GoSecure

USE CASE BROCHURE

REMOTE DESKTOP PROTOCOL (RDP)

ARE INCREASING EVERY YEAR

RDP IMPACT IN NUMBERS

95%

Attacks leveraging RDP in the first half of 2023, an increase from 88% in 2022.

74%

Of the 5.8 billion attacks on its UK honeypots in 2023, 74% targeted Remote Desktop Protocol (RDP).

Over 85%

Of organizations analyzed had Remote Desktop Protocol (RDP) internet-accessible for at least 25% of the month, leaving them open to ransomware attacks or unauthorized login attempts.

Your ally to consolidate, evolve & thrive

INFO@GOSECURE.AI

www.GOSECURE.AI

NAVIGATING THE RDP MENACE

In the fast-evolving landscape of cybersecurity, the utilization of RDP as a conduit for attacks has surged significantly. RDP is a network protocol enabling remote control of a computer attached to the internet.

This allows a remote user to see the computer's screen and control it as if physically present, with keyboard and mouse functionality. Authentication via a username and password is required for a remote desktop connection to be established.

Cyber actors can exploit vulnerabilities in the connection between local and remote machines, injecting malware or ransomware into the system. The insidious nature of RDP attacks lies in their ability to bypass user input, making intrusions challenging to detect.

This heightened risk is compounded by the surge in remote work during the pandemic, rendering RDP a favored target for criminal hackers. Just as phishing capitalizes on human error, RDP attacks target weaknesses in network defenses, emphasizing the urgent need for continuous vigilance and robust security reinforcement.

POTENTIAL RISKS WHEN FACING AN RDP ATTACK:

- UNAUTHORIZED ACCESS
- RANSOMWARE ATTACKS
- DISRUPTION OF OPERATIONS
- INTELLECTUAL PROPERTY THEFT
- FINANCIAL LOSS
- RESOURCE EXPLOITATION
- REPUTATION DAMAGE
- LEGAL CONSEQUENCES
- OPERATIONAL INEFFICIENCIES
- OPERATIONAL COSTS FOR REMEDIATION

Worse yet, users with elevated privileges could inadvertently give hackers the “keys to your kingdom”.

GoSecure

THE LEADER IN MANAGED DETECTION & RESPONSE

We deliver industry-leading response and mitigation speed to keep up with today's growing threats.

YOUR ULTIMATE ALLY

GoSecure combines more than 20 years of market-leading security technology with highly skilled professionals who become an extension of the in-house security team to mitigate threats before they can compromise sensitive data or business operations—maximizing valuable resources.

At GoSecure, we stand as a beacon of innovation and excellence in the ever-evolving landscape of cybersecurity. With a robust foundation built on cutting-edge research, unwavering dedication, and a relentless pursuit of knowledge, we have emerged as leaders in the field.

Choose GoSecure for your ultimate ally with a proven record of expertise, research excellence, and a commitment to addressing the ever-evolving landscapes of RDP and phishing threats. Our notoriety in the cybersecurity world is a testament to our dedication to providing innovative, effective solutions that safeguard organizations in an increasingly complex digital environment.

LEARN MORE

WHAT WE DO?

RESEARCH EXCELLENCE

Our commitment to cybersecurity is shown through 6,193 hours of research only on Remote Desktop Protocol (RDP) and phishing, contributing greatly to the field.

GLOBAL PRESENCE

GoSecure spans 3 continents and 4 countries, making its mark at major conferences like RSA and BlackHat, showcasing our leading-edge in cybersecurity.

NOTABLE CONTRIBUTIONS

GoSecure's real-world applications of its research have significantly advanced solutions to cybersecurity challenges, impacting the industry profoundly.

RDP AND PHISHING MASTERY

Specializing in RDP and phishing research, GoSecure's expertise is vital in protecting against these growing threats, ensuring organizations' cybersecurity resilience.

INFO@GOSECURE.AI

www.GOSECURE.AI

Your ally to consolidate, evolve & thrive

Your ally
to consolidate,
evolve & thrive

GOSECURE TITAN® MANAGED EXTENDED DETECTION & RESPONSE (MXDR)

DETECT & MITIGATE FASTER

GoSecure Titan® Managed Extended Detection & Response (MXDR) offers the best-in-class response time from threat detection to mitigate with a solution that identifies, blocks, & reports potential breaches.

With early warnings, GoSecure Titan® MXDR blocks many attacks before they can impact an organization while consolidate critical security data, provide unmatched visibility and deliver proven protection with customizable views. We work with teams to address evolving threats, changing technology and constrained.

UNVEILING GOSECURE TITAN® MXDR

ELEVATING CYBERSECURITY THROUGH RDP EXPERTISE

In the ever-evolving landscape of cybersecurity, GoSecure stands as a beacon of innovation, particularly in the realm of Remote Desktop Protocol (RDP). Our commitment to excellence is not merely a claim but is substantiated by a wealth of data that underscores our unrivaled expertise in the field.

Organizations grappling with the growing threat of RDP attacks find in GoSecure Titan® MXDR not just a solution, but a proactive and comprehensive defense strategy.

GoSecure Titan® MXDR offers an unparalleled RDP defense that is backed by years of dedicated research, a global presence that reflects our influence, and a commitment to turning insights into impactful solutions.

Our service offering is fortified by our commitment to translating insights into impactful solutions. As cyber threats evolve, GoSecure Titan® MXDR remains at the forefront, ensuring organizations fortify their cybersecurity resilience with cutting-edge expertise and proactive defense measures.

GoSecure Titan® MXDR stands as the epitome of excellence, providing organizations with a top-tier defense to navigate the complexities of the digital landscape.

A FOUNDATION YOU CAN TRUST & BUILD UPON

GoSecure Titan® MXDR consolidate critical security data, provide unmatched visibility, and deliver proven protection with customizable views. We work with teams to address evolving sophisticated threats like ransomware and fileless attacks, changing technology and constrained resources.

LEARN MORE