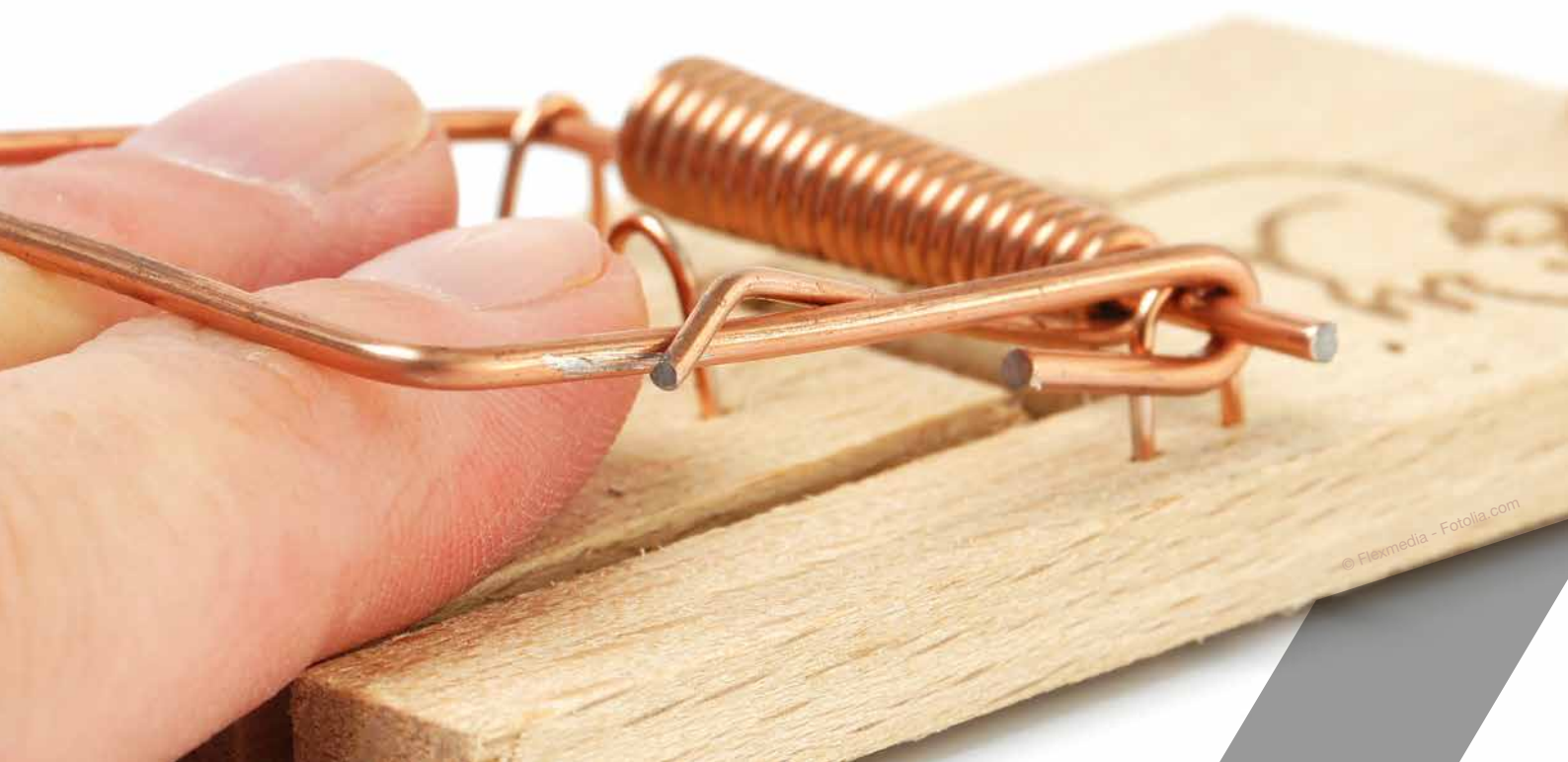


Constant Network Control

# SET A TRAP FOR HACKERS!

With **honeyBox®** for  
unwelcome visitors  
to your network.



## 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.“*

Quelle: „The HoneyNet Project FAQ“

## 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

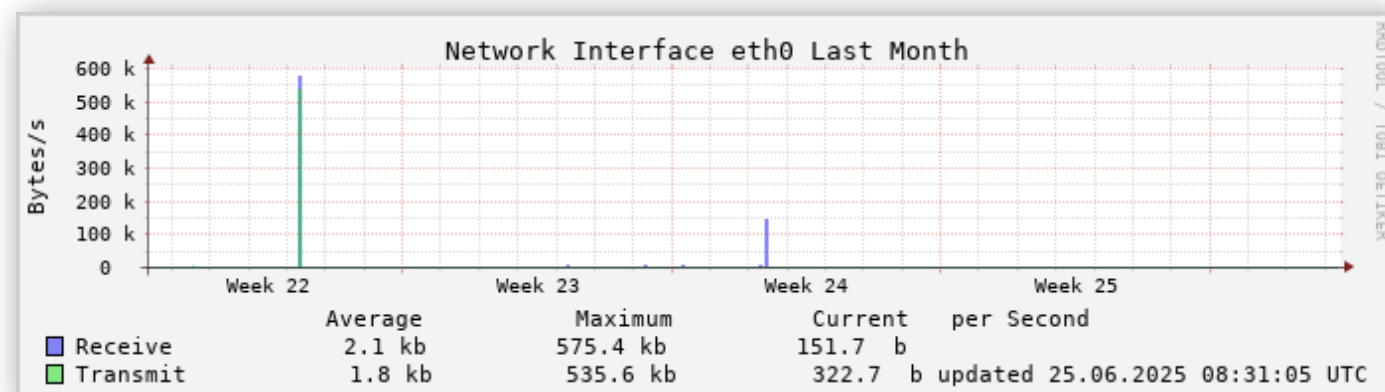
6. Search for trust relationships

7. Installation of backdoors

8. Covering up tracks

*Sequence of a typical cyber attack*

Significant events identified at a glance:



### 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.

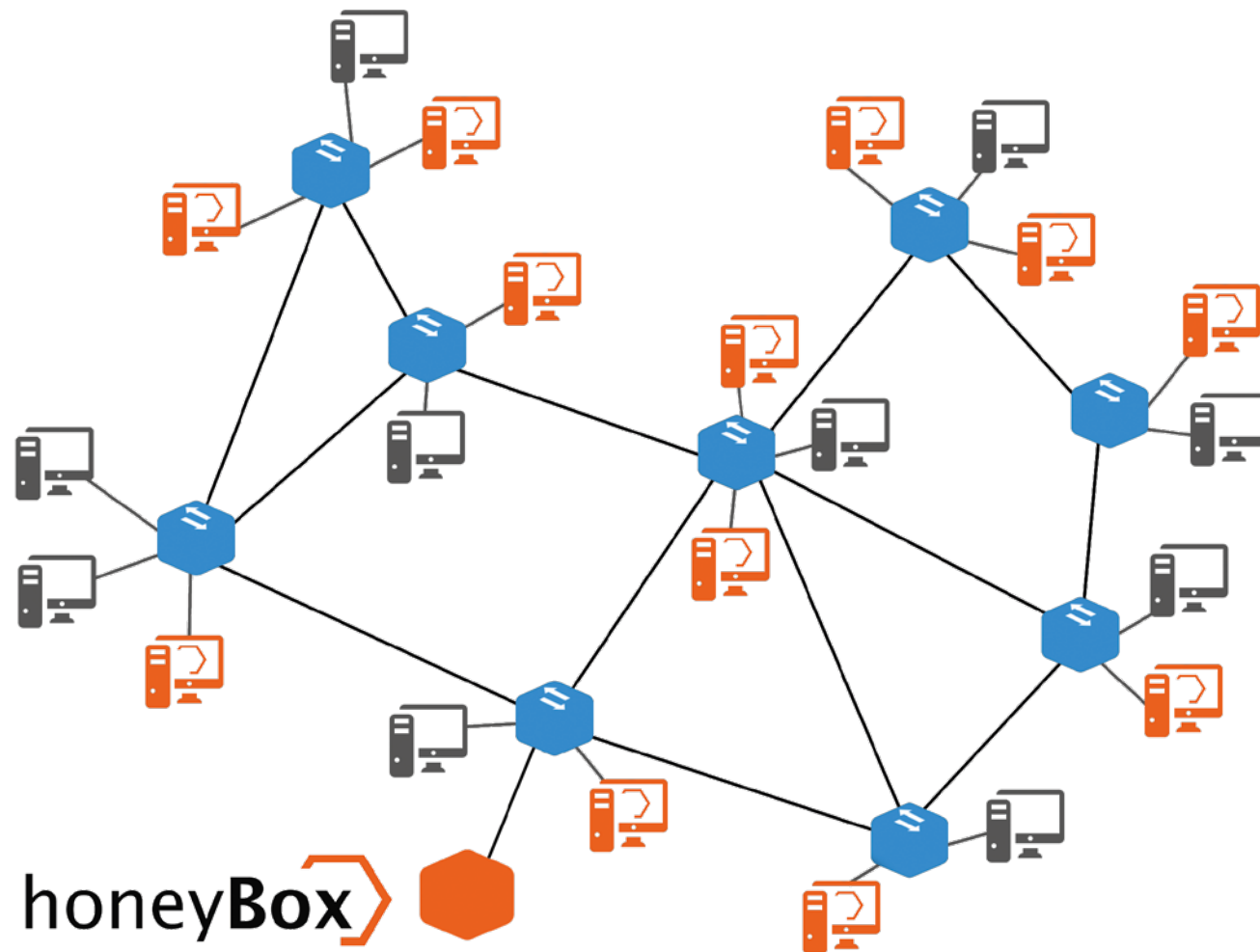




## Honeypots in a LAN:

*„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*



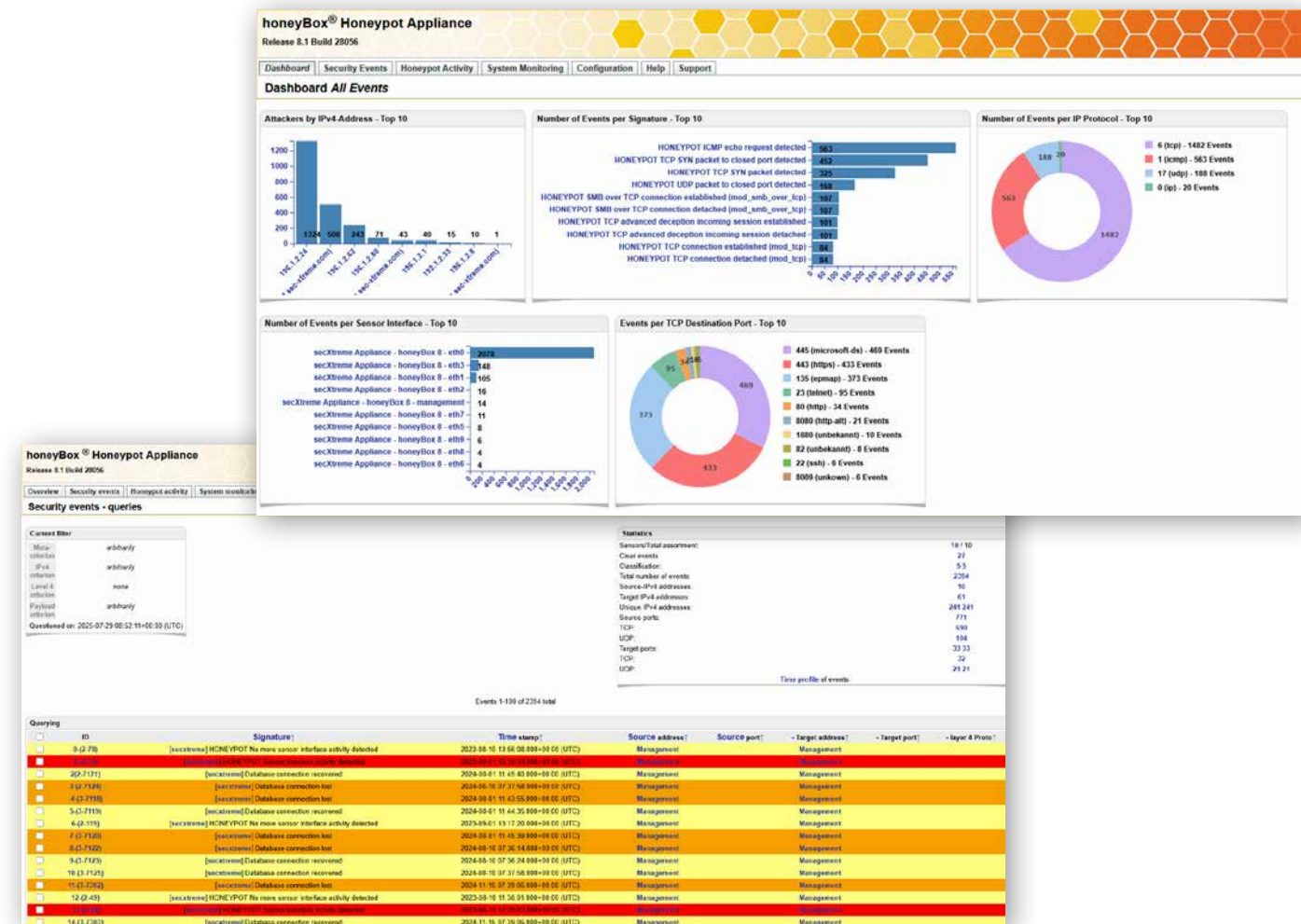
honeyBox

Honeypots interspersed among real systems

Designed by Freepik and distributed by Flaticon

| Hardware              | honeyBox®<br>industrial<br>Generation 2   | honeyBox®<br>micro<br>Generation 3  | honeyBox®<br>universal<br>Generation 3  | honeyBox®<br>enterprise<br>Generation 5   |
|-----------------------|---|---|---|---|
|                       |  |  |  |  |
| CPU                   | Intel Atom N2600,<br>1.6 GHz, 2-Core,<br>hyperthreading                             | Intel Celeron   | Intel Core i-5 10500  | Intel Xeon  |
| Working memory        | 2 GB DDR3 SoDIMM  | 16 GB DDR4  | 8 GB DDR4   | 32 GB Registered DIMMS  |
| Network               | 2 x 10/100/1000 copper  | 4 x 10/100/1000/2500  | 8 x 10/100/1000 copper<br>additional enhancements<br>possible                       | 4 x 10/100/1000 copper<br>additional enhancements<br>possible                       |
| USB (external)        | 4 x USB 2.0   | 1 x USB 3.1   | 2 x USB 3.0   | 2 x USB 3.2<br>1 x USB 2.0 (optional)   |
| Storage               | 60 GB, 2.5" S-ATA MLC SSD   | 64 GB, M.2 SSD  | 240 GB, 2.5" SATA SSD   | 2 x 300 GB SAS 12G HDD  |
| RS232                 | 2 x DB9   | 1 x RJ-45   | 1 x RJ-45   | 1 x DB9   |
| Power supply          | DC 9 – 32 Volt  | 100 – 240 VAC,<br>50 – 60 Hz  | 100 – 240 VAC,<br>50 – 60 Hz  | 2 x 200 – 240 VAC,<br>50 – 60 Hz  |
| Power consumption     | minimum 17 Watt,<br>typical 25 Watt   | 40 Watt   | 30 Watt typical<br>150 Watt maximum   | 105 Watt typical<br>800 Watt maximum  |
| Operating temperature | 0 to +50 °C   | 0 to +40°C  | 0 to +40 °C   | +10 to +35 °C   |
| Humidity              | 5 % – 95 %<br>non-condensing  | 5% – 90%<br>non-condensing  | 10 % – 90 %<br>non-condensing   | 5 % – 95 %<br>non-condensing  |
| Dimensions            | 50 x 145 x 115 mm<br>(W x H x D)  | 183 x 32 x 168 mm<br>(W x H x D)  | 438 x 44 x 344.4 mm<br>(W x H x D)  | 434.6 x 42.9 x 753.1 mm<br>(W x H x D)  |
| Certifications        | CE, RoHS  | CE/FCC Class B (Class A with<br>PoE), RoHS, UL, VCCI, UKCA                          | CE, FCC   | CISPR 32, EN6100-6-1,<br>EN62368-1, inter alia                                      |

## honeyBox® – assuredly greater control over your network.



| Functions            | Functional details                                 | honeyBox® industrial Generation 2 (1 Layer-3 Netzsegment) | honeyBox® industrial Generation 2 (2 Layer-3 Network segments) | honeyBox® micro Generation 3 | honeyBox® universal Generation 3 (4/8/12/16 Layer- 3 Netzsegmente) | honeyBox® enterprise Generation 5 | Management |
|----------------------|--|---|--|------------------------------|--|-----------------------------------|------------|
| Honeypot sensor      | Max. no. of honeypots per appliance                | 250   | 500  | 250                          | 4000/8000/12000/16000  | 40.000                            | ○          |
|                      | Max. no. of honeypots per 3-Layer network segments | 250   | 250  | 250                          | 1.000  | 500                               | ○          |
|                      | Max. no. of monitorable Layer-3 network segments   | 1   | 2  | 1                            | 4/8/12/16  | 80                                | ○          |
|                      | No. of usable network interfaces                   | 2 copper  | 2 copper   | 1 copper                     | 8 copper   | 4 copper                          | 1 virt.    |
|                      | No. of special services                            | 28+   | 28+  | 28+                          | 28+  | 28+                               | ○          |
|                      | No. of honeypot templates                          | 79+   | 79+  | 79+                          | 79+  | 79+                               | ○          |
|                      | 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, syslog, database, logfiles)  | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | Notification via digital outputs                   | Yes   | Yes  | No                           | No   | No                                | No         |
|                      | Backup/restore/recovery                            | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | Watchdog   | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | Hardware monitoring                                | ●   | ●  | ●                            | ●  | ●                                 | ○          |
| Installation         | ISO image  | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | USB drive  | ●   | ●  | ●                            | ●  | ●                                 | ○          |
| Integration          | Digitally signed updates via the Internet          | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | NTPv3 time synchronisation                         | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | Notifications to syslog server/SIEM                | ●   | ●  | ●                            | ●  | ●                                 | ●          |
| Security             | Hardened Debian Linux                              | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | SSHv2  | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | HTTPS (local CA)                                   | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | File system integrity checks                       | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | Security baselining                                | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | Local firewall                                     | ●   | ●  | ●                            | ●  | ●                                 | ●          |
| Support              | 5 x 8 by phone and e-mail (DE & EN)                | ●   | ●  | ●                            | ●  | ●                                 | ●          |
|                      | Managed Security Services (SOC, on-site)           | optional  | optional   | optional                     | optional   | optional                          | optional   |
| Hardware replacement | Standard warranty hardware replacement             | 3 years   | 3 years  | 3 years                      | 3 years  | 3 years                           | ○          |
|                      | Extendable by                                      | 5 years   | 5 years  | 5 years                      | 5 years  | 5 years                           | ○          |
|                      | Keep-your-hard/flash-disk option                   | ●   | ●  | ●                            | ●  | ●                                 | ○          |
| Neutral housing      | „Stealth Option“                                   | ●   | ●  | ●                            | ●  | ●                                 | ○          |

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® industrial Generation 2



honeyBox®-Management



honeyBox® universal Generation 3



honeyBox® enterprise Generation 5



honeyBox® micro Generation 3



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.

All trademarks used are the trademarks of the relevant trademark owners. Technical information subject to change – errors excepted.



secXtreme GmbH  
Alte Landstraße 21  
D-85521 Ottobrunn  
Phone: +49 89 18 90 80 68-0  
E-Mail: [info@sec-xtreme.com](mailto:info@sec-xtreme.com)  
[www.honeybox.com](http://www.honeybox.com)

Presented by your secXtreme partner:

