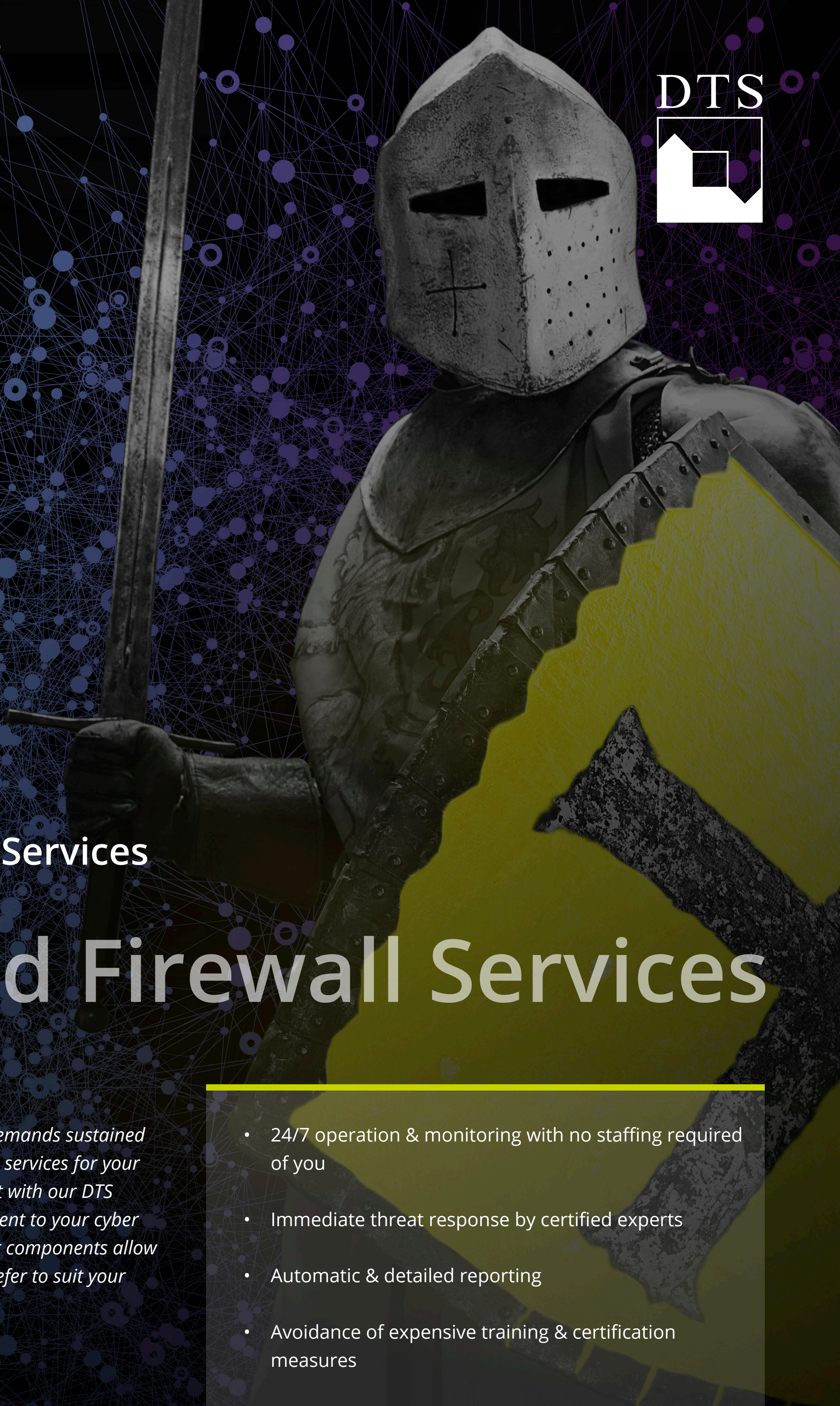


DTS
Managed Firewall Services

Managed Firewall Services

The rapidly growing threat landscape demands sustained attention and smarter, more responsive services for your IT security. We offer a service of this sort with our DTS Managed Firewall, as an ideal complement to your cyber security strategy. The following modular components allow you to combine the components you prefer to suit your individual needs.

- 24/7 operation & monitoring with no staffing required of you
- Immediate threat response by certified experts
- Automatic & detailed reporting
- Avoidance of expensive training & certification measures
- Overview of the monitored systems & applications
- Clearly defined services & costs
- Always up-to-date on potential security risks
- Maximum control over your network
- 24/7 DTS Security Operations Center (SOC)

DTS Next-Generation Firewall (NGFW) Basic Administration

- Support for rule systems
  - Configuration
  - Plausibility check for changes
- General support
  - VPN configuration
  - Support in the implementation of PAN-OS updates/fixes

  (DTS NGFW Basic Administration is also available with a hardware appliance).

DTS Next-Generation Firewall (NGFW) Backup Support

- Daily backup of the appliance configuration
- Configuration recovery support
  - 1-hour remote recovery support

DTS Next-Generation Firewall (NGFW) Health Check

- Active monitoring of the appliances by DTS Monitoring
  - Setup of monitoring including notifications in case of error messages
- Quarterly review
  - Best practice assessment of the policy including evaluation and suggestions for improvement
- Checking of the operating system (PAN-OS)
- Recommendations regarding release change
  - Recommended PAN-OS Release
  - Recommended GlobalProtect Release
  - Recommended User ID Agent Release
- Permanent technical contact for control of the PAN-OS and the BPA

DTS German WildFire Cloud
Increasingly, sophisticated cyberattacks are bypassing traditional cybersecurity measures. Conventional antivirus solutions and intrusion prevention as well as purpose-built sandbox appliances can no longer provide high-quality protection. Our unique DTS German WildFire Cloud, as a next-generation sandbox, detects novel zero-day malware as well as exploits through combined complementary analysis techniques and shares the information for complete protection with all connected networks, endpoints and clouds.

DTS's German WildFire Cloud runs infected files in a scalable virtual sandbox and scans them for malicious behavior using dynamic as well as static analysis techniques. All common file types are supported by WildFire, including: Microsoft Office documents, EXEs, DLLs, PDFs, fonts, Java, Android APK, ZIP, PE files. In this way, WildFire detects unknown malware, zero-day malware and exploits. When novel threats are detected, the infecting file is automatically assigned a signature, which in turn is delivered to anyone connected to the service in just 5 min - for near-complete protection.

Detecting a threat is the first step, but the true value of the German WildFire Cloud lies in protecting each user and network. Rapid protection deployment allows the rapid spread of the previously unknown threat and other future variations to be detected or blocked from all users without additional activity or analysis. In conjunction with protection against malicious files or exploits, we also provide in-depth analysis of malicious outbound communications, disruptive command-and-control activity with anti-C2 signatures, and DNS-based callback signatures. This is because this information also flows additionally into the Palo Alto Networks databases, where newly discovered malicious URLs are automatically blocked.

Approach of the German WildFire Cloud:

1. reducing the attack surface through active security controls.

2. blocking the known threats through continuous monitoring of traffic, ports and protocols.

3. rapid detection of the unknown threats by performing and monitoring the real behaviors of incoming unknown content.

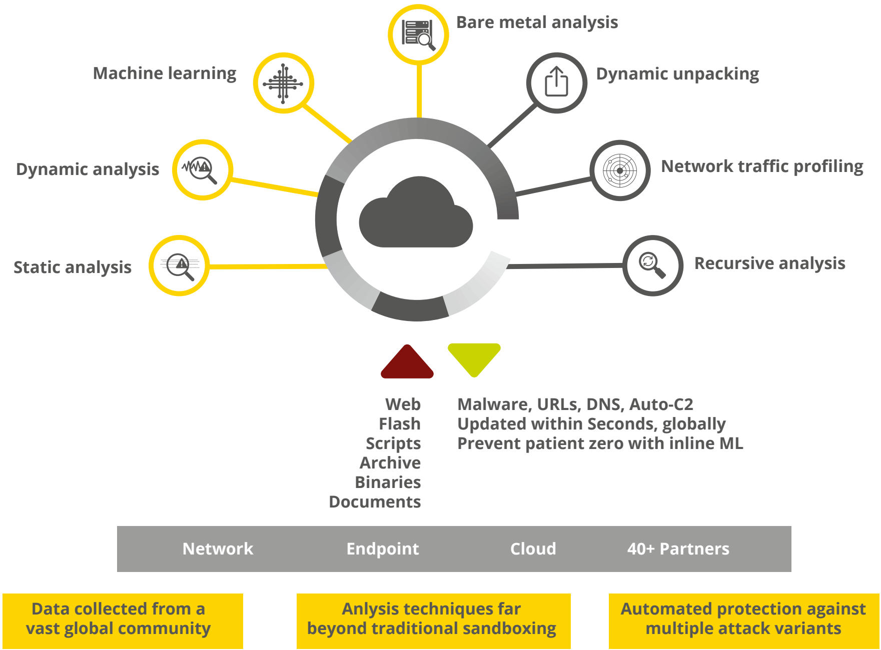
4. automatic development of new protection measures with subsequent integration into the defense mechanisms of all WildFire users.

In addition, WildFire provides you with built-in logs, analytics, and insights into WildFire events in the central administration interface. This gives you the ability to instantly investigate and correlate events observed on the network. The information provides important insights into, for example, probed domains, created files, or affected registry records. This allows you to quickly locate the data you need for early investigation and incident response, and then translate it into actions such as log requests or custom signatures.

To support IT security and detect infected hosts, WildFire also provides:

- Detailed analysis of every malicious file sent to WildFire, including both client- and network-based activity.
- Session data associated with the malicious malware, including source, destination, application, user ID, URL, etc.
- Access to, for example, original malware samples for reconstruction or replication, and all PCAPs from the dynamic analysis sessions
- Analysis provides many threat indicators that can be used to target the threats

The solution is operated in our own certified data centers. You can use the German WildFire Cloud through your existing Palo Alto Networks firewalls at no additional hardware cost, giving you access to dynamically scaled malware analysis and automated distribution of protection. Due to the redundant setup of the environment in the two German DTS data centers, we guarantee you a security solution that complies with German regulations or conformity according to the BSI as well as the DSGVO. All suspicious files are transferred. After analysis, benign files are destroyed, while malicious files are archived or safely stored for further analysis. We are the only German company to offer a virtual malware analysis sandbox in accordance with German law.



Bare metal analysis

Machine learning

Dynamic unpacking

Dynamic analysis

Network traffic profiling

Static analysis

Recursive analysis

Web
Flash
Scripts
Archive
Binaries
Documents

Malware, URLs, DNS, Auto-C2
Updated within Seconds, globally
Prevent patient zero with inline ML

Network | Endpoint | Cloud | 40+ Partners

Data collected from a vast global community

Anlysis techniques far beyond traditional sandboxing

Automated protection against multiple attack variants

USPs of the DTS German WildFire Cloud:

- Scalable, virtual malware analysis sandbox
- Detects previously unknown malware, zero-day malware & exploits in infected files
- Supports all common file types
- Automatic information & protection distribution within only 5 min.
- Can be used with existing Palo Alto Networks firewalls without additional hardware costs
- Deployment, operation & support in certified DTS data centers
- Only virtual malware analysis sandbox according to German law