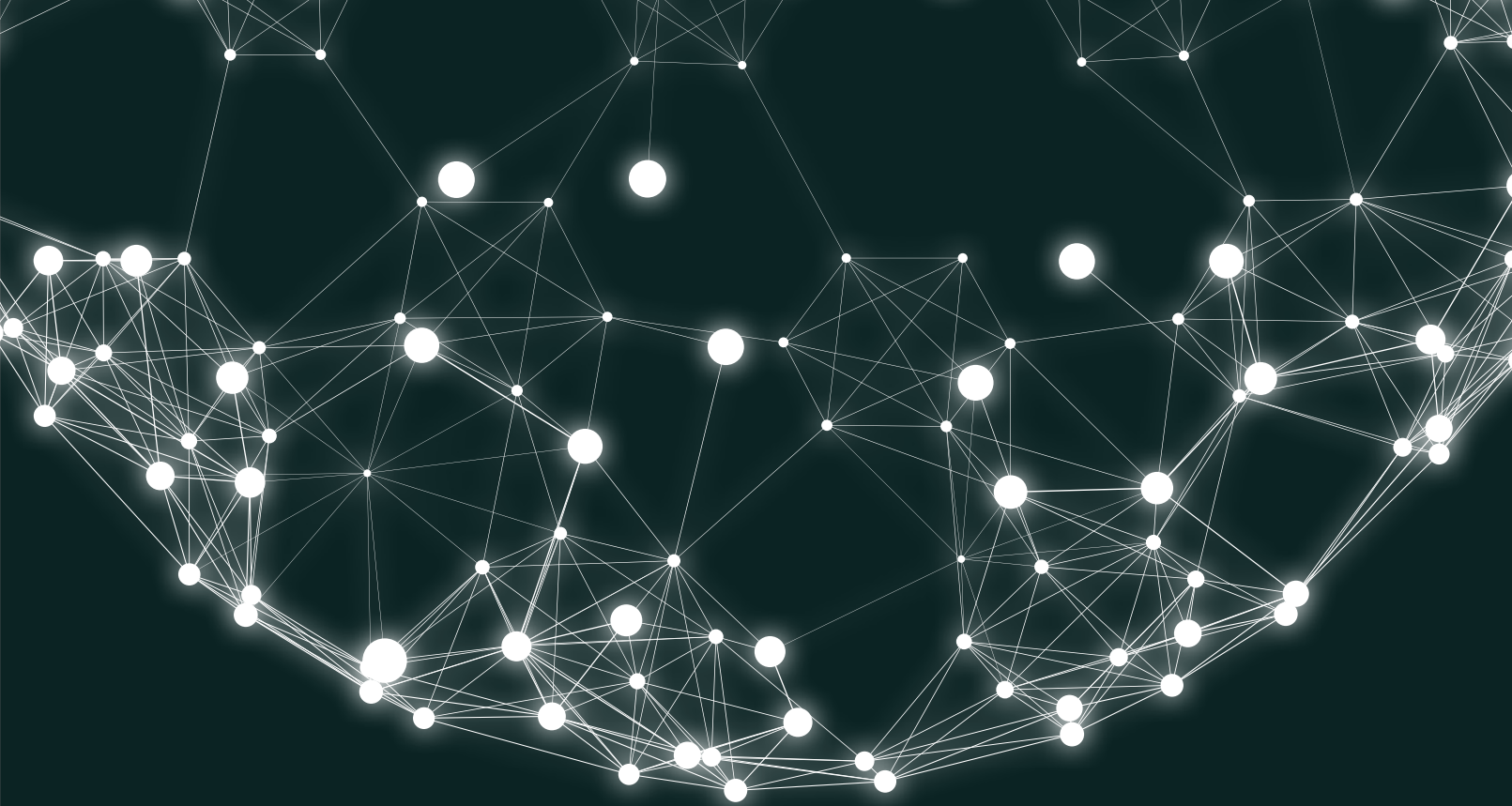

# sure[secure]

## UNTERNEHMENSBROSCHÜRE


# 00 VORWORT

**Warum wir die suresecure gegründet haben?**

Wir wollten das vereinen, was am Markt fehlte, und zwar mit Werten, die uns entsprechen.

Unser Bestreben war es, ein Unternehmen auf die Beine zu stellen, welches Partnerschaftlichkeit in den Fokus stellt; einen Raum zu schaffen, der Arbeiten menschlich macht; und die qualitativ hochwertigsten Leistungen im IT-Security Bereich anzubieten.

Seit 2010 die erste Malware gezielt Industrieanlagen angriff, stieg der Bedarf an IT-Security. Nur konnte oder wollte kein Unternehmen nur diesen Bedarf allein decken. Was dazu führte, dass wir bei Unternehmen gearbeitet haben, die ihre Aufträge nicht abarbeiten konnten, keine Zeit für Gewissenhaftigkeit hatten und schon gar keine Expertenteams zusammenstellten. Für unseren Anspruch einfach zu wenig. Die logische Konsequenz kam durch eine SMS von Andreas „Ich hab Bock auf Selbstständigkeit." Damit entstand die Idee der suresecure und heute lebt diese Idee durch eine Gemeinschaft von Mitarbeitenden, die Lust haben, gemeinsam die Welt zu verändern.

Und darauf sind wir stolz: Wir haben die Welt schon ein Stück weit verändert, indem wir vielen Unternehmen und den Menschen dahinter geholfen haben. Wir haben es geschafft, einen Ort zu schaffen, der zu familiärem Wachstum einlädt. Wir haben Mitarbeitende, die mit Leidenschaft an unserer Unternehmung teilnehmen und sicher sowie glücklich bei uns arbeiten. Wir haben Partnerschaften etabliert, die auf Vertrauen, Loyalität und Verantwortung beruhen.

**Wir können uns nur auf die Zukunft freuen!**

A. Papadamm

# 01 INHALT



# 02 VISION & MISSION

Wir machen die digitale Welt zu einem sicheren Ort. Niemand hat das Recht die fortschreitende digitale Vernetzung auszunutzen, um sich am Schaden der Anderen zu bereichern. Weder heute noch in Zukunft.

Wie das möglich ist? Indem wir Unternehmen dabei unterstützen, ihre IT-Infrastrukturen, Datenbestände und kritischen Geschäftsprozesse optimal zu sichern. Wir sind ausschließlich auf Kernthemen der IT-Security spezialisiert sowie die individuelle Konzeptionierung von Sicherheitsstrategien und die ganzheitliche Beratung in Fragen der IT-Sicherheit spielt die tragende Rolle der gesamten Unternehmung. Der alleinige Einsatz von Softwarelösungen schafft keine sichere Umgebung. Kann er allein schon aus einem Grund nicht: Die digitale Welt lebt von rasanten Veränderungen.

So ändern sich nicht nur die Anforderungen an die IT, sondern auch die Angriffsmuster. Und auf diese gilt es mit hohem Qualitätsbewusstsein flexibel und vor allem zeitnah zu reagieren. Dafür benötigt es unsere Spezialisten, die jeden Tag mit Leidenschaft an den effizientesten Sicherheitslösungen arbeiten.

## HARDFACTS

Die suresecure ist ein unabhängiges, hochspezialisiertes Beratungsunternehmen der IT-Security mit Sitz in Nordrhein-Westfalen und qualifizierten Mitarbeiter:innen in ganz Deutschland. Als international ausgerichteter IT-Security Berater bietet unser Portfolio Leistungen von strategischen IT-Security Lösungen bis zu umfänglichen as a Service Angeboten sowie Incident Response Verträgen.

# 03 WERTE

Wir stellen Partnerschaftlichkeit ins Zentrum unseres Handelns. Vertrauen investieren wir dabei bedingungslos als Risikokapital. Als Partner gehen wir alle Wege mit uneingeschränkter Unterstützung gemeinsam – unabhängig der Beziehung: Ob Mitarbeitende, Hersteller, Geschäftspartner oder Dienstleister.

### Gemacht mit purer Leidenschaft

Alles was wir tun, tun wir mit Leidenschaft. Genau diese Passion ist unser Treibstoff, um täglich das beste Ergebnis zu erzielen. Das beste Ergebnis ist für uns erst dann erreicht, wenn sich Zufriedenheit aller Beteiligten einstellt.

### Mut ist Herausforderung

Unsere Entscheidungen treffen wir mit Mut und Entschlossenheit. Wir vertreten unsere Grundhaltung konsequent mit dem Ziel die eigene Unternehmung zu schützen. Die Werte der suresecure bestimmen dabei jegliches Handeln.

### Wir vertrauen auf Vertrauen

Bei uns erfährt jeder bedingungsloses Vertrauen. Dieses Vertrauen ist unser höchstes Gut und die Basis für Loyalität, Zuverlässigkeit und Transparenz. Wir vertrauen darauf, dass alle Mitarbeitenden jederzeit im Sinne der suresecure handeln, weshalb wir Fehler nicht als Fehler, sondern als Chance zur Verbesserung thematisieren.

### Respekt ist der Schlüssel

Jeder genießt Achtung aus Gründen der gegenseitigen Wertschätzung. Diese Wertschätzung ist unabhängig von Religion, Geschlecht, Herkunft oder Beeinträchtigungen. Diese Toleranz bildet den Nährboden für einen respektvollen Umgang.

### Veränderung heißt Fortschritt

Unser Bestreben ist eine kontinuierliche und konsequente Weiterentwicklung der suresecure und aller Mitarbeitenden. Neue Gegebenheiten, Anforderungen oder Bedürfnisse greifen wir auf und binden diese dynamisch in unser Handeln ein.

# 04

# SORGLOSE IT-SICHERHEIT

Unser Unternehmensansatz schont allerlei Ressourcen. Wir bieten ganzheitliche IT-Security aus einer Hand. Dieser Ansatz bewirkt vor allem eins: Risikoreduzierung.

Wir verfügen über tiefgreifende technische Expertise im gesamten IT-Security Spektrum: Vom Aufbau komplexer Infrastrukturen und der Konzeptionierung von Sicherheitsstrategien über Awarenesstrainings bis zur vollumfänglichen Betreuung der gesamten Umgebung und dem Betrieb von Security Operation Centern.

Dabei ist es uns besonders wichtig, unser Know-how agil und schnell zur Verfügung zu stellen. Deshalb haben wir uns zusätzlich auf das Incident Response Management spezialisiert und betreuen effektiv Unternehmen beim gesamten Handling von Security Incidents.



## KOMPETENZBEREICHE UNSERER EXPERTEN

Was uns besonders macht? Unsere Experten! Wir haben viele ausgewiesene Spezialisten in unserem Team, wodurch wir alle Kompetenzbereiche der IT-Security abdecken können.

| Technical Security | Organizational Security | Security Intelligence |
|---|---|---|
| Device Security | Process Security | Security Inside / Insights |
| Network Security | Employee Security | Vulnerability Management |
| Security Awareness | Documentation | Data correlation & interpretation |
| Server Security | Legal Guidelines | |
| Gateway Security | Compliance Security | |
| Cloud Security | Data Security | |

# 05 KERNBEREICHE

Unser Portfolio beschreibt vier Kernbereiche. Mit der strategischen IT-Security Beratung steht und fällt eine effektiv geschützte IT-Umgebung. Die weiteren drei Bereiche spielen in der aktuellen Situation der Cyber-Sicherheit und somit auch der Unternehmenssicherheit zentrale Rollen. (s. Abbildung S. 14)

## 1. Strategische IT-Security Beratung

Alle Maßnahmen innerhalb der IT-Abteilung beginnen mit einer Aufnahme des Status quo und der anschließenden ausführlichen Planung einer Sicherheitsstrategie. Erst auf dieser Basis erfolgen weitere Schritte wie die Auswahl passender Technologien, Implementierung von Sicherheitssystemen oder das Einhalten von Datenschutzvorgaben.

Wir transformieren den Status quo in Handlungsempfehlungen mit einer Priorisierung nach Impact, Ressourcen und Zeit. So garantieren wir, dass der normale IT-Alltag während eines Projekts weiterlaufen kann. Mithilfe der Roadmap implementieren wir die Security-Services und erläutern den entsprechenden Verantwortlichen die gesamte Konfiguration der Systeme.



## 2. Incident Response Management

Daten sind mittlerweile zu einer Währung geworden. Und diese Währung gilt es zu beschützen. Denn verlieren Sie Daten, verlieren Sie auch Reputation. Damit ein Security Incident nicht zum Worst Case führt, haben wir verschiedene Services kreiert.

**Prävention statt Frustration:**

Wir begleiten Sie durch 3 Phasen zur bestmöglichen Vorbereitung auf einen Security Incident. Auch hier starten wir in Phase 1 mit der Evaluierung des Status quo. Danach entwickeln wir gemeinsam einen individuellen IR Notfallplan, das das zentrale Steuerungsmittel für einen Security Incident darstellt. Abschließend definieren wir technische und organisatorische Maßnahmen, die es zur Prävention in ihrem Unternehmen umzusetzen gilt.





## HILFE IM NOTFALL

Brennt es? Dann stehen wir als Partner zur Seite. Um den Vorfall schnellstmöglich zu beheben, sind wir 24x7 erreichbar, stellen während der gesamten Dauer ein Cyber Emergeny Response Team (CERT) und einen dedizierten Incident Response Manager vor Ort zur Verfügung. Das CERT bestehend aus Security Consultants sowie Data- und Malware-Analysten übernehmen die Kommunikation, das Management und die gesamte Forensik. Der IR Manager stellt das zentrale, interdisziplinäre Organ im Notfall dar, indem er das gesamte Krisenmanagement koordiniert, organisiert und steuert. Ziel dabei ist immer die Schadensbegrenzung und schnellstmögliche Wiederaufnahme des Regelbetriebs.

## 3. Security Operation Center as a Service

Wir betreiben das Security Operation Center (SOC), welches alle sicherheitsrelevanten Aspekte eines Unternehmens an zentraler Stelle managt. Das System erkennt Anomalien, indem es den Datenfluss aller angeschlossenen Log-Quellen beobachtet. Logs bzw. Events werden durch Clients, Firewalls, Server, Datenbanken oder Produktionsmaschinen geschrieben. Diese enorme Datenmasse kann durch ein SOC nutzbar gemacht werden, indem diese nicht nur analysiert, sondern auch korreliert wird.

Werden Anomalien festgestellt, erfolgt die Evaluierung einerseits softwarebasiert und andererseits durch unsere Security Analysten, die das SOC betreiben. Technologie ist nur das Werkzeug, doch es bedarf Expertise, die gesammelte Daten den individuellen Zielsetzungen entsprechend nutzbar zu machen. Hier gilt: Je besser die Detections, desto sicherer die IT-Infrastruktur. Ziel ist es mit einem hohen Automatisierungsgrad eine bestmögliche Absicherung gegen Cyberangriffe zu erreichen. Handelt es sich um einen bösartigen Befund, leiten wir sofort eine Gegenmaßnahme – ein Counter-Measure – ein.

### Was das SOC as a Service Angebot verspricht?

Wir managen alle sicherheitsrelevanten Themenbereiche an einer zentralen Stelle und sorgen so dafür, dass die Systeme zu jeder Zeit optimal geschützt sind. Dabei arbeiten wir volumenbasiert, weshalb genau die Use-Cases umgesetzt werden, die gewünscht sind. Das Monitoring verläuft proaktiv - das gilt insbesondere auch für die fortlaufende Anpassung der Konfiguration an die Systemumgebung.

### HARDFACTS

In unserem SOC sitzen nicht nur die besten Analysten, sondern wir setzen zudem auch auf die marktführende Technologie des Vendors splunk>.

Skalierbarkeit gewährleisten wir durch ein großes Team von Experti:innen und einen zertifizierten Partner im Bereich Rechenzentrum.

Unsere Services laufen über die Binary GmbH in Essen, die ein ISO9001 und ISO27001 zertifiziertes TIER3 Rechenzentrum betreiben. So können wir eine hohe Verfügbarkeit unserer Services garantieren.

## 4. Managed Security Services

Ein gutes Sicherheitskonzept bedeutet immer auch, dass die Security-Umgebung inklusive aller Services betrieben und gewartet werden muss. Ohne Betrieb, Wartung und Monitoring hat dieses keinen großen Wert. Es sind vier Kernbereiche zu betrachten, die für den Aufwand und die damit einhergehende Ressourcenplanung von Bedeutung sind: Updates und Patchmanagement, Change-Prüfungen, Upgrades und ServicePacks und das Reduzieren von False-Positives.

Hier sorgen wir mit unterschiedlichen Dienstleistungskontingenten für Abhilfe, indem wir die Security-Services managen. Neben der Entlastung reduzieren unsere Managed Security Services das IT-Risiko, vereinfachen Prozesse und verbessern die Geschäftsabläufe. Dabei sind 24x7 Servicezeiten in den höheren Ausbaustufen buchbar. Sollte etwas Unvorhergesehenes passieren, reagieren wir innerhalb von nur 2 Stunden – egal zu welcher Uhrzeit.

Schonen Sie Ihre eigenen Ressourcen durch unsere Managed Security Services. Wir betreuen Ihre IT-Lösungen auf höchstem Sicherheitsniveau, während Sie sich um Ihr Kerngeschäft kümmern.



## MANAGED SECURITY SERVICES

Unsere Managed Security Services sind in 3 Varianten verfügbar: Light, Standard, Premium.

| | Light | Standard | Premium |
|---|---|---|---|
| Dediziertes IT-Security Personal? | | ✓ | ✓ |
| Durchführung von Major-Releases? | | ✓ | ✓ |
| Ressourcen für einen 24x7 IT-Betrieb? | | ✓ | ✓ |
| Security-Events erkennen und bewerten? | | | ✓ |
| Reaktionszeit & Abrechnung | next Business Day nach Aufwand | bis zu 2h pauschal | bis zu 2h pauschal |

# 06 LEISTUNGSSPEKTRUM IM ÜBERBLICK

| Services | Solutions as a Service | Lösungen |
|---|---|---|
| Incident Response Management | Security Operation Center | First Check |
| Professional Services | Vulnerability Management | [secure] check |
| Managed Security Services | Security Awareness | [secure] alert |
| | | Health Check |

# 07

# STARKE PARTNERSCHAFTEN

Uns ist eins an unserer Arbeit besonders wichtig: die vollumfängliche, ehrliche und transparente Beratung. Eine solche Arbeitsweise geht immer einher mit Vertrauen. Menschen vertrauen uns und wir vertrauen ihnen. Das geht über reine Geschäftsverhältnisse hinaus.

Wir stellen Partnerschaftlichkeit ins Zentrum unseres Handelns. Deshalb werden Kunden bei uns zu Partnern. Als Partner gehen wir alle Wege mit uneingeschränkter Unterstützung gemeinsam.

Wir sind stolz auf all unsere bisherigen sehr erfolgreichen Partnerschaften.



NORDSEE
ebmpapst
Lück
HEIN LEHMANN
ELBE KLINIKEN STADE · BUXTEHUDE
SWIM
OQEMA
DEICHMANN
OPTIMA
wortmann SCHUH-HOLDING
eregio
H.C.Starck
Getränke Markt
KORIAN
MAX BÖGL
Fortschritt baut man aus Ideen.

# 08 ERFOLGS-GESCHICHTEN

Wir wollen nicht nur von starken Partnerschaften schwärmen, sondern diese auch zeigen: Mit unseren Partnern setzen wir jeden Tag umfangreiche IT-Security Lösungen um, welche die Unternehmen nachhaltig zu einem verbesserten Sicherheitsniveau führen. Damit machen wir die Welt ein Stückchen sicherer. Die folgenden drei Geschichten verdeutlichen, wie wir für jede Herausforderung die passende Lösung finden.

Sei es die individuelle Konzeptionierung einer ganzheitlichen Sicherheitsstrategie, der Einsatz unseres Incident Response Managements oder die Implementierung unseres Security Operation Centers. Uns ist keine Herausforderung zu groß.

## LÜCK GMBH

Die Lück GmbH & Co. KG ist Marktführer in Sachen Füllungen für Bett- und Polsterwaren aller Art, hat sich nach mehr als 40 Jahren seit Gründung zu einem Global Player mit internationalem Produktionsnetzwerk entwickelt.

### Herausforderung

Das IT-System der Lück ist täglich für:

- 80.000 EDI-Abwicklungen
- 60.000 Lagerumbuchungen
- 20.000 BDE-Meldungen und
- 18.000 Fertigungsauftrags-buchungen
- 1.800 NVE-Paletten
- 1.200 DPD-Pakete
- 80 - 100 LKW verantwortlich

Und das im internationalen Kontext mit Standorten in Deutschland, Polen, Litauen und China.

### Die Lösung

Die Antwort: Ein individuelles Securitykonzept, welches insbesondere kritische Geschäftsprozesse bestmöglich absichert.

Netzwerk, Endpoints, Server und Gateways wurden intensiv auf den Prüfstand gestellt und in einem übergreifenden, synergetischen Sicherheitskonzept abgesichert.

### Erreichte Erfolge

Rund 90% der Meldungen werden mittlerweile automatisiert durch das implementierte Sicherheitskonzept bearbeitet und gelöst.

- Gruppenweite Sicherheitsrichtlinien
- Sicherheitssysteme nach Best-Practice
- Qualifiziertes Personal
- Managed Security Services
  - Premium
- Produkte: DDI, DDAN, DS, AO, AC, IWSVA, IMSVA, CAS, HES, TP


## EBM-PAPST GMBH

Die ebm-papst Unternehmensgruppe ist Weltmarktführer bei der Herstellung von Elektromotoren und Ventilatoren mit Sitz in Mulfingen. Mit über 20.000 Produkten bietet ebm-papst für praktisch jede Aufgabe Lösungen.

### Herausforderung

Ein schwerer Security Incident trat noch vor Projektstart auf, sodass dieser umgehend behoben werden musste.

In den Incident Response Management Prozess waren über:

- 15.000 Clients
- 100te Server
- 29 Produktionsstandorte in ganz Europa
- 48 Vertriebsstandorte involviert

### Die Lösung

Die Antwort auf eine sehr komplexe Herausforderung war: splunk.

So konnte jede aufkommende Fragestellung als Detection im Dashboard sichtbar gemacht werden.

Zusätzlich wurde die Connected Threat Defense von Trend Micro implementiert.

### Erreichte Erfolge

Ganzheitliches IT-Security Konzept einhergehend mit einer erheblichen Verbesserung der IT-Infrastruktur:

- Machine Learning
- Sandboxing
- Behaviour Monitoring
- Intrusion Prevention
- Visibilität im Netzwerk
- Einführung eines SIEM (splunk)
- Network Intrusion Detection
- Automatisierte Reaktion
- Connected Threat Defense
- Unterstützung von APIs, IOCs

## OPTIMA PACKAGING GROUP GMBH

Die OPTIMA packaging group GmbH mit Stammsitz in Schwäbisch Hall ist eine internationale Unternehmensgruppe und Hersteller von Abfüll- und Verpackungsmaschinen.

### Herausforderung

Bei einem Ransomware-Angriff auf das Unternehmen wurden weltweit über 1000 Sever verschlüsselt mit insgesamt 1.600 betroffenen Clients.

Alle geschäftskritischen Prozesse kamen zum Erliegen. Die IT-Abteilung bemerkte den Angriff frühzeitig und stoppte alle betroffenen Systeme.

### Die Lösung

Durch den gemeinsamen Einsatz und die Übernahme des Incident Handlings durch unser CERT inklusive eines IR Managers konnte das Ausmaß des Schadens deutlich reduziert werden:

- Forensische Überprüfung
- Neuaufsetzung der Infrastruktur in sicherem Netzbereich
- Migration zentraler Datenbanken und Datenbestände in Netzbereiche
- Migration zentraler Server
- Neuaufsetzung verdächtiger Server- und Client-Betriebssysteme

### Erreichte Erfolge

Erfolgreiche Abwehr des Major Incidents, mit Bereinigung aller Systeme von Malware und Neuaufsetzung der Umgebung. Jegliche Geschäftsprozesse wurden in den Regelbetrieb übergeben.

Bedrohungen werden zukünftig frühzeitig erkannt, durch die Anbindung an unser Security Operation Center (as a Service).

Verbesserung der IT-Infrastruktur:

- Apex One
- Threat Intelligence
- Sandboxing
- Deep Security

# 08 BEST-OF-BREED

Nur wenn Menschen, Know-How, Prozesse und Technologie im Einklang sind, können Security-Lösungen ihre maximale Wirkung entfalten. Dabei spielt die Technologie natürlich eine zentrale Rolle.

Richtig konfiguriert, verlassen Sie den Pfad der Standardlösung. Wir bieten Ihnen ein breites Spektrum der marktführenden Sicherheitslösungen und Technologien und zwar aus einem guten Grund: Ihre IT-Sicherheit verdient es.

Mit unserem Best-of-Breed Ansatz schaffen wir Synergien zwischen den Technologien und produzieren erlebbare IT-Security Umgebungen.

suresecure GmbH
Hausbroicher Str. 296D
47877 Willich

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de