Vision 2021
Breaking Barriers

Orange Cyberdefense

Introduction

Definitely 2020 was a remarkable year, and one not to forget soon. As the government imposed measures and restrictions due to the COVID pandemic, an accelerated digital transformation happened for most organizations. Different ways of working, different ways of doing business and new opportunities were thrown (unsolicited) into our lap.

Our last year's vision talked about "there is more to secure" and being cyber smart, and yes we were right in saying that, without knowing that the security of the digital workforce would be top priority of many organizations during the shift to work from home as the standard.

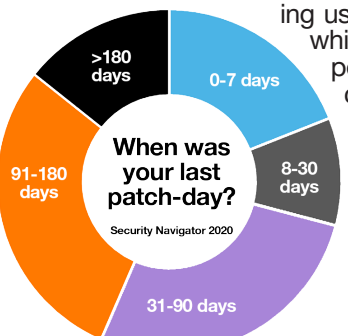
The percentage of companies with a majority of employees working remotely tripled from 21% before COVID-19 to 70% after. And 40% of the companies are permanently keeping a large scale of workers remote and most likely will close down offices.

The business and the threat landscape adapted quickly as well, which brought even more complexity and challenges which also need to be addressed. Forrester has investigated and repeated in one of their recent reports that the biggest security challenge for an organization still is the complexity of the IT environment.

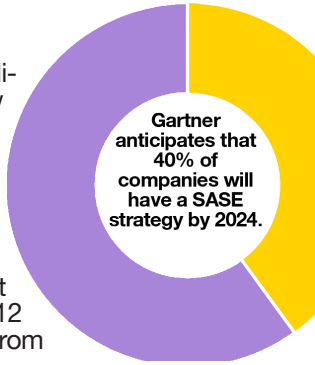
In this vision document we will guide you to break barriers with adopting the right solutions and services to strengthen your critical control points in order to continuously reduce the attack surface. It is not just about introducing new technologies, it is mainly about emphasizing the importance and adopt early on the future frameworks/architectures. All insights are meant as a strong guidance and input for the cyber security program in your organization.

Recent observations

With the massive migration of services towards the cloud (public and private), the dispersed workforce, we basically can state that the internet is the new corporate network. For the last decades, networks have been connecting users to applications in the datacenter, which both were surrounded by a secure perimeter utilizing multiple security controls to keep users, applications and data safe from the outside. This notion of network security is no longer viable in the new mesh connected digital world.



Actually, the above requires a more radical change and an embracement of new models like Secure Access Service Edge (SASE) or Zero Trust Edge (ZTE).



In our recent extensive security navigator report, we share a lot of our research results and valuable insight information about the evolving threat landscape and vulnerabilities of the last 12 months. You can download your copy from our website.

Credential theft, human errors and social attacks are the three most common culprits in breaches. Employees working from home could be particularly vulnerable to these attacks. In these uncertain times, it makes sense to focus on prevention efforts here. In the Verizon DBIR2020 it is stated that the human error is the root cause in almost 95% of the breaches.

Break barriers into the future

In this vision document you can conclude that things change rapidly, and discuss whether your organization can keep the pace on consuming the new necessarily cybersecurity solutions.

But, while continuing the digital transformation, the same security basics still need to be applied: the fundamentals of zero trust. It is all about protecting your data, managing identities, securing applications, endpoints and access.

Likewise, as security professionals, we know that ensuring the confidentiality, integrity and availability of your assets are key security concepts. They are foundational of any of good security practice.

A quick adoption of innovative frameworks or models in your blueprint or roadmap is our advice to become agile and stay cyber resilient. This requires CISO and lead architects involvement during the discussion that involves acquiring or transforming the networking security solution.

Themes or frameworks like: The borderless enterprise, Secure Access Service Edge (SASE), Zero Trust Edge (ZTE), Intelligence led security, Intrinsic security, the connected factory, eXtended Detection and Response (XDR) definitely need to be considered, discussed and evaluated within every organization.

Social engineering & home office

Various research and blogpost mentioned an unprecedented high number of attacks that link up with the corona virus and working from home. We have seen an emerging trend of credential phishing, malware, Business email compromise (BEC) and social engineering lures around COVID-19.

Threat actors have launched coronavirus campaigns to spread remote access trojans (RATs), keyloggers, information stealers, and bankers. It is important to take pre-emptive steps to ensure the resiliency and security of your organization's operations as attackers seek to exploit human courteous or careless behaviour. Gartner describes in one of their analyst reports the 7 focus areas to protect your people and organization from risk.

7 Focus areas

1. Ensure the organization's Incident response protocols reflect the altered operating conditions and are tested early;
2. Ensure all remote access capabilities are tested, secure and endpoints used by workers are patched
3. Reinforce the need for remote workers to remain vigilant to socially engineered attacks
4. Ensure security monitoring capabilities are tuned to have visibility of the expanded operating environment
5. Engage with security services vendors to evaluate impacts to the security supply chain
6. Account for cyber-physical systems security challenges
7. Don't forget employee information and privacy

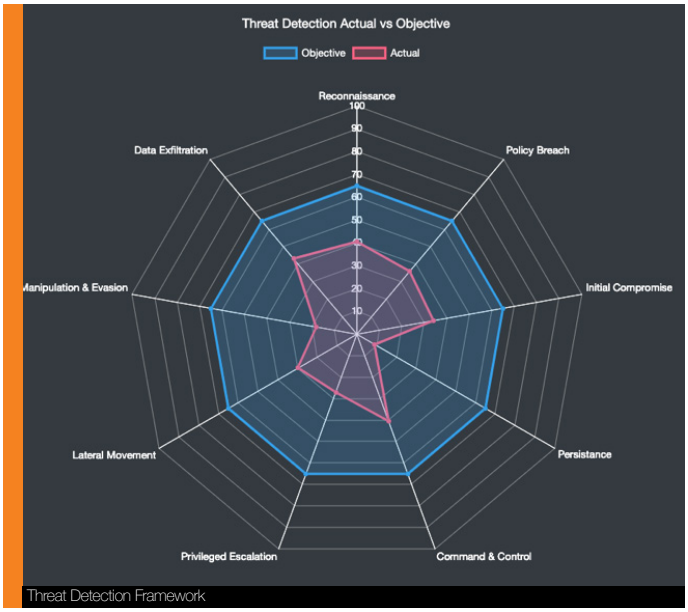
The borderless enterprise

Your organization wants to embrace the cloud and all its benefits—yet you need a simpler, more reliable way to manage your network, devices, apps and services across all locations. How can you solve networking challenges at the edge with fewer enterprise resources and offer the required user experience?

As employees become more dispersed and remote—data and services are being accessed more and more in the cloud—the network perimeter is vanishing. Multi-cloud and cloud-first networking have created a borderless enterprise.

The challenge? Traditional networking architectures no longer work. The "modern" distributed network must now offer an edge user experience that mirrors on-premise, while network managers have to transition how they manage the exploding demand for services anywhere, at any time.

SASE or ZTE mandates the "thin branch" and "heavy cloud" with a light IT footprint in remote locations, e.g., an SD-WAN router and all security services provided inline (and nearby) in the cloud. The benefits of this approach are lower TCO, less latency, consistent security policies, significant threat surface reduction and no congestion point.



Threat Detection Framework

The adoption journey towards the borderless enterprise can be challenging and requires a phased approach that is likely to take several years. My advice is to get started and discuss this journey with the CISO and lead architects.

Intelligence led security & Threat detection framework

You cannot protect against the unknown. Everything starts with the threat! If we do not understand the threat-characteristics, we cannot understand how to identify the threat, nor how to detect the threats in your infrastructure or how to effectively build protections against them. But just the threat isn't everything. Real intelligence led security requires a view to the security environment through multiple lenses (understand the total environment – attack surface, IT assets, vulnerabilities, user behaviour and more).

My definition of a intelligence led security is: "Leveraging actionable context-based intelligence for a proactive cyber defense posture to reduce risk."

WorldWatch service
World Watch is the process and product through which we produce and distribute tactical security intelligence to our customers.

It sounds not too complex, but it really requires the right tools, organization, knowledge and insights to apply the right filters on all available information (from threat researchers and various threat intel sources) to get to the right actionable and usable intelligence.

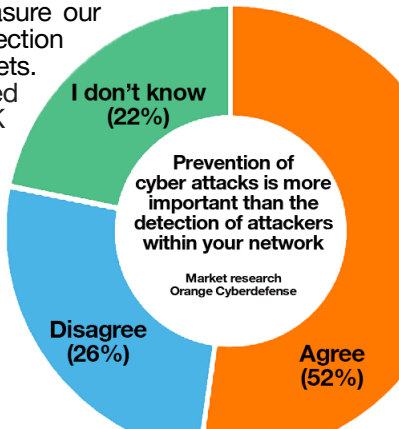
We have provided intelligence led security services to several organizations and experience from that strengthens our vision that organizations will increasingly be looking for Managed Detection and Response services (MDR).

Last year, we mentioned the security operations and analytics platform architecture (SOAPA) from the Enterprise Security Group (ESG). The architecture being used within our CyberSOC for MDR services is in a way a SOAPA. It includes SIEM and a combination of our own, EDR (endpoint), NDR (network) tooling, threat intelligence, vulnerability scanners and incident response services. Additional capabilities known in the market as UEBA and SOAR helps to automate tasks and reduce the manual interaction. Our pattern-based detection model is an example of such an innovation that serves automated continuous detection.

Security remediation operations can also be orchestrated to take actions across multiple security controls, such as security gateways, network proxies, web or DNS gateways, etc.

Based on the platform, the experience and full SOC Triad services with experienced security analysts across Europe, Gartner recognized us as one of the representative vendors in the Managed Detection and Response services market in their latest report of August 2020. With attackers operating nonstop, you can't afford not to have an MDR service.

The threat detection framework is our continuous baseline in which we measure our customers' visibility and detection capabilities against their targets. By applying industry recognized standards like the MITRE ATT&CK framework in combination with our operational knowledge, we designed a score system that stretches across all phases of the attack lifecycle. This gives a visualization of your capability to detect attacks, based



on the actual/current deployment of detection tools in your environment.

Business continuity

Managing through a cyber incident, recovering your business, and regaining normal operations requires practice and a lot of planning. In addition to good backups, impact analysis, documenting critical business functions and regular testing (preferably automated) needs to occur to ensure disaster recovery groups are ready to manage these kinds of incidents.

While getting up and running is crucial, it is just as important to effectively communicate with internal and external stakeholders during a cyber crisis. Who should be involved, which roles are needed, who decides when external help is required, who has the mandate, who communicates with the press, who reports the breach, etc.

Our expert consultants can help fast-track your business continuity program maturity with service options including:

- Maturity roadmap
- Business Impact Analysis (BIA)
- Threat and vulnerability assessment
- Recovery Point Objective/Recovery Time Objective (RTO/RPO) documentation
- Interview business owners

Take business continuity with regards to cybersecurity very seriously.

Visibility in encrypted environments

How do you maintain security visibility in the new encrypted world? The increase in encryption between the browser and the rest of the internet causes some problems (to say the least) for network security controls. Especially the adoption of TLS 1.3 (which is roughly about 37% right now) is growing at a much higher rate than TLS 1.2 did in the past. Another evolution that makes a lot of security controls less effective is the use of DNS over HTTPS (DoH) or DNS over TLS (DoT) and Encrypted SNI. These new privacy protocols remove the metadata that is being used by almost every security control in the current infrastructure knowing where the traffic is going to or where it is coming from (based on reputation scores, URL filtering, DNS filtering and Threat intel).

Enterprise advice

- Block TLS 1.3 until you can reliably intercept it (your security gateway will get there);
- Decrypt HTTPS traffic or block DoH traffic between internal IP addresses and external DNS servers, forcing employees to use the by IT-managed DNS infrastructure and ensuring that security policies are enforced;
- Block encrypted SNI for now. There is no good reason your employees should be using it through your network.

My estimate is that there is a two-year window that need to be bridged before an enterprise ready solution will be widely available. Next to the business advises (in the textbox), it is important to have endpoint security and email security at the right level of course.

We understand that some of the business advises can lead to privacy discussions, but the benefits of the deployed security controls are also required to safely enable your business.

Endpoint Security

Endpoint security has never been so important. It can easily be the headline of this document. With the acceleration of the digital transformation, combined with the “new normal”, encryption and the uptick of breaches and vulnerabilities, it is needless to say the control on the endpoint is crucial. Endpoint management, protection, detection and incident response need to be addressed and incorporated in the CyberSOC operations.

DLP on the endpoint is a true requirement, and since most endpoint solutions don’t include DLP per se, they do examine exfiltration (data theft), that will become visible as part of the detection and response dashboard.

End-to-end user experience

The new way of working, using the new technologies to select the most optimal path between the user and the data should lead to an optimal user experience independent of time of the day, role or location.

With our extensive portfolio of solutions and our improved telemetry and growing number measurable metrics on our platforms, we are advancing towards combining this data that will give us an indication of the performance of our service, end-to-end. We will start the discussion with you on how to package these metrics in order to guarantee you the user experience on our services in the form of an end-to-end SLA.

This is obviously a customer requirement when it comes to architectural or security services. Think of it as getting a service using the mini-platform architecture, but with SLA’s and KPI’s over the whole solution.

Core network services cloud based include threat defense. Enterprises are eagerly embracing the cloud for its agility, elastic scalability, and cost efficiency. In order to enjoy all those benefits, the core network services that make cloud interactions possible need to be as agile, scalable and efficient as the cloud itself. Core Networks Services has often been a topic in our yearly vision, and these services have traditionally been built as a dedicated and easy to manage and operate platform offering the necessary availability and capacity.

The evolution as described above, requires a scalable platform that provides DNS, DHCP, IP Address Management (DDI) and security capabilities (DNS security & threat intel) in the form of services and apps managed through the cloud. This way organizations are no longer constrained by factory-delivered hardware. They are instead empowered to consume services or personalize solutions as the circumstances dictate.

A unified foundation for today’s modern, cloud-powered environment as a 100% cloud-native, cloud-managed platform based on microservices and container-based architectures can be offered. It radically transforms your ability to simplify and automate networking and security across diverse multi-cloud infrastructure, streamline operations, accelerate DevOps and launch new applications at cloud speed.

DDI and DNS security are critical core services in any environment. The cloud-based approach is the foundation for any future architecture, where still some services can run on-premise when required.

OT security & Identity of Things

Due to the ‘digital transformation’, ‘Smart Manufacturing’ and ‘Industry 4.0’, companies are increasingly opening up the OT domain towards the IT domain, with the aim of process optimization, efficiency and extensive analysis of process data. The pressure or importance to get the

factory connected could be bigger than the adequate protection against cybersecurity attacks. This risk exposure can lead to unavailability or financial/physical damage.
The connected factories are a massive domain with a lot of connected devices where basic security controls are often lacking. Most industrial environments have legacy devices that are difficult to patch and are developed many years ago when security was not a primary design principle.

“We advise a phased approach to continuously reduce critical infrastructure risk with zero impact to operations.”

OT security will be mentioned regularly by many vendors and integrators, but to not make the mistake by solving actual issues with point solutions, the approach also requires a strategy and a framework to cooperative work towards the most efficient solution to address the security challenges for the connected factory.
Larger companies will definitely continue to work on securing their OT domain in 2021. Medium-sized businesses are most likely not ready for this yet and will not follow until a few years from now. As a result, cybersecurity incidents will occur especially there.

Assessing advisories and adopting standards like IEC62443 and NIST 800-82 are crucial. Due to alerts like the AA20-205A, awareness and call to action should get the highest priority within organizations that deal with an industrial environment. The in June 2020 discovered Ripple20 vulnerabilities once again endorse the importance of security in the (I) OT environment.

We advise a phased approach to continuously reducing critical infrastructure risk with zero impact to operations. This starts with visibility and context of the assets (identity of things) and securing the demarcation points in the architecture (and adding detection and response capabilities).

Cloud security

If the pandemic teaches us anything, it is that our approach guarding data needs to change. Within many companies, this data was locked into vaults with barriers and perimeter security. This all changed as the digital transformation is kicked into high gear and people started working from home. Enterprises need the data to be fluid, but still guarded. The adoption of cloud based application gateways and (sanctioned) SAAS exploded with security lacking. You need to add the necessary security to stop data leakage before it happens. Also the risk of using unsanctioned cloud applications need to be identified and mitigated.

Deploying cloud environments and building cloud applications using modern or cloud native (micro)services or based on containers requires to include security measures from the start. Things like “shift left”, micro-segmentation and policies on workload or process level based on tags/labels make it agile and flexile as it should be to reduce the attack surface and avoid human mistakes.

Cloud Security Posture Management (CSPM), automates governance across multi-cloud assets and services including visualization and assessment of security posture, misconfiguration detection, and enforcement of security best practices and compliance frameworks.

In combination with context aware authentication, your enterprise will enjoy unrivaled security and end-to-end protection of any cloud experience.

Breaking through barriers

The process of being safer every day and to securely enable the digital transformation requires a plan, a strategy and a roadmap.Based on the risks, the architecture for prevention, detection and response must be made and followed.

This is an ongoing and dynamic process that requires smart decisions and a well-experienced strong partner.

Identify and execute on the right next steps in breaking through barriers in your organization for 2021.

Breaking barriers when it comes to cyber for 2021.

**Peter Mesker CTO &
Solutions Architects, Orange
Cyberdefense Netherlands**