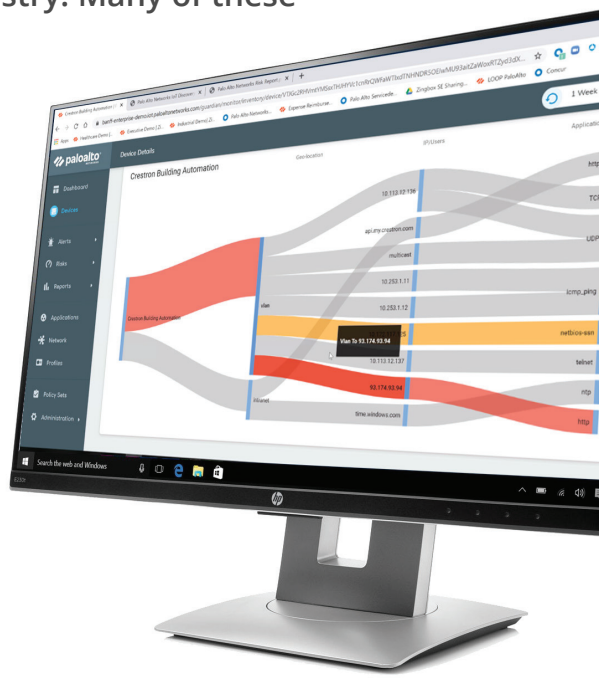
THE ON2IT IOT REACH AND RISK ASSESSMENT

A QUICK SCAN OF YOUR IOT SECURITY POSTURE

We know from experience how difficult it is to stay on top of the explosion of intelligent devices in your network, regardless of your industry. Many of these devices don't pop up on the cybersecurity radar.

At the same time, IoT is literally everywhere, from your security cameras bought from Alibaba, to the robots in the car factory, the blood pressure monitors in the hospital or the smart TVs at the office and in your living room. Our IoT Reach and Risk Assessment gives you an IoT overview.



THE CHALLENGE

IoT is everywhere

In most enterprises today, more than 30% of all network-connected endpoints are IoT devices. These are projected to keep growing. A report by Gartner predicts adoption of IoT endpoints worldwide to soar to 5.81 billion this year.

Security teams are already tasked with protecting IoT endpoints connected to a company's network. Under the new normal—with the exciting new concept of IoT in control—they also have to contend with challenges arising from the increasing prevalence IoT devices connected to an enterprise's central network.

In short, the main IoT security challenges are:

- **Inventory:** not having a thorough understanding of which IoT devices there are in the network and how to keep track of new ones;
- **Threats:** a lack of well embedded security in IoT device operating systems that are hard or impossible to patch;
- **Data volume:** overseeing vast amounts of data generated from both managed and unmanaged IoT devices;
- **Ownership:** new risks associated with management of IoT devices by various teams within the organization;
- **Diversity:** the sheer diversity of IoT devices in terms of their limitless forms and functions;
- **Operations:** the unification crisis in which IoT devices are critical to core operations yet difficult for IT to integrate into a core security posture.

What are the must-haves of a good IoT security solution?

IoT did not appear out of the blue, and in many ways, it falls in line with the strategy and measures we use for 'regular' IT and OT every day. This applies to our own data center as well as in the cloud.

Furthermore, cybersecurity companies have in recent years added specific IoT security solutions to their portfolio.

Your IOT security solution must provide:

- **Complete visibility into all IoT devices connected to the enterprise**
  It is important to have full visibility into your IoT attack surface. This is where your IoT security lifecycle begins. To understand your IoT assets, employ device discovery for complete visibility.
- **Proactive monitoring of IoT devices to continually detect risky behavior**
  Your solution must always actively monitor IoT devices. Real-time monitoring, reporting, and alerting are crucial for an organization's management of IoT risks.

THE ON2IT REACH AND RISK ASSESSMENT PROVIDES INSIGHT INTO:

- The number of IoT devices in your network;
- The vulnerabilities and the risks;
- The effectiveness of your current security measures;
- Detected malware / malicious activity.

Our report provides your devices with risk profiles and insight into known vulnerabilities. this enables us to help you determine the priorities within the organization.

After the scan, we send you our Executive Report and we provide you with the findings through a PowerPoint Presentation.

This report provides insight into your IoT devices, existing risks, types of traffic and the applications in use.

ON2IT's Managed Security Services

IoT Security is only a small part of your overall cybersecurity. Our Reach and Risk Assessment provides a snapshot of your IoT security status, whereas our managed services go beyond that.

ON2IT's Managed Security Services is the solution to taking security concerns out of your hands. Our managed services mean your devices are under constant surveillance and when a threat is detected, our mSOC™ responds instantly.

- **Automated risk-based security policy recommendations and enforcement**
  Your IoT security solution must be easy to deploy without the need for any additional infrastructure or investment from your side. An ideal solution leverages your existing firewall investment for comprehensive and integrated security posturing. The solution needs to automatically recommend and natively enforce security policies based on the level of risk and the extent of untrusted behavior detected in your IoT infrastructure.
- **Swift action on preventing known threats**
  The diverse nature of IoT devices creates a highly distributed environment in your network with numerous points of compromise. Insights flowing from the previous steps ensure better detection and prevention of known threats, and better protection against new threats.
- **Fast detection and rapid response to unknown threats**
  Your IoT security solution should be capable of leveraging a new approach, drawing from a collective threat intelligence engine that delivers real-time malware analysis and protection from zero-day attacks on your IoT devices.

ON2IT AND PALO ALTO NETWORKS: ZERO TRUST INNOVATORS

ON2IT's full support of Palo Alto Networks technology since 2009 truly reflects the importance of cybersecurity innovation in our DNA.

ON2IT is a Palo Alto Networks ASC Elite, ATP, CPSP, MSSP, CSSP, Diamond Partner, winner of a Traps Global Award and Global Managed Services Partner of the year.

We offer worldwide managed cybersecurity services for organizations with complex and dynamic IT infrastructures. Our managed services are modular, scalable, cost-effective, and always based on Zero Trust.

We are on to it, and you?

FOR MORE INFORMATION ABOUT OUR REACH AND RISK ASSESSMENT:

Hogeweg 35, 5301 LJ Zaltbommel, The Netherlands
Email: sales@on2it.net - Phone: (+31) 088 22 66 200

5717 Legacy Drive, Suite 250, Plano, TX 75024, USA
Email: sales@on2it.net - Phone: (+1) (214) 206 8446