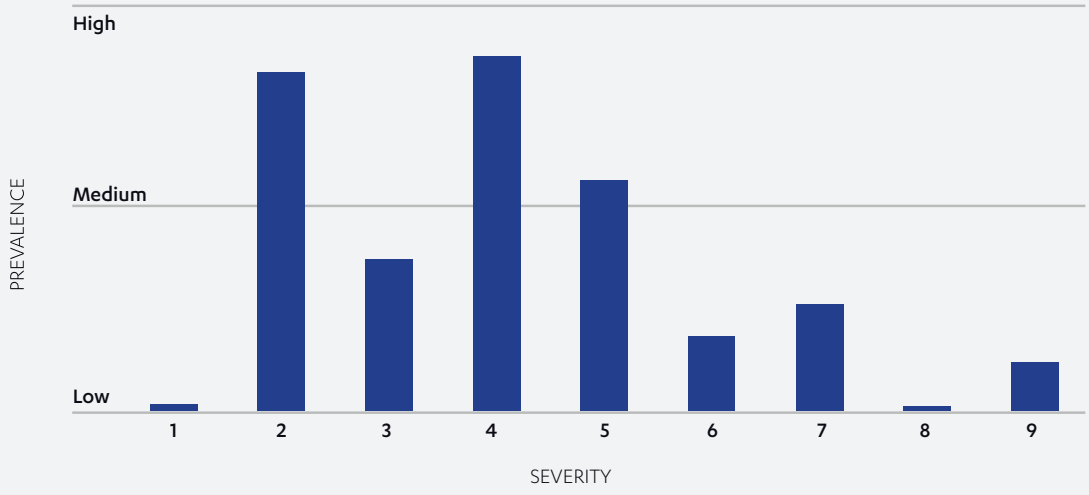
Of course, you're going to perform triage when a new high-severity vulnerability surfaces. But what about the rest of them? Applying every patch to every piece of software on every system on your network, as the patch is released, is just not feasible. That's why admins rely on periodic patch cycles to fix low-severity vulnerabilities, if they do fix them at all. Taking time out of their day to understand the implications of every new vulnerability out there is too much to ask from most IT admins.

And so, in many cases, they simply don't bother. When looking to apply patches, admins often ask questions such as:

- how exposed is the system?
- will this patch break something else?
- do I even know what this vulnerability means?

Using our RADAR service to analyze vulnerability trends within our customer base shows exactly this. High severity vulnerabilities were rare to non-existent. The vast majority of unpatched vulnerabilities we found were of low-medium severity. Of these, it's interesting to note that TLS/ SSL and OpenSSH misconfigurations were fairly common. Remember, though, that although they're labelled misconfigurations, it's possible these systems were configured that way in order to interoperate with the customer, partner, or proprietary in-house services.

Our Information Security Manager, a member of our CISO office, looked at this graph and concluded that if this represented the situation at our own company, he'd be able to sleep at night.



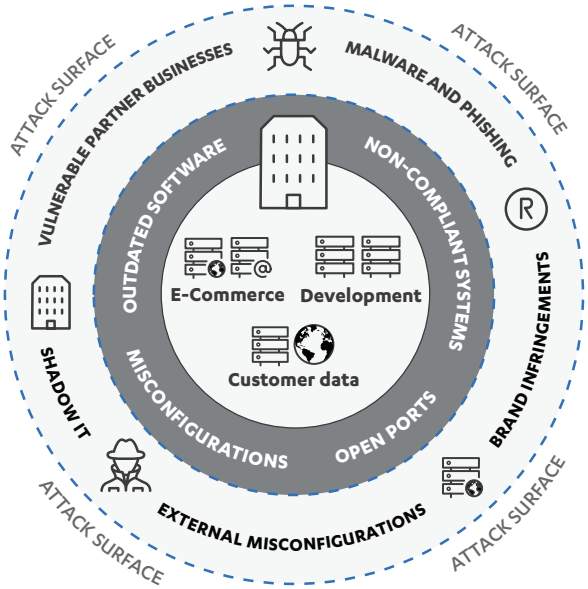
The data in this graph was collected during the first 6 months of 2018, over F-Secure's customer base, with our Radar product. F-Secure Radar is a vulnerability management and security scanning solution that performs platform and web application vulnerability scans.

WHAT ARE THE CONSEQUENCES IF YOU DON'T WATCH YOUR SURFACE?

The Risks

Establishing and then actively maintaining the secure configuration of ICT systems should be seen as a key security control. ICT systems that are not locked down, hardened or patched will be particularly vulnerable to attacks that may be easily prevented.

Organisations that fail to produce and implement corporate security policies that manage the secure configuration and patching of their ICT systems are subject to the following risks:



Unauthorised changes to systems

An attacker could make unauthorised changes to ICT systems or information, compromising confidentiality, availability and integrity

Exploitation of unpatched vulnerabilities

New patches are released almost daily, and the timely application of security patches is critical to preserving the confidentiality, integrity, and availability of ICT systems. Attackers will attempt to exploit unpatched systems to gain unauthorized access to system resources and information. Many successful attacks are enabled by exploiting a vulnerability for which a patch has been issued prior to the attack taking place.

Exploitation of insecure system configurations

An attacker could exploit a system that has not been locked down or hardened by:

- Gaining unauthorized access to information assets or importing malware
- Exploiting unnecessary functionality that has not been removed or disabled to conduct attacks and gain unauthorized access to systems, services, resources, and information
- Connecting unauthorized equipment to infiltrate information or introduce malware
- Creating a back door for future malicious endeavours

Increases in the number of security incidents

Without an awareness regarding vulnerabilities and the availability (or unavailability) of patches and fixes, the business will be increasingly disrupted by security incidents.

Security breaches hurt small businesses most

Only 31 percent of small businesses take active measures to guard themselves against security breaches. Furthermore, 41 percent of small businesses are unaware of the risks associated with human error, and only 22 percent are willing to improve their security measures from last year.

It might not surprise you that security breaches hurt small businesses the most. More than 70 percent of attacks target small businesses, and it is estimated that 60 percent of hacked SMBs go out of business after just six months. This research may be a bit skewed, since the number of people who ignore cyber security is high. People still consider traditional security measures, like antivirus and firewalls, sufficient enough.

Cost of data breach is higher than you think

A lack of awareness, coupled with exposure to threats, has led to a drastic increase in the number of attacks: data breaches' share of cyber attacks has increased to 31 percent from a mere 18 percent in 2014. If you think that you can get away easily after an attack, think again. The cost of recovery is staggering, and in most cases, it leads to the shutdown of businesses. The average cost of recovery from SMB data breaches is $36,000 and can lead to losses of up to $50,000. This amount may even be the total value of small businesses. Recovery may be next to impossible if you are the victim of a data breach.

Since most small businesses aren't able to recover after security breaches, it is always good to keep precautionary measures ready against an attack.

The company internal discussion about the cyber risk

When a CISO approaches management with a budget request for a new technology or security initiative, it's a meeting between people speaking two different languages. The CFO and CEO think in terms of monetary amounts – business value and ROI. Without those numbers to refer to, the CISO must somehow convince top management that the investment is necessary. The CISO resorts to the only argument the executives will respond to: fear. "If we don't do this, the sky's going to fall on our heads."

After all, no company wants to be the next news headline for the wrong reasons.

But at the end of the day, how does a company know if its security investments are effectively reducing or eliminating risks to the extent that its executives hope or imagine they are? The expensive employee training program, the event monitoring system, the replacement of security software across the organization? How does a company know if it's investing in the right places, or if it has purchased the proper level of insurance to adequately cover itself in the event of a data breach, ransomware incident, or DDoS attack?

And how does the CISO show top management how important these investments are to the company, without resorting to FUD (Fear, Uncertainty, Doubt) to get the message across?

The answer lies in being able to quantify the impact of a cyber breach to your company, the very practice CISOs often shy away from. It's true that using ambiguous rating systems or using red, green, and yellow color coding to indicate risks doesn't give you much to go on.

"Most managers rely on qualitative guidance from 'heat maps' that describe their vulnerability as 'low' or 'high' based on vague estimates that lump together frequent small losses and rare large losses", write Chacko, Sekeris and Herbolzheimer in the Harvard Business Review article "Can you put a Dollar amount on your companys cyber risk" from October 05, 2016. "But this approach doesn't help managers understand if they have a $10 million problem or a $100 million one, let alone whether they should invest in malware defenses or email protection. As a result, companies continue to misjudge which cybersecurity capabilities they should prioritize and often obtain insufficient cybersecurity insurance protection."

Yet, it is possible to put real numbers in your cyber security risk assessments. It is possible to speak in a language the boardroom will understand.

"Implementing this technology will cost $100,000, but it will reduce our risk by $2 million," or "We can reduce our cyber insurance coverage by $50 million, and here's why." These are statements CISOs and CFOs can make, and confidently back up, with the help of new ways of measuring and quantifying cyber security risks. F-Secure's method is called Cyber Breach Impact Quantification (CBIQ), and it predicts how much a cyber incident will cost an organization. It also shows how much companies will reduce their risk by implementing a specific security control.

2019 Cost of Data Breach Study: Global Overview

IBM Security and Ponemon Institute, study conducted between July 2018 and April 2019.

- 507 companies globally studied
- $3.92 million is the average total cost of data breach
- $150 is the average cost per lost or stolen record
- 25,575 average size of a data breach
- 279 days is the average time to identify and contain a breach
- 29,6% is the probability of experiencing a data breach in the next two years

GDPR – FEARSOME PENALTIES OR AN OPPORTUNITY TO ELEVATE YOUR ORGANIZATION?

As if the costs of recovering from a data breach aren't enough, the cost of potential fines resulting from GDPR enforcement must now be considered as well. Under the GDPR, which came into effect in May 2018 with a goal of protecting the data privacy of EU citizens, companies who experience a data breach could face fines of up to 4% of annual turnover, or €20 million ($22.5 million), whichever is greater.

The directive may be aimed at strengthening the privacy rights of EU citizens, but its scope is not limited to Europe. Under the GDPR, any company that processes, stores or transmits personal data belonging to EU residents is required to comply – a broad demarcation that affects practically any company with a Web presence. And because the GDPR is likely to set a standard other countries will want to follow, getting company policies, procedures and technologies on board is a good idea whether a company is technically affected or not. Data privacy laws worldwide are likely to get stronger, not weaker.

To look at the Equifax breach through a GDPR lens, it is estimated that the personal records of more than 147.9 million people were exposed. Had the company been subject to GDPR and its 72-hour deadline for reporting a discovered breach, it would have failed miserably. Equifax discovered the breach on July 29, 2017 and disclosed it well over a month later, on September 7. With over $3 billion in annual turnover, a rough calculation based on the maximum penalty reveals that Equifax could have potentially faced well over a hundred million in fines.

Securitywise, the GDPR does not detail specific requirements for keeping data safe. But because implementing solid security practices is critical to protecting data and being compliant, a comprehensive security program encompassing threat prediction, prevention, and breach detection and response should be in place. Effective vulnerability management, as the Equifax case illustrates, is a critical part of that program and of GDPR compliance.

Another important aspect of the GDPR is data inventory – knowing what you are storing, where you're storing it, and where multiple copies of data are located across your company infrastructure. Discovering and documenting machines where data may reside is the first step in this process. The discovery scan capabilities of F-Secure Radar can help you find and map out your network assets and shadow IT. A server set up by the marketing department for last year's campaign, for example, may contain customer information that is not part of the company's GDPR processes.

All in all, the GDPR is a reality to be approached in one of two ways: As a fearsome penalty to be avoided by meeting the minimum qualifications for compliance; or as an opportunity to appreciate its goals and proactively elevate your organization to where it should be in our increasingly data-driven world.

WHAT IS RADAR OFFERING?

The best threat response is to predict and map your cybersecurity threats. No other technology does that better than vulnerability management.

An organization's attack surface crosses all network infrastructures, software, IOT, and web applications internally and in the global Internet. It includes an understanding of all points of interaction. Information security managers need to be able to approach vulnerability assessment from several perspectives in order to get an accurate assessment of risks, minimize security threats, and maintain compliance.

Unlike any other vulnerability solution on the market, F-Secure Radar features web crawling technology, called Internet Asset Discovery, that also covers the deep web. Radar allows you to easily browse through all targets to quickly identify risks and potentially vulnerable connections, and to expand the analysis of the possible attack surface beyond your own network.

Identify and expose the possible threats

Successful intellectual property and brands often make companies the target for fraudulent or malicious activities. With a little bit of experience with Radar, any IT security manager can generate a threat assessment report concerning activities such as brand violation or phishing sites intended to scam or infect visitors.

F-Secure Radar identifies your organization's assets, and pinpoints exactly where they are vulnerable, allowing you to minimize your attack surface while reducing risk. With Radar, your IT security team maps your organization's attack surface in the aggregate of:

- all known, unknown, and potential vulnerabilities critical to business
- controls across all software, hardware, firmware, and networks
- shadow IT, external misconfigured systems, malware websites, website-linked hosts
- partner and contractor security entropy
- brand infringements and phishing

SECURITY CENTER DASHBOARD
Keep on top of the current status of vulnerabilities and incidents, prepare standard and custom reports on risk and compliance, and more

INTERNET ASSET DISCOVERY
Enumerate possible attack vectors with an internet and web threat assessment

DISCOVERY SCANS
Map your attack surface with network and port scanning.

VULNERABILITY SCANS
Scan systems and web applications for publicly-known vulnerabilities

VULNERABILITY MANAGEMENT
Manage vulnerabilities centrally with security alerts and forensics

PCI DSS COMPLIANCE
Ensure compliance with current and future regulations to reduce risk of data loss

Internet asset discovery

You can find your organization's Internet-facing systems in Radar with Internet discovery. Internet discovery uses crawling and port mapping to allow you to collect data on public systems. You can search for data based on location, top-level domain, pay-level domain, keywords, hostname, and IP address.

You can add the discovered hosts to a scan group for vulnerability scanning using either passive or active scanning. Passive scans check for vulnerabilities without connecting to the target host. Active scanning runs a regular system scan on the host. The internet asset discovery includes all of this:

- Attack Surface Enumeration
- BGP (IP to AS)
- Public sources (RIPE, Public BGP, CERNET)
- IP & Service information
- Port scans & banners
- Domain names
- Reverse DNS, zone transfer, brute force
- WhoIs information
- Linking all the above together
- Geolocation
- Public/private databases

Discovery scans

Radar Discovery is responsible for the first step in the vulnerability management workflow process and security auditing. It lets you discover hosts and network devices in your infrastructure (within defined network range(s)).

Discovery scan uses ICMP PING / TCP SYN / UDP scan / Fragment scan techniques to enumerate all hosts available on a network. Additionally, it lists services that each host are exposing and what operating systems they are running.

IP range is the only required input information to conduct network discovery scan. The other configuration options are the following:

- TCP port scanning and defining the port range
- UDP port scanning and defining the port range
- Limiting the port range to Top 100 or 1000 most common open ports
- Enabling detection of the services on the discovered hosts
- Detecting the operating system on each live host
- Scanning hosts which do not respond to PING request
- Control scanning performance by adding additional delay time between subsequent packets sent
- Control the number of simultaneous threads used during scanning

The output from a network discovery scan is a report with the list of all scanned targets with all services detected, accompanied by supplemental information depending on which options are used.

In the case when the only purpose of the scan is to determine if the host is alive, not the services it is running, the “discovery mode” can be enabled. The scan procedure in discovery mode, for each host in scope, includes ARP resolution (in local segments), ICMP PING, and a limited port scan of the default ports for SSH, HTTP, HTTPS, and Remote Desktop services. If any of those indicate that the host is active, the scan marks the host alive and proceeds to the next target.

System scans

System scan is a network-based vulnerability scanner that is able to scan any system with an IP for common vulnerabilities.

System scan's vulnerability detection is based on both active and passive vulnerability checks. For example, it will attempt to identify the service (product) and its version number. Once that is identified, the system scan checks if that particular software has any known vulnerabilities. In addition to passive scanning based on banner grabbing, the system scans also run active checks in an attempt to confirm the existence of certain vulnerabilities or system misconfigurations. It can also identify missing security patches and outdated software if authenticated scanning has been enabled.

> **Note:** System scan is non-disruptive and designed not to cause Denial of Service conditions on your systems.

When you start a system scan, it first performs a port scan of the target, and once all the open ports (services) have been identified, they are assessed for vulnerabilities. These are just some of the systems that can be examined with system scans:

- Web servers
- Firewalls
- Email servers and gateways
- Routers and switches
- Domain controllers
- DNS servers
- Antivirus gateways
- Workstations

The checks that the scanner runs include the following:

- Detect services and operating systems discovery (UDP / TCP / ICMP)
- Testing for vulnerabilities and misconfigurations in services
- Testing for vulnerabilities and misconfigurations in operating systems
- Testing for vulnerabilities and misconfigurations in network devices
- Secure configuration testing (SSL / SSH)
- Default passwords discovery (operating systems/services/network/devices)

All vulnerabilities are reported with a CVSSv2 score, CVE, BID, BugTraq, and other references when available.

Web scans

Web scans allow you to examine and test web applications. You can use web scans during the development of new applications as part of the development lifecycle. As vulnerabilities are discovered early on in the development process, the cost and amount of resources required to mitigate vulnerabilities at a later stage is reduced significantly.

Web scan is considered a complementary scan, which can be applied on top of an existing System Scan. In other words, it is recommended that whenever you scan a target with a System Scan, systems with web applications should be scanned with Web scan as well.

Defining the targets for web scans

When defining the target URL for a web scan, take into account that automated site discovery (crawling, and what is actually being scanned) is limited to locations that have:

- the same port number as the defined scan target (i.e.: port 80 - default for http://.. , port 443 - default for https:// , port 8080 - if explicitly specified like this: https://www.some-site.com:8080/)
- the same protocol as the defined scan target (in other words, if you specify the URL http://www.company.com, the scan does not automatically scan https://www.company.com in addition)
- the same FQDN as defined in the scan target (in other words, if you specify the URL https://service.com, the scan does not automatically cover content available under https://www.service.com)

This is to protect against scanning something that the customer does not intend to scan. For example, **http://www.bank.com** can consist of an official website of a bank with some generic info. Whereas **https://www.bank.com** can host a completely different service, for instance online banking The same web scan is not necessarily intended to scan both.

Custom web applications

Before you create a new web scan, you must first understand the situations where it'll be effective. As a rule of thumb, you should only scan custom web applications. If you have a system running a standard deployment of WordPress (without any custom modules installed), for example, it does not make sense to scan it with a web scan, because system scans are able to detect the WordPress version and any known vulnerabilities. However, if you know that your WordPress contains custom-developed modules, it makes sense to scan it with both system and web scans. Keep in mind that you only need to scan the custom code or module, and not the entire website.

We are using both - the top 10 and the static 55 categories

Web scans detect security vulnerabilities within commercial and custom-built web applications, testing for numerous vulnerabilities, including the OWASP Top 10.

- A web application scanner - able to identify vulnerabilities in custom applications
- Supports simple form-based authentication
- Supports assisted crawling (recordings)
- Scalable to cover expanding needs
- Certified PCI ASV scanning tool

In addition to the top 10, F-Secure Radar also refers to the 55 static categories of threat classification that are defined by the Web Application Security Consortium (WASC).

The WASC Threat Classification is a cooperative effort to clarify and organize different website security threats. The members of the Web Application Security Consortium have created the project to develop and promote industry-standard terminology, so that application developers, security professionals, software vendors, and compliance auditors have access to consistent language and definitions for web security-related issues.

Scan Node Agent

The Scan Node Agent is an F-Secure Radar component that manages all scanning processes running on the scan node.

It guards all scan jobs (the list of system, web, and discovery scans) and contacts Radar Security Center, checking whether there are any new scan jobs waiting in the queue. The Scan Node also has its own capacity, and knows how many simultaneous scans it can run at a given time based on the configuration.

Once a scan is finished, the Scan Node Agent sends the report back to the Security Center and removes all temporary scan data from the node, including the report and log for the scan. It is very important to note that the scan node does not store any vulnerability data after the scan has been completed. It is a Radar component that can be exchanged, by reinstalling, at any time when there are no ongoing scans.

The Scan Node Agent is run as a service in the operating system, and it's deployed and shipped together with an additional application for system admins that allows them to preview the scan node configuration and actual status of scan jobs, meaning the details of the scans currently running on the node.

Management

The Account management page allows you to control user access to Radar using Role Based Access Control (RBAC) principles. User management in Radar involves three concepts: Users, User groups, and Roles.

Users

The Account management page shows you a list of all users with access to your Radar account. On this page, you can review the users and what they have access to and, of course, add or remove users.

User groups

User groups act as containers for one or more users. With groups, you can control which scan groups users have access to and with what permissions (roles). The User groups column shows you which groups each listed user belongs to.

Roles

Roles are used to define the content a user can access. For example, you can create roles like "View only", "System owner" and "Administrator". To view and edit the roles for your Radar account, click the Account management menu button and select Manage roles.

Reporting

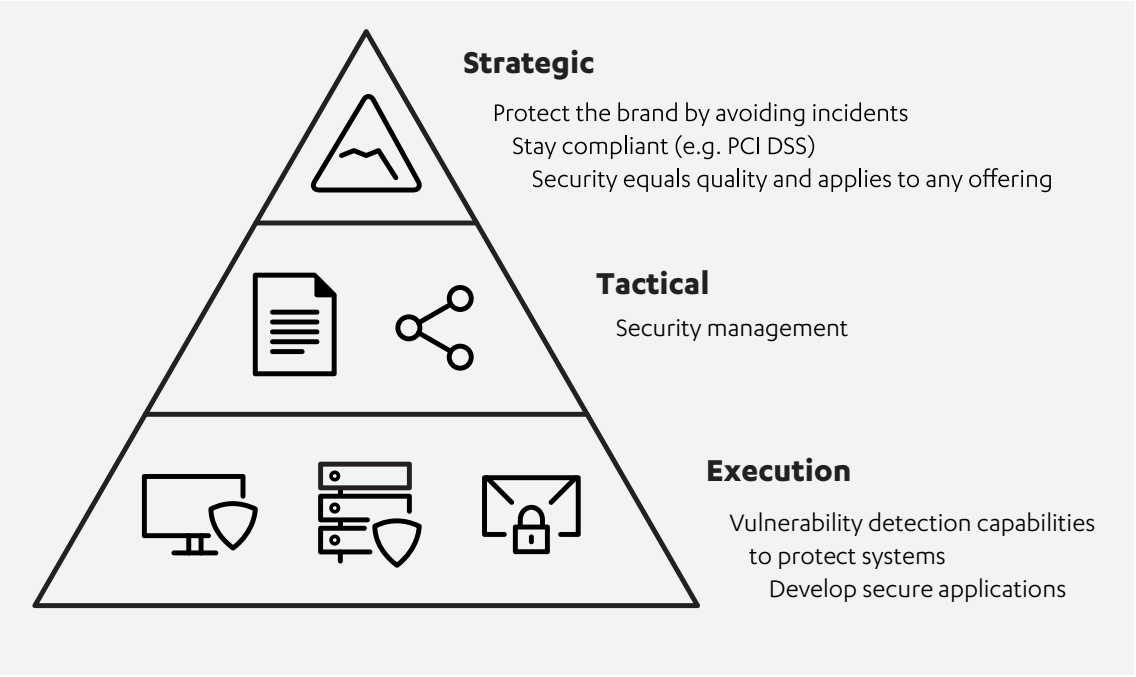
Reporting is another extremely vital part of the Radar Security Centre. With Radar, you can generate customized reports that suit the needs of your manager, system administrator, or your third-party service provider.

You can create your own report on the Reports page. Once the report is created, it is added to the list on the Summary Reports page. You can view each report in several formats:

- XML: Download the raw report data in XML format.
- Word report grouped by hosts: Contains all the technical details of the hosts in scope, organized by the host. This is useful when your scope does not cover a large number of hosts.
- Word report grouped by vulnerabilities: Contains all the technical details of the hosts in scope, organized by vulnerability type. This gives you a smaller report if the scope is very large.
- Excel report grouped by vulnerabilities: Contains all the technical details of the hosts in scope and gives you the freedom to use the features available in Excel.
- Word report, executive summary: Designed to be a light-weight report with few pages even if the summary report scope covers thousands of hosts.

Note: After generating a report, it creates a snapshot of the current state of your vulnerabilities. To update the report, click the menu icon in the actions column and select Refresh report data. Select Create a new report based on this if you do not want to overwrite the existing report.

VALUE PROPOSITION



Getting visibility into your environments

The biggest fears of any company include reputation damage, negative publicity, and the loss of trust due to incompetence or negligence. In addition to the above, other negative consequences include productivity loss, the disintegration of a firm's competitive edge due to stolen key intellectual property, and potential regulatory violations associated with the GDPRR.

What you need is visibility into the overlap between the vulnerabilities in your environments and the security holes being exploited in the wild. Furthermore, you need to focus on the vulnerabilities with the most impact to your business, and prioritize the issues in these environments first.

Complete threat management, done by F-Secure Radar

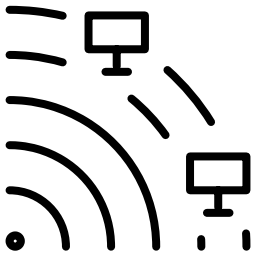
F-Secure Radar is a vulnerability scanning and management service operated by F-Secure Corporation. F-Secure Radar is available either as a cloud-based service (SaaS) solution or as an on-site solution. Radar consists of the following components:

- Radar scan nodes
- Radar Security Center

The scan nodes perform the actual scanning. The Security Center manages and coordinates the scan nodes, collects the results and provides reports of the findings.

F-Secure Radar detects weaknesses and threats immediately, boosting network and application security and ensuring regulatory compliance. Unparalleled central reporting and in-depth analysis effectively improve security management.

F-SECURE RADAR



Comprehensive visibility

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

Streamlined productivity and security management

Quickly address problems across multiple domains with an efficient service workflow, including vulnerability monitoring, automated scheduled scans, and ticketing for prioritized remediation and verification.

Streamlined security management

Simplified integration with an efficient service workflow and ticketing system that monitors vulnerabilities with automated scheduled scans, and assigns them for prioritized patching and coordination with system administrators (e.g. ServiceNow).

Reporting on risk

Produce reports with credible information about your organization's security posture over time. Show and justify how IT security enables business continuity.

Reduced costs

Vulnerability management can lower the cost of security significantly. It's less costly to deal with security before serious problems than during a crisis or incident recovery. Additionally, Radar's cloud resources allow organizations to lower their expenses.

Ensure compliance with current and future regulations

F-Secure Radar is compliant with the PCI ASV vulnerability scanning requirements. We are your EU-based partner that complies with EU regulations. When you use F-Secure Radar, you achieve compliance with an approved PCI ASV scanning solution and get PCI-compliant with a Qualified Security Assessor (QSA) partner. Carry out regular testing and identify new vulnerabilities. Generate user-friendly reports for all users.

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com | **twitter.com/fsecure** | **linkedin.com/f-secure**

F-Secure