- SECURELINK -

MANAGED SERVICES

EXTEND YOUR IT TEAM WITH PROVEN SECURITY EXPERTISE

WHITEPAPER

Secure Link | SAFELY ENABLING BUSINESS

TABLE OF CONTENTS

WHERE THE SHOE PINCHES 5

SECURELINK TO THE RESCUE! 6

IT IS ABOUT PEOPLE, PROCESS AND TECHNOLOGY! 6

WHY BUY A SERVICE? 6

SECURELINK SERVICES PORTFOLIO 7

SECUREINSIGHT SERVICES 8

SECUREPREVENT SERVICES 8

SECUREOPERATE SERVICES 9

SECUREDETECT SERVICES 10

SECURERESPOND SERVICES 11

SUMMARY 12

> The board of directors is becoming aware of the risks of security incidents and the impact that these can have on their business, brands, public image and even their financial results.

WHERE THE SHOE PINCHES

In any democratic society, privacy and cyber security are no longer a concern of the IT department alone. It is also the responsibility of the board of directors who are becoming aware of the risks of security incidents and the impact that these can have on their business, brands, public image and even their financial results. Therefore, it shouldn't come as a surprise that many companies are starting to take initiatives to improve their security posture.

Unfortunately, in most cases, they are soon faced with two major problems. They first face troubles starting because they wonder which initiatives will lead to a quick return on investment. Secondly, they are confronted with a lack of security expertise and resources. For many years, the demand for skilled security professionals has been much higher than the available resources in the market. Despite all good initiatives, the reality is disappointing: the already overburdened IT team must fit these security improvement projects into their already busy schedule, resulting in delays or unfinished and cancelled projects.

SECURELINK TO THE RESCUE!

As the leading European company in cyber security, SecureLink can help you make the right choices for your company and we can extend your own IT department with the required security expertise, 24/7 if necessary, through our managed services

This whitepaper will provide you with more details on SecureLink's portfolio of managed services, ranging from standard operate services to advanced security incident detection services that you can rely on to protect your organization effectively against today's threats.

IT IS ABOUT PEOPLE, PROCESS AND TECHNOLOGY!

Most organizations have invested the majority of their security budget into protection measures. Almost nothing went to the detection of and response to threats. No matter how much you invest in protection, you will never reach 100% coverage. It's even a certainty that you will get compromised at some point. How should you detect what you have missed and how should you respond accordingly?

The main challenges that need to be addressed to improve the detection of threats and breaches are:

- Lack of visibility of data stored in different silos;
- Lack of understanding regarding correlation and the complexity of enrichment and security analytics;
- Lack of resources when it comes to detecting threats.

This requires people, processes and technology that most companies do not have, cannot find or retain, or cannot afford to invest in. In an attempt to try and compensate for the lack of people, many organizations find themselves spending more on technology, hoping to achieve a higher degree of automation with less human analysis; however, this can only take you so far.

WHY BUY A SERVICE?

An increasing number of companies today choose to buy Managed Services. The main benefits of this approach are:

- Access to a larger team of experienced analysts with high level of skills and expertise on a 24x7 basis if required
- Global view of threats across geographies, industries and companies of all sizes
- Lower and more predictable monthly costs

SECURELINK SERVICES PORTFOLIO

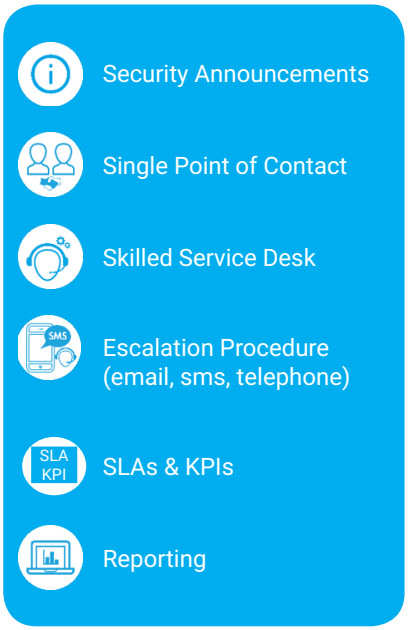
SecureLink has a broad portfolio of its own Managed Security Services. Many formulas are possible, all our services are classified in our Security Lifecycle.

The SecureLink Services

As a customer, you can choose to have multiple services simultaneously or you can pick them separately. Several items are common across all services, whatever combination you choose.

These are, among other:

- A single point of contact for all your questions, incident reporting, support cases, service requests, RMAs …
- Access to a team of specialists and this 24x7!
- Service Level Agreements (SLAs) and Key Performance Indicators (KPI) that allow SecureLink to measure and watch over the quality of the provided services
- Service reporting on a regular basis to discuss the measured results and adjust if necessary.



SECUREINSIGHT SERVICES

It all starts by understanding your risks and your current security posture. The SecureInsight Services will help you get actionable information about gaps, weaknesses and risks.

SecureLink will help you build an action plan and roadmap which will enable you to prioritize the improvements you need to make regarding your security posture and will help you maximize the outcome of your investments into cyber security.

Security Maturity Assessment

- Security Maturity Assessment
- GDPR Advisory
- Management Advisory
- Security Awareness Training

SecureInsight - Assess

- Penetration Testing
- Vulnerability Assessment
- Phishing Assessment
- Compromised Assessment
- Firewall Assessment

SecureInsight - Intelligence

- Global Threat Monitoring
- Targeted Threat Intelligence
- Digital Threat Management

SecureInsight Services are divided into three different areas:

SecureInsight Advisory
SeccureInsight Advisory is about gathering information that will help you with your overall security plan.

SecureInsight – Assess
These are services that will help you assess/verify your current security status across both technology and people, which offers an 'internal view'.

SecureInsight – Intelligence
These are services that will look at what is happening outside of your company and may impact your company's risks ('external view'). New vulnerabilities, leaked credentials, darknet discussions about your company, rogue apps or domains that try to impersonate yours etc.

SECUREPREVENT SERVICES

Prevention remains an important part of any security strategy. By choosing a strong endpoint protection solution and by actively scanning your devices for vulnerabilities, you can already prevent a lot of bad things from happening.

SecurePrevent Endpoint

- Managed next-gen endpoint protection service based on leading AV solutions

SecurePrevent Vulnerability Management

- Risk-based service that enables you to prioritize and measure your vulnerability management work.

SecurePrevent Endpoint
SecurePrevent Endpoint, is a managed service based on a next generation endpoint solution using artificial intelligence to detect and prevent threats on the endpoint. SecurePrevent Endpoint is a fully managed service from SecureLink that offers you the protection you need, while having a very low system impact.

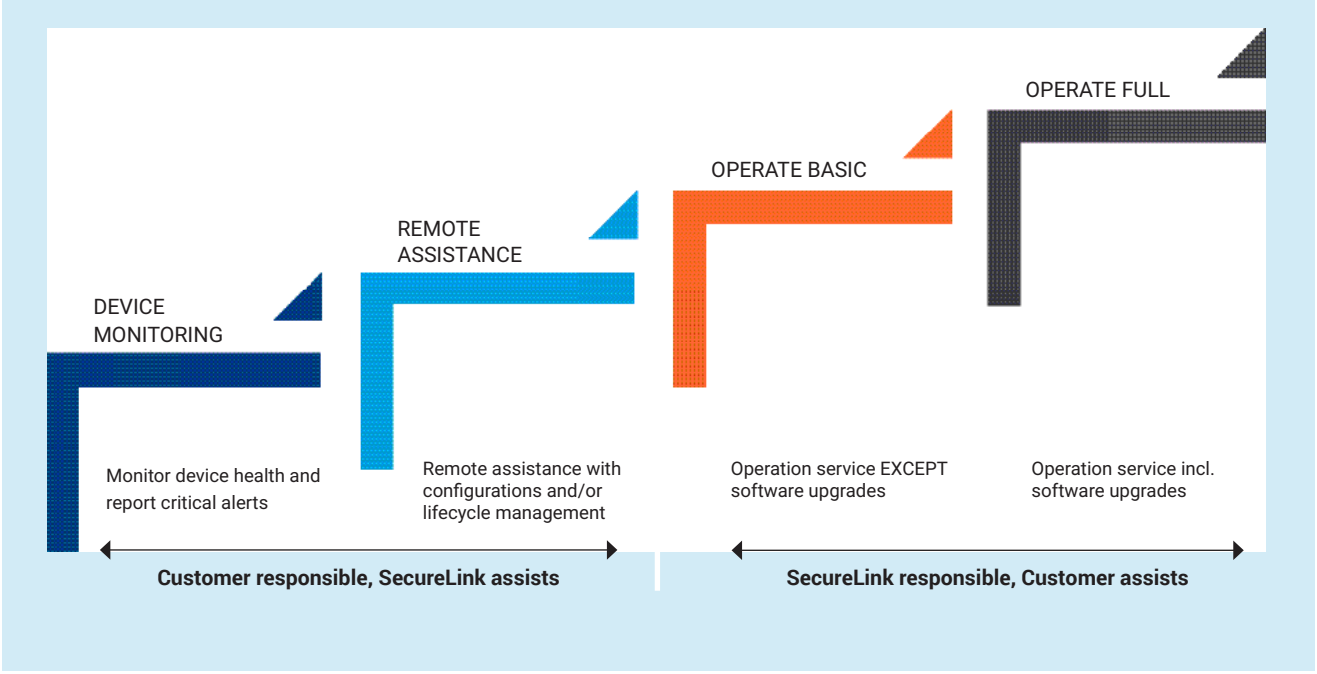
SecurePrevent Vulnerability Management
Through our experience, we have seen two big issues at our customers. The first one is that they do not scan for vulnerabilities in a consistent way. The second big issue is that the number of vulnerabilities is so massive that it is almost impossible to understand which one to prioritize.

SecurePrevent Vulnerability Management is a service that will take vulnerability scan data and enrich it with external threat intelligence based on current attacks in the wild, exploit-kits, malwares, and more to help provide a relevant risk-based view and recommendations for your vulnerabilities. This service is delivered through a portal to which internal stakeholders have access. This gives them visibility on workflows which enables them to prioritize and measure the vulnerability management work.

SECUREOPERATE SERVICES

The management and control of the complex infrastructure appears to be a true challenge for many organizations. SecureLink provides hands-on knowledge and expertise through our Network Operate Centers (NOC). Rely on specialists to manage your infrastructure; enabling you to focus on your core business.

SecureLink offers different types of operate services. Depending on your requirements you can choose for device monitoring and remote assistance or for a full managed service which includes resolution of incidents, execution of configuration changes and the installation of new firmware and software updates. All operate services are combined with solid Service Level Agreements (SLAs) that are reported on regular intervals and in line with industry standards such as the ITIL services framework.



SECUREDETECT SERVICES

Security is more than just installing the necessary security devices. It includes the continuous processing of the information from these devices. Our European Cyber Defence Centers (CDC) provide the 'security services glue' between all your infrastructure components. Security analysts and specialists monitor your infrastructure 24x7 so they can intervene immediately once your security is at risk. SecureDetect services are offered in three different flavours as we believe that there is not one single solution that will detect everything.

SecureDetect SIEM

- Detecting threats by managing, enriching, correlating and analyzing events

SecureDetect Network

- Detecting threats by deploying Network Traffic Analytics (NTA) sensors

SecureDetect Endpoint

- Detecting threats by analyzing behaviors on the endpoints

All our SecureDetect Services collect events from our customer's systems, enrich the events through threat intelligence, add context and then match it to a set of use cases regarding threat detection that are relevant for our customers and their environment. This provides a high detection rate and a low amount of false positive alerts.

The created indicators are then forwarded to the security analysts in our Cyber Defence Centers (CDC). They will analyse, verify and classify the incident, and then report back to our customers with information about the incident and recommended actions to mitigate it.

SecureDetect SIEM

Collecting and analysing logs is really a basic requirement for all customers. This is needed not only for threat detection, but also to comply with industry standards and other reasons like troubleshooting or performance monitoring by IT-operations teams.

You should really start with log collection, however, not all threats will generate a log. Network, OS and applications may not have been setup to log everything. If there are no logs, there is no way to detect it in the SIEM, and this is where our next service comes in.

SecureDetect Network

Network Traffic Analysis (NTA) is sometimes considered as the replacement of old legacy IDS systems. It resides on the network and applies rules and machine-learning to the traffic. That way, it can detect threats that do not trigger logs and that do not have any endpoint detection agents installed (ex: Printers, IoT…).

However, a big part of the traffic today is encrypted. This makes it harder to profile and detect threats on the network and makes impossible to detect what is happening within an endpoint (ex: Privilege escalations etc…). This brings us to our third service.

SecureDetect Endpoint

EDR (Endpoint Detection & Response) is a specific part of endpoint security that focuses on recording all activities and detects risky behaviours. It enables visibility and remediation of local threats that are very hard to detect using logs or network traffic. EDR is a very powerful service but requires a lot of resources and expertise in order to be advantageous and sort out the true positives from the false positives.

SECURERESPOND SERVICES

After you have detected a threat, you need to make sure to respond in an adequate way. A fast detection and response minimizes the negative impact and therefore reduces costs. At SecureLink, we help you build a solid Incident Response Strategy.

Not all customers have a 24x7 CSIRT team or the capability to reverse engineer malware or perform digital forensics and incident response work.

The goal of the SecureRespond Services is to help our customers in this domain.

SecureRespond Quarantine
- Limit the impact of a detected breach by intervening quickly

SecureRespond Malware
- Analyzing suspicious files to perform in-depth analysis

SecureRespond Incident
- Rapid remote forensics
- Incident retainer services with onsite SLAs

SecureRespond Quarantine

This is an add-on service to the SecureDetect Services. It will make sure that when the Cyber Defence Center detects an infected endpoint, this endpoint can be isolated from the network to limit its ability to do callbacks and lateral movement.

SecureRespond Malware

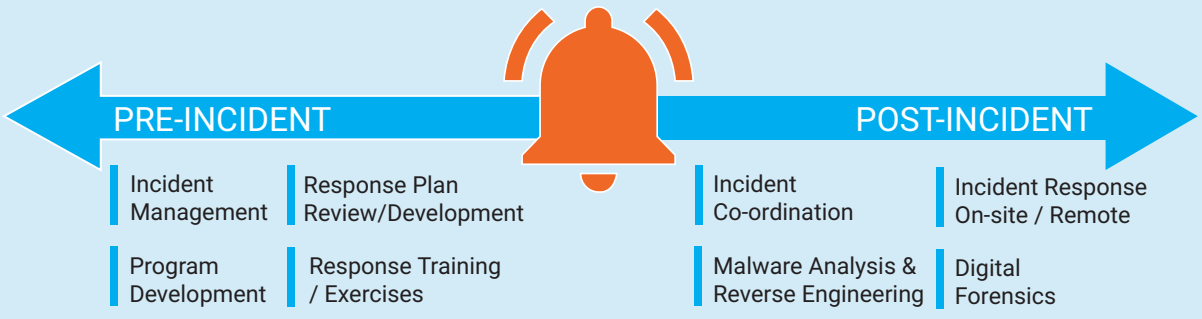
SecureRespond Malware Analysis Service uses a combination of static and dynamic analysis on submitted malware and can help you with:

- Analytics of what the malware tries to do;
- Identification about where it comes from (targeted or not);
- Collection of IOC to identify other breached endpoints

SecureRespond Incident

SecureLink offers several different levels of incident response services that help you with a wide range of topics from initial breach notification reports (GDPR requirement) based on remote forensics, to full onsite incident response with SLAs by our CREST certified incident responders.

Preparation is key when it comes to incident response. We can assess your current processes or build new ones. Checking your incident response plan upfront – gives you a head start when a real incident occurs.

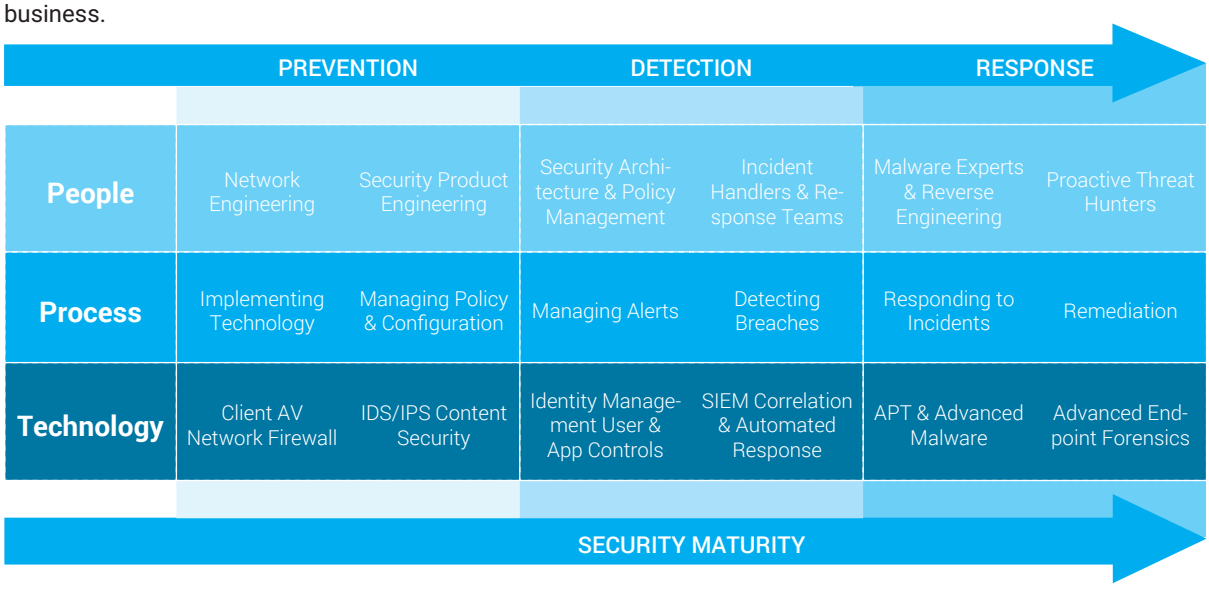


SUMMARY

Making substantial investments to build your own Cyber Defense Center and staffing it with skilled analysts is something which is only affordable for large enterprises. By subscribing to our Managed Services, these advanced protection services become available to all companies

SecureLink's services help your organization with detecting, preventing and responding to data breaches. You will be able to make the appropriate decisions when responding to these breaches.

We are cyber security specialists. We empower organizations to protect themselves in an increasingly online world so they can maintain the trust and confidence of their customers. In short, security incident detection and response are key components that should be incorporated in your cyber security strategy in order to safely your business.



Do you have a question, comment or are you looking for more information about **SecureLink's Managed Services?** Ask our SecureLink Experts.

Author Peter Beerten
Business Developer Managed Services @ SecureLink
Mobile: +32 496 50 93 94 | peter.beerten@securelink.be

@SecureLinkBe SecureLink Belgium

SECURELINK

Safely Enabling Business

SecureLink specializes in the design, the implementation and the support of the most reliable and innovative networking, virtualization, security and data center infrastructure solutions. Over the years, we have become one of the largest Pan-European cyber security integrators.

We offer more than just advanced technology; we are also service providers who offer vendor-independent advice. Thanks to our extended security expertise, we are able to solve the most complex cyber security challenges.

Our experience in Managed Security Services offers you security and continuity. The SecureLink cybersecurity specialists are available 24/7 to assist you from the Cyber Defense Center. Our experts are known for their results-oriented, no-nonsense approach and strong expertise.

SecureLink's know-how, passion and personal customer approach result in an innovative service, high customer satisfaction and acknowledgement from the most renowned vendors in the industry. We safely enable your business.

Fields of expertise:

- SecureWorkspace
- Virtualization
- Next Generation Security Gateways
- Endpoint Security
- Proxy Security Gateways
- Managed Services
- Dynamic Network Access Control
- Core Network Services; Secure Infrastructure
- Visibility & Analytics
- Cloud Security

We offer more than just advanced technology; we are also service providers who offer vendor-independent advice. Thanks to our extended security expertise, we are able to solve the most complex cyber security challenges.