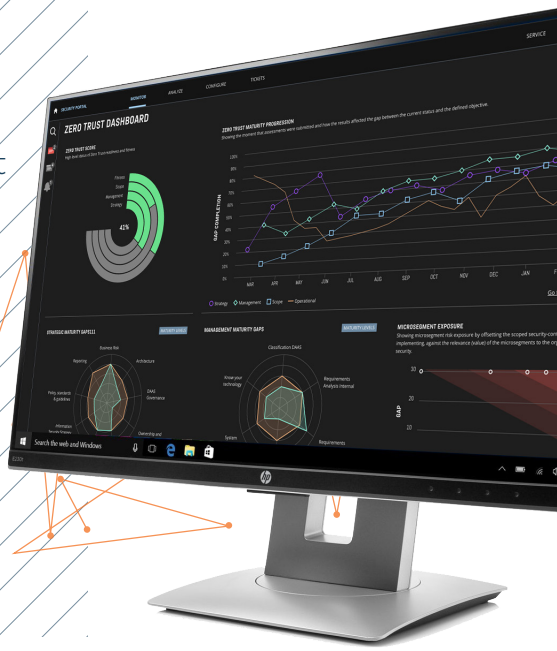
ON2IT Customer Cases: **health care**

CUSTOMER PROFILE This general hospital has 3,700 employees, 1,600 of which are medical professionals. Annual revenue in 2019 totalled 380 million dollars and the number of patients per year was 60,000. The annual IT-budget totals 19.8 million dollars, with staffing (32%) and software (32%) as the major cost categories. The 2019 budget for networking and data was 1.8 million dollars.

In 2016, the hospital embarked on a plan to modernize the EHR and the IT-infrastructure. All critical applications had been run in an on-premise datacenter, with a backup facility shared with several regional hospitals.



THE CHALLENGE

The Information Security Manager and an outside management consultancy firm drafted a board advisory in 2019, which, among other recommendations, concluded that the cost of the internal SIEM system (licenses, hardware, services, education) was prohibitive. The skills and capacity to maintain this system 24/7 was beyond the capacity of the hospital's IT-department.

THE SOLUTION

SOC-as-a-Service

"As part of our infrastructure upgrade we decided to replace our previous generation firewalls with Palo Alto Networks NGFW's. ON2IT was initially in scope only as an implementation and maintenance partner for these devices. But during our discussion, we learned more about their Zero Trust approach and specifically about their managed solution detection and response (MDR) and prevention and compliance (MPC).

Following a presentation to our board, they proposed replacing the older SIEM solution with their managed SOC. Their cloud-based software service includes all the security functions we require in a SIEM. All security events generated by our firewalls, endpoint software (at that time Traps, which is now called Cortex Prevent) and cloud management software are enriched and evaluated by the ON2IT EventFlow engine. The ON2IT SOC-engineers research all incidents requiring human inspection. Depending on protocol, they can either mitigate threats, or escalate critical cases to our IT-department contact on duty."

Outcome

"Replacing our internally run SIEM with a predictable managed OPEX-model, we have been able to free up our heavily strained IT-staff for other projects and in the process cut our cost for outside IT-consultants who were required to run these other projects. So the cost advantage is important. Just as important, we can now be confident that we have access to experienced and well-trained security professionals. I'm convinced that for organizations of our size (around 3,700 FTE), it's economically and practically impossible to run a 24/7 SOC in house. It's just not our business; we can't attract and keep top-talent."

The best remediation is no remediation:

From a security perspective, the most important outcome is that ON2IT considers MDR and threat hunting as not just a goal, but as a tool to build better prevention.

"By continuously validating policies against best practices and the requirements of our specific compliance frameworks, we are actually building a better security posture. Before ON2IT, most of our security measures were infrequently evaluated. Some of them were really just a tick-box in the annual auditor report. With ON2IT, learnings from security events are used to continuously evaluate and update policies and measures. We like their vision of the continuous audit. We process highly sensitive and personal data, and we feel that privacy and cybersecurity are an integral part of what constitutes good healthcare.

We consider the ON2IT consultants and SOC-engineers to be a proactive extension of our inhouse IT-team, offering policy advice, security advisories and a way to keep abreast of new risks and technologies."

ON2IT Customer Cases: **manufacturing**

CUSTOMER PROFILE This global manufacturer operates production locations in more than 40 countries, employing 12,000 people worldwide. It has customers in more than 100 countries. Its 2019 revenue was close to 2.3 billion dollars.

ON2IT has installed on-premise Next Generation firewalls on all global locations, as well as in the data center, as part of their full-service managed solution.

THE CHALLENGE

The group went through a period of rapid growth by a series of acquisitions. They were faced with a patchwork of security solutions, technologies and vendors. “We were finding ourselves stuck in a situation where most of our security was “incident driven”, the CIO says. "Rather than be prepared for whatever security threat would come our way, we were finding ourselves having to react on the spot. There was no time to develop and implement an overall global solution."

They realized that, with a company their size, the IT team or staff was simply not big enough to handle these security issues, especially since it was never meant to be their core competence.

THE SOLUTION
Managed Security Services

A complete overhaul of the company’s security was set in motion, starting with ON2IT’s ‘fresh eyes’, evaluating their data and understanding which data was most valuable. “I first heard about the Zero Trust strategy at a meeting where John Kindervag was the keynote speaker. The concept immediately made sense to us, and we realized it could be a guiding light to structure our approach to cybersecurity across all our facilities.”

The CIO told his team that they need outside eyes. ON2IT plays the part of the outsider with a vast amount of IT security knowledge, which helps companies view their security infrastructure in new ways. This outside experience works in two ways. “First, it is pointless and even dangerous to design a Zero Trust architecture in a relatively short time if you don’t have the experience of dozens of implementations under your belt. We have our skills, ON2IT has theirs. Equally important: a trusted outside consultant can help a CIO ‘convince’ colleagues around the globe that they must adopt a new way of thinking about cybersecurity.”

“ Companies like ON2IT know what they’re doing; they've been doing this for many years. They know exactly what kind of tech solutions you need. ”

Due to the company’s limited number of IT staff, ON2IT was put in charge of the Zero Trust architecture design, the global implementation of firewalls, segmentation and policies as well as 24/7 monitoring, detection and remediation. “We have limited people. We need a partner for that. Without them? Mission impossible. An added bonus is that the IT staff is happy they now have more time for focusing on their core competences.”

ON2IT has installed on-premise Next Generation firewalls on all global locations, as well as in the data center as part of their full-service managed solution. This saves bandwidth and cost by offloading internet traffic locally. The security was further optimized by inspecting the data traffic between the legacy and global IT and also by placing the internet traffic locally under one central policy. The service was expanded to include SaaS (O365/ OneDrive) inspection to inspect and relocate data to the cloud.

The endpoints have all been provided with the ON2IT managed endpoint solution for better cross-platform inspection and to minimize risk and impact at the smallest level.

“My message to other companies is: get help with your security. Companies like ON2IT know what they’re doing; they've been doing this for many years. They know exactly what kind of tech solutions you need, and have practical experience with legal requirements and industry-specific compliance frameworks.”

Outcome

“We’re now using a future-proof architecture across the whole group. We've found that the Zero Trust principles work equally well in SD-WAN and cloud environments as they did in the corporate data center. Our IT-staff is happy that they can spend their time on tasks that immediately contribute to our core business. And most importantly: we've not had a severe incident since the overhaul of our cybersecurity.”

ON2IT Customer Cases: **local government**

CUSTOMER PROFILE As a municipality undergoing major changes, this city was looking to set up a flexible network infrastructure, with scalable network port capacity and optimal IT security. With a population of 123,000 and 1130 employees, there was a lot of ground to cover.

THE CHALLENGE

The municipality was facing two basic problems: navigating a multiple location set up; that their IT service management was in-house. "Fixing and replacing hardware was something we had to do ourselves. This meant that we regularly had to drop everything to resolve issues. Obviously, that's annoying when you're in the middle of a project or meeting. We were therefore looking for a partner who could take this off our hands."

They were also interested in an upgrade to a secure data center and secure network, as well as an option to up- and downscale network capacity. "Our old network infrastructure was built at multiple locations. In recent years we've closed a number of branches and as a result, some of the hardware (switches) had become redundant. When developing a new network, it was important to us that we could easily match the network capacity to our needs."

THE SOLUTION

SOC-as-a-Service

ON2IT offered a solution including a virtual network based on Zero Trust (VMWare NSX), a flexible network service based on capacity subscriptions and a managed security monitoring and policy service. "What's special about ON2IT's solution is that they see the network and IT security as a whole. They start with IT security and build the network around it."

With around 3000 network ports in use across the municipality, some of which were at locations no longer in use, it was important for the municipality to be able to scale their network ports both up and down. "With our new network infrastructure, we can scale up and down network ports depending on capacity requirements. We pay a fixed price per port and not for unnecessary capacity."

" What's special about ON2IT's solution is that they see the network and IT security as a whole. They start with IT security and build the network around it. "

Instead of the municipality's own IT department monitoring all the resources and hardware, ON2IT's SOC now monitors it all for them. The SOC maintains the hardware, monitors the network traffic and performs policy management from ON2IT's SOC location. "In ON2IT we found a strategic implementation partner that at the same time takes the 'fix and replace' part out of our hands."

All employees of the municipality will soon switch to 'the new way of working'. They can work from any laptop, tablet or from a fixed or mobile workplace and will always be connected. Using Palo Alto Networks Prisma AccessGlobal, they are always connected safely.

Zero Trust Innovator **CYMBEL**

Cymbel's full support for Palo Alto Networks technology reflects the importance of true cybersecurity innovation in our DNA.

Combining machine learning, advanced threat intel and enriched clients' security events data, we help our clients build and implement improved managed security polices and measures. We believe detection and incident response are ineffective without a 24/7 focus on prevention and compliance.

Cymbel Corporation Headquarters / 154 Wells Avenue / Newton, Massachusetts 02459
E-mail: sales@cymbel.com / Phone: (617) 581-6633 / Fax: (617) 581-6637