HealthCare Digital Webcast
25.01.2023

SONICWALL®

UNBEKANNTE BEDROHUNGEN UND DIE RISIKEN FÜR B3S UND KRITIS

UNBEKANNTE BEDROHUNGEN DIE UNTERSCHÄTZE GEFAHR

Marcus Lind

Enterprise Account Manager - HealthCare

SonicWall GmbH

Unbekannte Bedrohungen und die Risiken für B3S und KRITIS

Was erwartet Sie heute?

Sie erhalten im Vortrag eine Übersicht der aktuellen Bedrohungslage, welche sich gerade dramatisch ändert und welche Maßnahmen für 2023 auf Ihrer Agenda stehen sollten. Einige der Punkte wie den Schutz vor unbekannten Bedrohungen werden explizit im Bereich KRITIS & B3S aufgeführt.

Cybersecurity Versicherungen nehmen diesen Punkt Explizit in Ihre Bewertungsfragenkataloge auf

Was heißt dies für Sie als Cybersecurity Verantwortliche?

SONICWALL®

Unbekannte Bedrohungen und die Risiken für B3S und KRITIS

Gliederung

1. Überblick über die aktuelle Bedrohungslage
2. Was sind aktuelle Anforderungen für B3S und KRTIS und die sich daraus ergebenden Handlungsempfehlungen
3. Ein Fallbeispiel aus der Praxis eines Krankenhauses

SONICWALL®

1. Überblick über die aktuelle Bedrohungslage

SONICWALL

A CYBER WAR OF REVENUE

CYBERSECURITY

1X

2021 Market Value **$160 Billion**
Averaged as **11% CAGR**
2025 Estimate **$250 Billion**

CYBERCRIME

40X

2021 Market Value **$5 Trillion**
Averaged at **15% CAGR**
2025 Estimate **$10 Trillion**

Driver: Responsibility, duty
Focus: Stretched, multiple responsibilities
Overhead: Reactive, manual tasks (or log/alert fatigue)
Effort: Individuals; limited skills and resources

Driver: Earnings, greed
Focus: Likely to be very focused on the task
Overhead: Automation, scaled and efficient
Effort: High volumes, millions of sources

1. Überblick über die aktuelle Bedrohungslage

THE REALITY

Risk escalates with the explosion of exposure points and remote/ mobile work

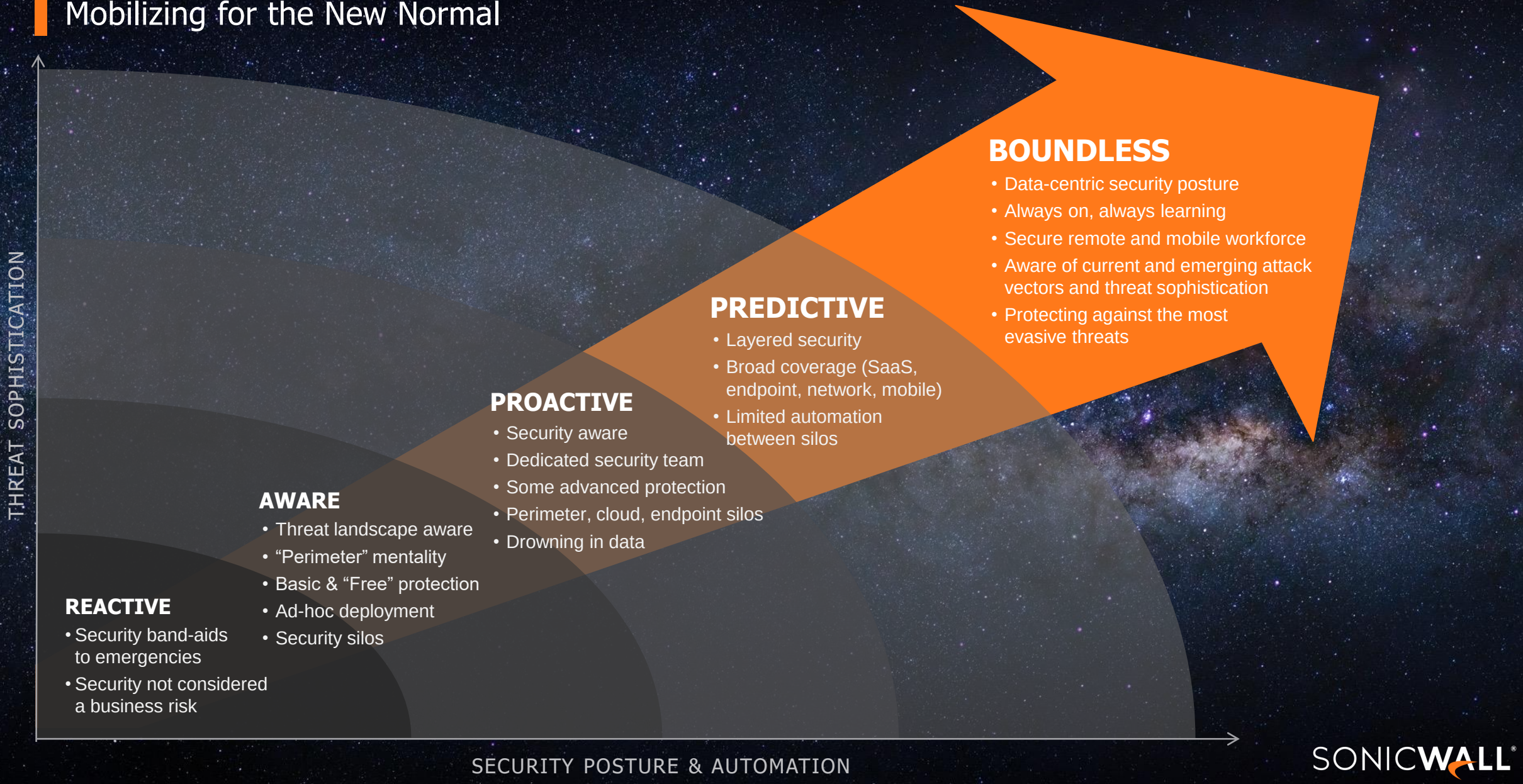
Cost becomes prohibitive and the shortage of trained personnel becomes more acute

Constrained resources can't keep up

SONICWALL®

THE JOURNEY TO BOUNDLESS CYBERSECURITY

Mobilizing for the New Normal



SONICWALL®

1. Überblick über die aktuelle Bedrohungslage

BOUNDLESS CYBERSECURITY

Bridging the Cybersecurity Business Gap

- **WHEREVER HUMANS WORK**
  remote/mobile, any location, across borders
- **WHEREVER APPS ARE**
  on-prem apps to cloud apps
- **EVERY KIND OF THREAT**
  known and unknown threats
- **EVERY POSSIBLE ENDPOINT**
  IoT, sensors, devices (PCs to wearables)
- **EVERY TYPE OF INFRASTRUCTURE**
  SaaS, IaaS, containers, virtualization, cloud, hybrid
- **ANY TYPE OR SIZE OF NETWORK**
  segmented networks, 5G
- **ANY TYPE OF BUSINESS**
  size of company, verticals

SONICWALL®

2. Was sind aktuelle Anforderungen für B3S und KRTIS und die sich daraus ergebenden Handlungsempfehlungen

- B3S + KRITIS Anforderungen für 2023
  - ✓ Beide Vorgaben haben als einen der neueren Kernpunkte die Erkennung von Unbekannten Bedrohungen
  - ✓ Das heißt eine Echtzeitanalyse zum Schutz vor aktuell noch nicht Bekannten Bedrohungen durch Analyse von Verhaltensmustern, Anomalien und der Kombination von bereits Bekannten Bedrohungen mit abgewandelten Komponenten
  - ✓ Lösen von Pattern basierten Lösungen hin zu Verhaltensbasierten Lösungen welche sich auch zukünftig Dienstübergreifend austauschen

- Cybersecurity Versicherungen nehmen die Themen TLS 1.3 und Schutz vor Unbekannten Bedrohungen in Echtzeit in Ihren Fragenkatalog auf um Anhand die Analysen zu Bewerten ob sich ein Unternehmen/Institution auf dem Stand der Technik schützt.

SONICWALL®

2. Was sind aktuelle Anforderungen für B3S und KRTIS und die sich daraus ergebenden Handlungsempfehlungen

- Dies Betrifft alle Bereiche von Vektoren die einen Angriff/Zugriff von Außen, aber auch aus dem Inneren Ermöglichen.
- Welche Bereiche sind dies?
- z.B. Firewalls, E-Mail Security, Endpoint Security, Access Points, Secure Mobile Access Lösungen, Zero-Trust Umgebungen, On Prem Sandboxlösungen, Mobile Devices
- O365 ist ebenfalls davon betroffen, eine Echtzeiterkennung von Bedrohungen hat auch Microsoft nicht im vorhandenen Sicherheitspaket und sollte somit dringend ergänzt werden

SONICWALL®

SONICWALL®

BOUNDLESS CYBERSECURITY

3. Ein Fallbeispiel aus der Praxis eines Krankenhauses

Im Fallbeispiel geht es um einen Krankenhausverbund mit 25+ Niederlassungen im Ruhrgebiet.

<u>Situation:</u>

Ziel ist die Erneuerung der Sicherheitsinfrastruktur auf den aktuellen Stand der Technik (unter andrem zum Schutz vor unbekannten Bedrohungen) im Rahmen der KRITIS Vorgaben, ein zentralisiertes Management und Konsolidierung aller Firewalls mit einheitlicher Bedienoberfläche, gesicherte E-Mail Kommunikation, Antiviren und SPAM Schutz mit aktueller Echtzeiterkennung (Sandboxlösung) sowie Secure Mobile Access, gesicherter Zugang zum Netz aus dem Home Office oder von unterwegs.

Wichtig war auch eine flexible Lösung für z.B. mögliche weitere Lockdown Szenarien.

SONICWALL®

3. Ein Fallbeispiel aus der Praxis eines Krankenhauses

Lösung:

Beratung hinsichtlich Vorgaben nach KRITIS und IT Sicherheitsgesetz 2.0 sowie Augenmerk auf die Erkennung von unbekannten Bedrohungen

Zum Einsatz kamen mehrere Firewall Cluster verschiedener Leistungsklassen, die Stück für Stück die zuvor gemischte Umgebung von mehreren Herstellern hin zu einer zentralen Managementoberfläche ablösten. Ziel war eine Segmentierung, die sowohl als Hardware wie auch in verschiedenen virtuellen Umgebungen Anwendung fand - über eine einheitliche Konsole.
Es wurde eine Secure Remote Access Lösung implementiert, die Mitarbeitern im Falle von z.B. Lockdown erlaubt, flexibel von Zuhause oder im Office zu arbeiten.

Ergänzend wird eine Email Security Lösung als Appliance mit Advanced Threat Protection (ATP) eingesetzt.

SONICWALL®

SonicWall 7x in Folge ausgezeichnet von den ICSA Labs mit 100% Erkennungsquote bei 0 False Positives

SonicWall setzt neuen Maßstab beim Schutz vor ausgeklügelten Bedrohungen.

Tag für Tag werden Tausende Organisationen zur Zielscheibe von Angriffen. Hand aufs Herz: Wenn Sie irgendwann im Fadenkreuz stehen, werden Sie einfach nur *hoffen*, dass Ihre Cybersicherheitslösung den gefährlichsten Bedrohungen von heute standhält – oder werden Sie sich entspannt zurücklehnen, weil Sie *wissen*, dass Ihr System Sie nicht im Stich lässt?

Über die letzten sieben Quartale – mehr als 223 Tage mit 9.071 Tests – wurde SonicWall Capture ATP mit RTDMI unabhängigen Tests durch das Prüfinstitut ICSA Labs unterzogen. Und über die letzten sieben Quartale hat SonicWall jede einzelne der 4.251 wenig bekannten Bedrohungen, von denen viele nicht einmal eine Stunde in Umlauf waren, identifiziert. So konnte SonicWall eine Bedrohungserkennungsrate von 100 % für knapp zwei Jahre aufrechterhalten.

Kein anderer Anbieter konnte so exzellente Ergebnisse auf diesem Niveau erzielen. Mehr noch: Niemand konnte auch nur annähernd so gut abschneiden wie wir. Erfahren Sie in unserer Lösungsübersicht mehr über den beispiellosen Erfolg von SonicWall bei der Perfektionierung der Sicherheit.

SONICWALL®

Sie möchten mehr zu Sicherheitslösungen im Gesundheitswesen erfahren?

- Besuchen Sie ww.SonicWall.de und laden Sie unser aktuelles Whitepaper „2022 - KHZG, KRITIS und IT-Sicherheitsgesetz 2.0: Sind Ihre Cybersecurity-Investitionen effizient geplant?“ herunter

- Erfahren Sie alles was wichtig ist in unserem IT-Security Podcast *Grenzenlos Sicher?* in der Folge „Operation KRITIS: Das Gesundheitswesen im Fokus von Cyberkriminellen“

- Sprechen Sie uns an – wir beraten Sie gerne!

SONICWALL

Vielen Dank für Ihre Aufmerksamkeit. Gibt es Fragen?

SONICWALL®

Marcus Lind
Enterprise Account Manager
SonicWall GmbH
Mobil +49 179 6904106
mlind@sonicwall.com

www.sonicwall.com

30 Years of SonicWall