www.honeybox.com

honeyBox

Constant Network Control

SET A TRAP FOR HACKERS!

With honeyBox® for unwelcome visitors to your network.

honeyBox

constant network control

Keep security risks permanently under control with honeyBox® based on honeypot technology.

Network security mechanisms are usually active and are directed against attacks or try to prevent malpractice. Honeypots take a different approach. They actually invite attackers to engage with them, giving administrators time to detect and repel attacks. honeyBox® fits in well with industrial control networks.

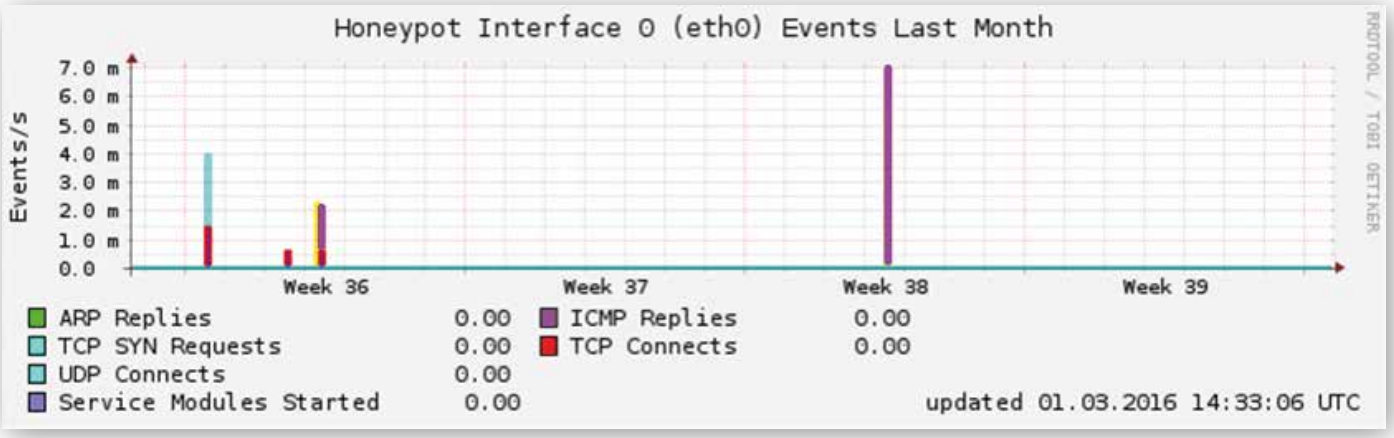
How does honeyBox® work?

honeyBox® puts out a large number of virtual honeypots. honeyBox® security alerts are gathered centrally and alarms are issued to the administration. The messages can be analysed according to various criteria via a secure HTTPS connection in the browser. This makes it possible to drill down systematically to the root cause. The messages can also be sent to external systems (e.g. via syslog).

„A honeypot is a system whose value is being probed, attacked or compromised – you want the bad guys to interact with your honeypot."

Source: „The Honeynet Project FAQ"

Significant events identified at a glance:



Systematic attacks – honeypots tie up an attacker's resources in the important stages of an attack.

honeyBox® does not monitor content. Instead it observes the way an attacker behaves. Virtual honeypots allow several levels of an attack to be detected and reported. These include the initial scan of available IP addresses and ports as well as a search for vulnerable systems and attempts to access them.

A simple principle: virtual bait is intended to attract and challenge attackers.

1. Information search on the Internet
2. **Scanning (ARP, ICMP, ports, operating systems)**
3. **Discovery (services, users, software)**
4. **Access to systems**
5. Extension of privileges
6. Search for trust relationships
7. Installation of backdoors
8. Covering up tracks

Sequence of a typical cyber attack

honeyBox

constant network control

honeyBox® in an office environment

Contain security risks permanently with honeyBox® – the ideal solution for industrial and office environments.

Deployment scenario in an office environment:

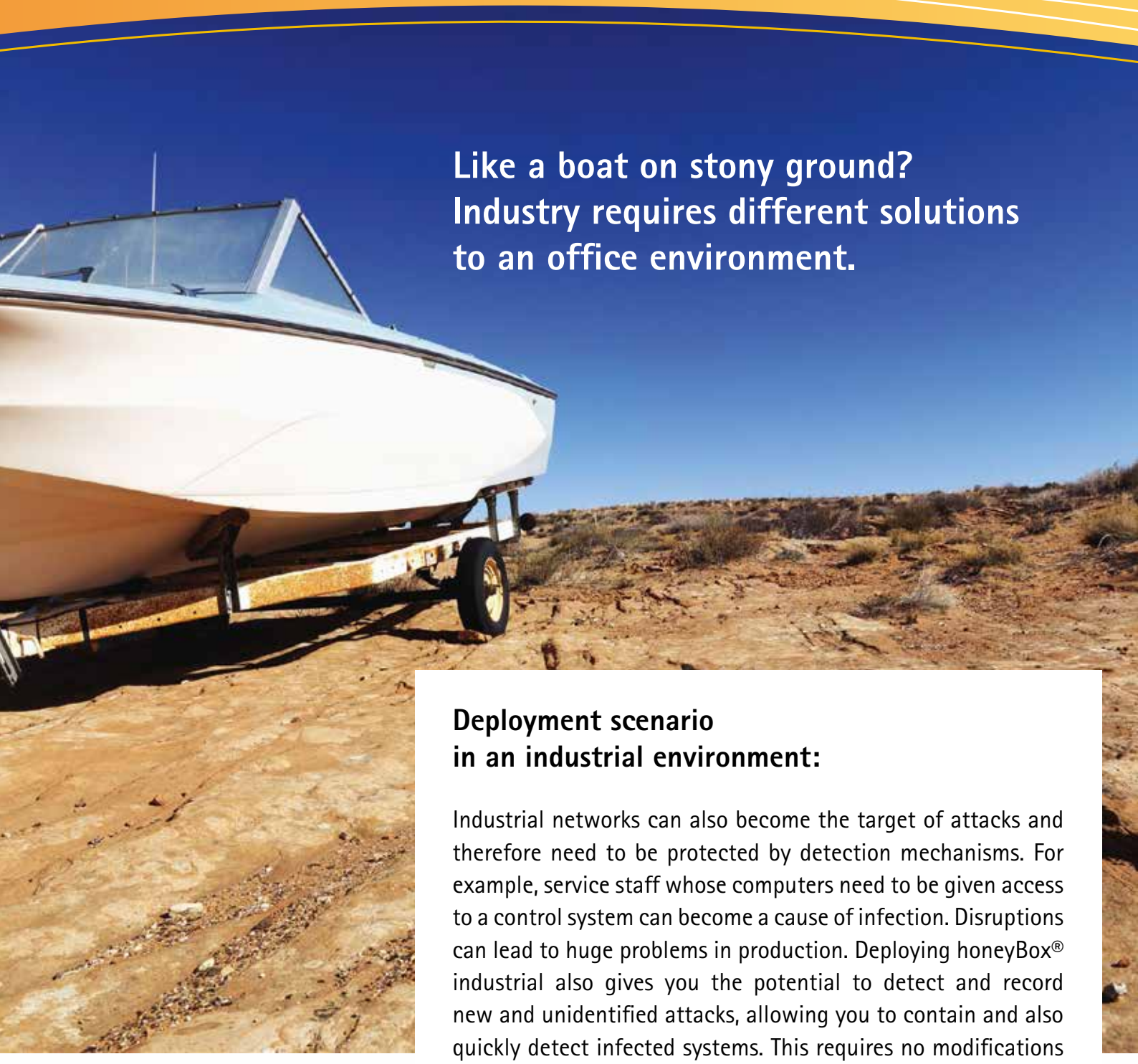
If you are running a large network, you have no effective universal monitoring. While you may have installed additional DMZs, your IPS cannot detect and prevent proliferation within the DMZs if an attacker assumes control of one of the DMZs. An IDS/ IPS will not provide reliable and comprehensive data about the security status of your network. You need an additional solution for this requirement.

Christian Scheucher (CEO of secXtreme) speaking to magazine Behörden Spiegel:

Behörden Spiegel: Is it possible for traditional solutions to cause outages or to interfere with data traffic?

Scheucher: Yes. Unfortunately that is the case. As one of the key aims of IT security, availability usually has very high priority. Firewalls and IPS are located directly within the data stream. This means additional risks of failure. This operating principle also means that data traffic, which operated perfectly prior to an update, is now disrupted.

The interview was conducted by Guido Gehrt, editor with magazine "Behörden Spiegel"



Like a boat on stony ground? Industry requires different solutions to an office environment.

Deployment scenario in an industrial environment:

Industrial networks can also become the target of attacks and therefore need to be protected by detection mechanisms. For example, service staff whose computers need to be given access to a control system can become a cause of infection. Disruptions can lead to huge problems in production. Deploying honeyBox® industrial also gives you the potential to detect and record new and unidentified attacks, allowing you to contain and also quickly detect infected systems. This requires no modifications to your network structure.

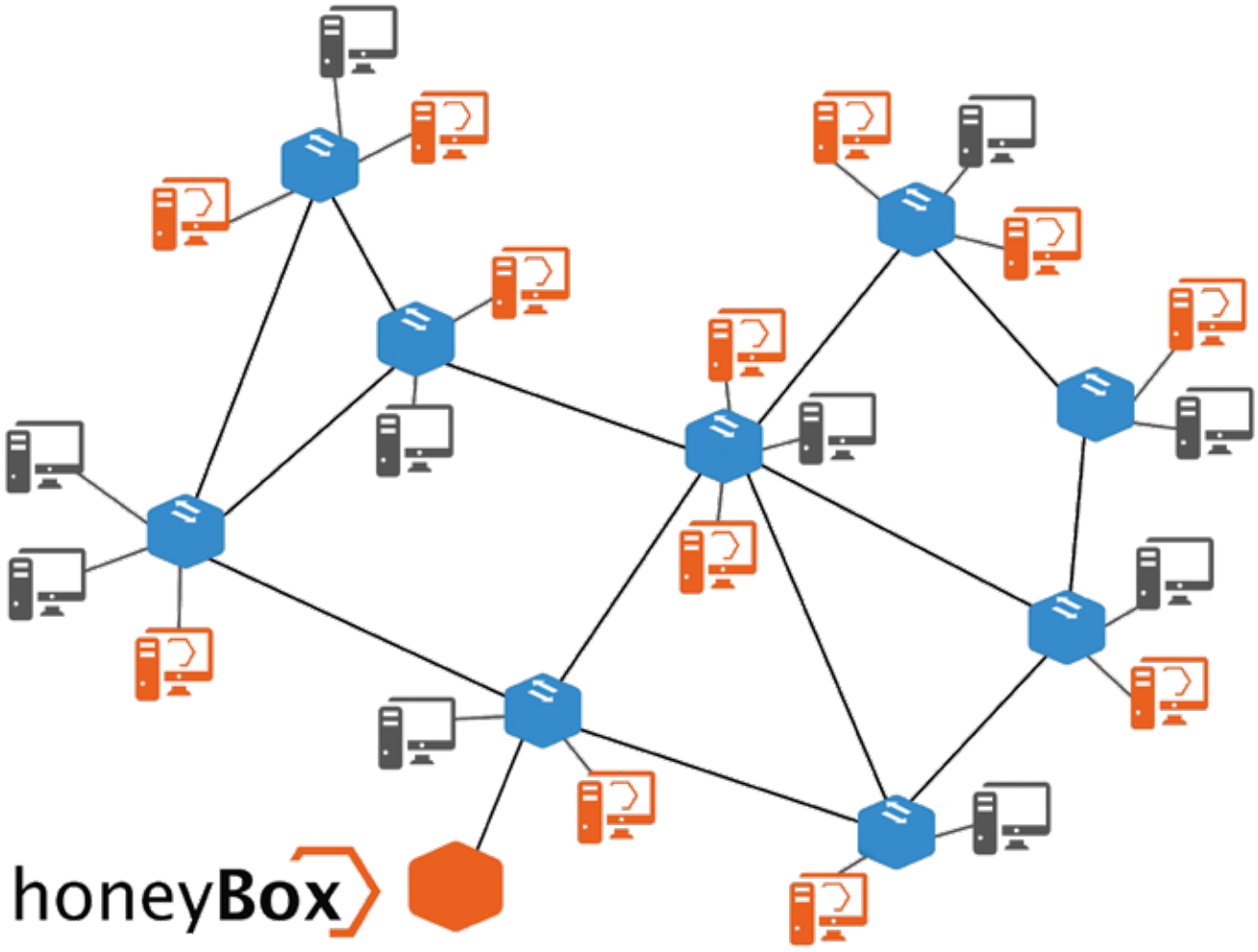
honeyBox

constant network control

Honeypots in a LAN:

„secXtreme's professional implementation and technical competence proved to us that choosing honeyBox® was the right decision."

Statement by customer Reinhard Görtner, Head of IT & Services, RTL II



Honeypots interspersed among real systems

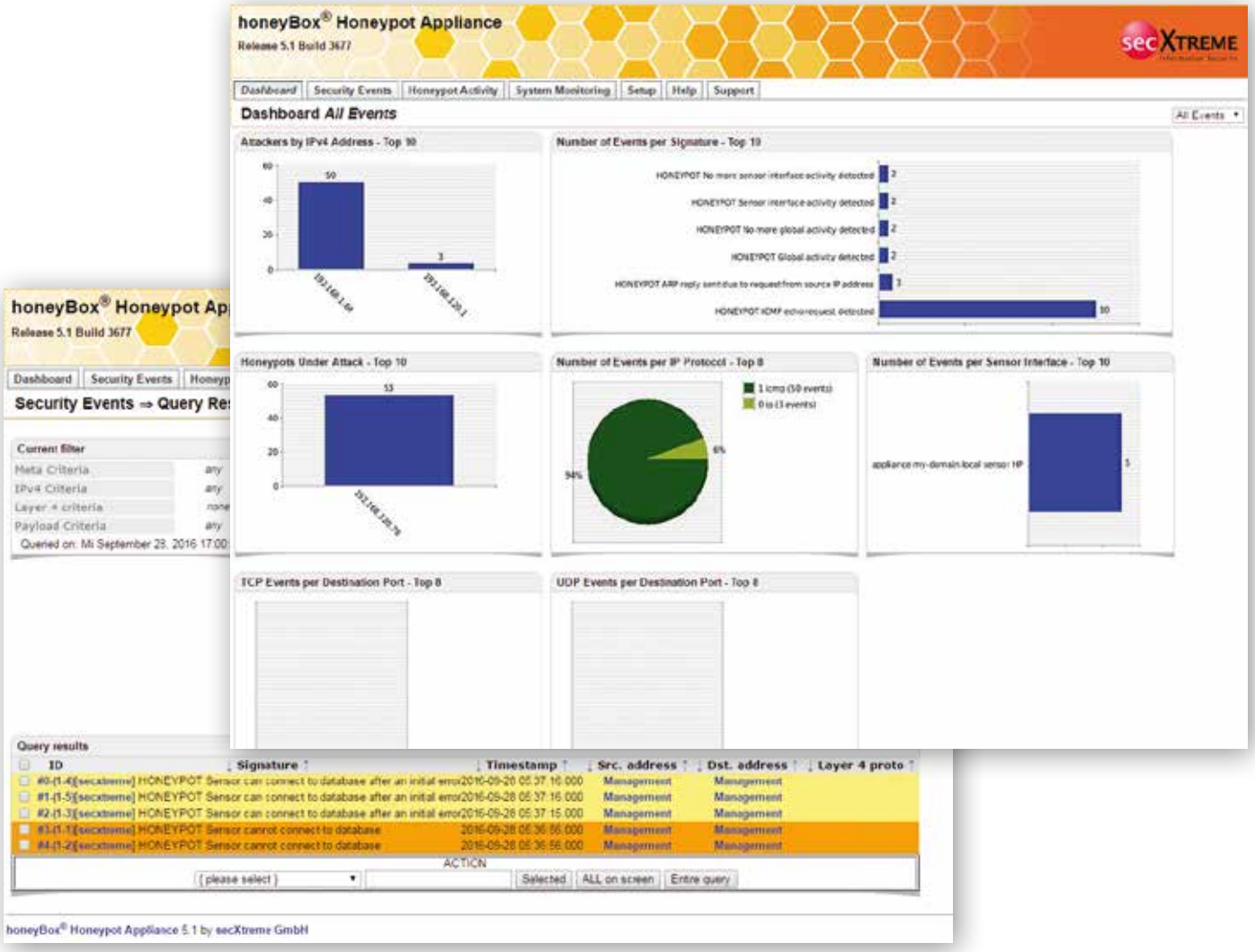
Technical information

Hardware	honeyBox® industrial Generation 2	honeyBox® universal Generation 1	honeyBox® enterprise Generation 2
			
CPU	Intel Atom N2600, 1.6 GHz, dual core, hyperthreading	Intel Core 2 Duo E8500, 3.16 GHz	Intel Xeon, six core
Working memory	2 GB DDR3 SoDIMM	2 GB DDR3 SDRAM, non-ECC	8 GB registered ECC DIMMs
Network	2 x 10/100/1000 copper (1-Port license or 2-Port license)	8 x 10/100/1000 copper (4-Port license or 8-Port license)	4 x 10/100/1000 copper
USB (external)	4 x USB 2.0	2 x USB 2.0	3 x USB 3.0
Storage	4 GB industrial C-Fast card (1-Port license) 60 GB 2.5 inch SATA MLC SSD (2-Port license)	250 GB, SATA-300, 7200 RPM	2 x 146 GB, 6G SAS, 15 000 RPM (RAID 1)
RS232	2 x DB9	1 x RJ45	1 x DB9
Power supply	DC 9 – 32 Volt	100 – 240 VAC	2 x 100 – 240 VAC, 50 – 60 HZ
Power consumption	minimum 17 Watt, typical 25 Watt	200 W maximum	approx. 200 W, 750 W maximum
Operating temperature	0 to +50 °C	0 to +40 °C	+10 to +35 °C
Humidity	5 % – 95 % non-condensing	10 % – 90 % non-condensing	8 % – 90 % non-condensing
Dimensions	50 x 145 x 115 mm (W x H x D)	426 x 44 x 366 mm (W x H x D)	482 x 43 x 742 mm (W x H x D)
Certifications	CE, RoHS	CE, FCC, RoHS	CISPR 22, EN55022, EN55024, FCC u. a.

honeyBox

constant network control

honeyBox® – assuredly greater control over your network.



Technical information

Functions	Function details	honeyBox® industrial Generation 2 (1-Port license)	honeyBox® industrial Generation 2 (2-Port license)	honeyBox® universal Generation 1 (4-Port license)	honeyBox® universal Generation 1 (8-Port license)	honeyBox® enterprise Generation 2	Management
Honeypot sensor	Max. no. of honeypots per appliance	250	500	4.000	8.000	40.000	○
	Max. no. of honeypots per network interface	250	250	1.000	1.000	500	○
	No. of usable network interfaces	1	2	4	8	4	○
	Max. no. of VLANs	○	○	○	○	80	○
	No. of special services	28+	28+	28+	28+	28+	○
	No. of honeypot templates	50+	50+	50+	50+	50+	○
	Network data recorder	○	●	●	●	●	○
Honeypot management	Monitoring web GUI	●	●	●	●	●	●
	Alarm analysis with centralised management	●	●	●	●	●	●
	Management component included	○	●	●	●	●	●
	Setup via SSHv2 and serial	●	●	●	●	●	●
	Alert system (e-mail, pager, syslog [CSV and CEF], database, logfiles)	●	●	●	●	●	●
	Backup/restore/recovery	●	●	●	●	●	●
	Watchdog	●	●	●	●	●	●
	Hardware monitoring	●	●	●	●	●	○
Installation	ISO image	○	○	○	○	○	●
	USB drive	●	●	●	●	●	○
Integration	Digitally signed updates via the Internet	●	●	●	●	●	●
	NTPv3 time synchronisation	●	●	●	●	●	●
Security	Hardened Debian Linux	●	●	●	●	●	●
	SSHv2	●	●	●	●	●	●
	HTTPS (local CA)	●	●	●	●	●	●
	File system integrity checks	●	●	●	●	●	●
	Security baselining	●	●	●	●	●	●
	Local firewall	●	●	●	●	●	●
	Signed software packages	●	●	●	●	●	●
Support	5 x 8 by phone and e-mail (DE & EN)	●	●	●	●	●	●
Hardware replacement	Standard warranty hardware replacement	2 years	2 years	1 year	1 year	3 years	○
	Extendable by	5 years	5 years	5 years	5 years	5 years	○
	Keep-your-hard/flash-disk option	●	●	●	●	●	○
	NBD service possible (country-dependent)	○	○	●	●	●	○
Neutral housing	„Stealth option"	●	●	●	●	●	○

○ *Not supported* ● *Supported*

honeyBox

constant network control

The honeypot appliance brings significant benefits in terms of security, speed of implementation, investment and operating costs.

honeyBox® offers:

- Reliable detection of network attacks and fast identification of worm outbreaks when monitoring up to 80 subnetworks on one device (honeyBox® enterprise with VLAN support)
- No impairment of network availability and virtually no false alarms
- Simple integration, low operating costs and no changes to network infrastructure required

Winner of the Bavarian Security Award 2009

honeyBox® won the Bavarian Security Award 2009. It ranked among the top entrants in the SME Innovation Award in 2009 and 2010 and received the BEST OF certificate in 2013 and 2014. It also won BEST OF in the 2016 Industry Award.

honeyBox®-Modelle

honeyBox® industrial Generation 2

honeyBox®-Management

honeyBox® universal Generation 1

honeyBox® enterprise Generation 2

honeyBox

constant network control

About secXtreme: secXtreme GmbH specialises in protecting your information. This involves the areas of auditing, penetration testing, security analysis and training. In addition to these areas, secXtreme also develops custom solutions in the security field. secXtreme offers managed security services and supports its customers with incident management and forensic work.

secXtreme Information Security

secXtreme GmbH
Alte Landstraße 21
D-85521 Ottobrunn
Telefon: +49 89 18 90 80 68-0
Telefax: +49 89 18 90 80 68-77
E-Mail: info@sec-xtreme.com
www.honeybox.com

Presented by your secXtreme partner:

by dievirtuellecouch.net // August 2019