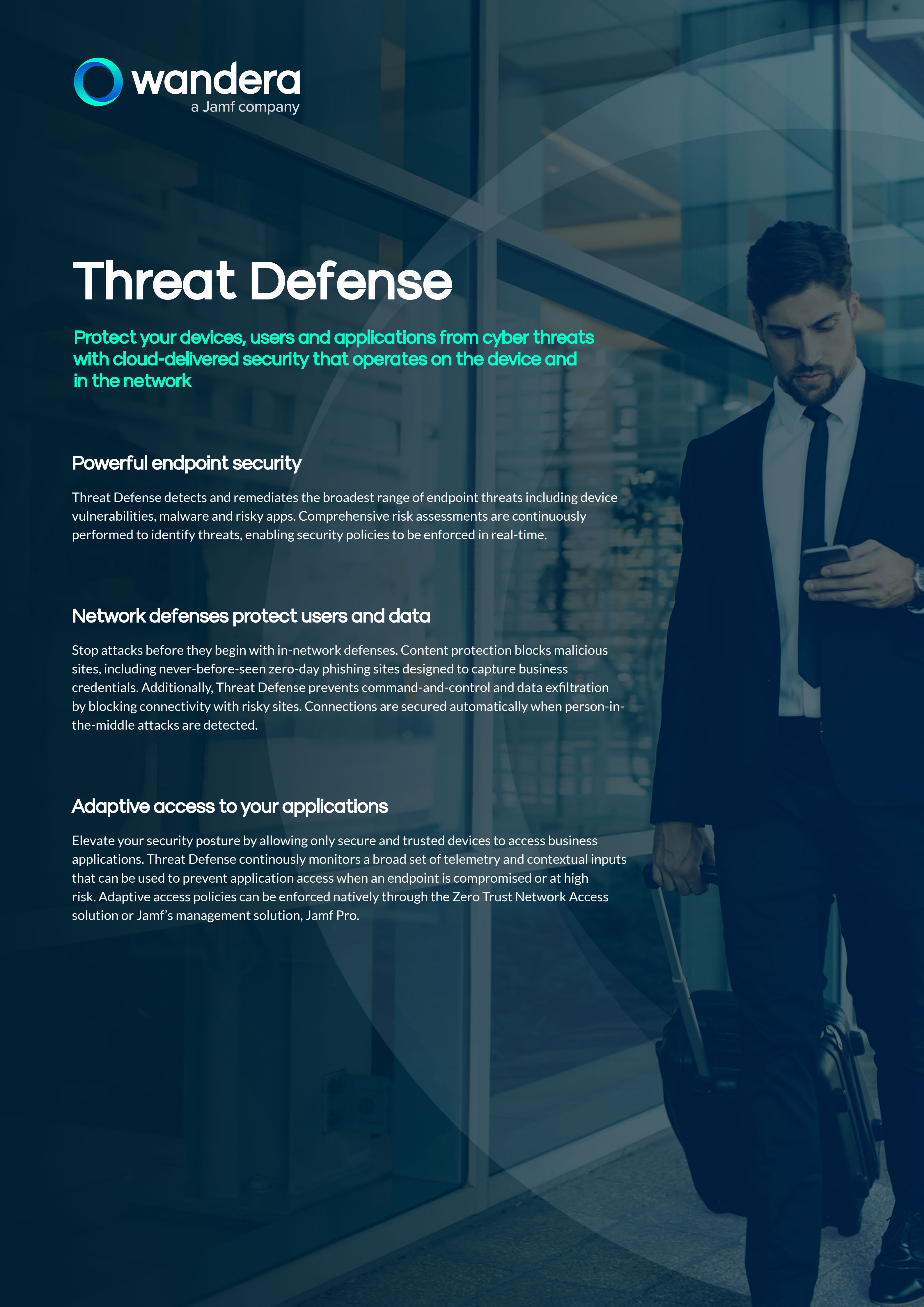

wandera
a Jamf company

# Threat Defense

## Protect your devices, users and applications from cyber threats with cloud-delivered security that operates on the device and in the network

### Powerful endpoint security

Threat Defense detects and remediates the broadest range of endpoint threats including device vulnerabilities, malware and risky apps. Comprehensive risk assessments are continuously performed to identify threats, enabling security policies to be enforced in real-time.

### Network defenses protect users and data

Stop attacks before they begin with in-network defenses. Content protection blocks malicious sites, including never-before-seen zero-day phishing sites designed to capture business credentials. Additionally, Threat Defense prevents command-and-control and data exfiltration by blocking connectivity with risky sites. Connections are secured automatically when person-in-the-middle attacks are detected.

### Adaptive access to your applications

Elevate your security posture by allowing only secure and trusted devices to access business applications. Threat Defense continously monitors a broad set of telemetry and contextual inputs that can be used to prevent application access when an endpoint is compromised or at high risk. Adaptive access policies can be enforced natively through the Zero Trust Network Access solution or Jamf's management solution, Jamf Pro.

## Comprehensive threat detection and prevention

Threat Defense identifies and stops the broadest range of cyber threats

### Real-time network protection

Threat Defense dynamically detects and blocks attempts to steal user's credentials to ensure that even never-before-seen phishing attacks are unsuccessful. A wide range of factors are scanned such as brand imitation, suspicious punycode and subdomain entropy. The in-network protection denies attacks sent via email, social media and SMS.

### Risky configuration detection

Detailed posture assessments provide organizations with visibility of endpoint risks, from escalated privileges to outdated OSs. Granular controls enable security policies to be enforced via remediation actions, such as end user prompts, blocking malicious connections or restricting access to corporate resources.

### Detailed app insights

Understand the risk apps pose at a glance, known vulnerabilities are highlighted along with MI:RIAM's app risk score and recommended remediation actions. Detailed forensics can be reviewed to understand the permissions required, URL communicated with or third-party libraries used by specific versions of an app.

### Communication interception prevention

Public Wi-Fi connections are an ideal platform for malicious actors to launch attacks. Threat Defense protects devices connected to Wi-Fi with Failsafe Encryption. When an attack is detected, Threat Defense automatically encrypts the user's traffic allowing them to continue working in safety without disrupting their connection.

## Leading security features and capabilities

Strong protection for every use case and compatible with any system

### Always-on endpoint defense

Protect users and devices from cyberthreats no matter where they are. Wandera's endpoint app identifies malicious software, vulnerable configurations and risky connections before a breach can occur. Remediation actions and alerts are triggered automatically to mitigate any potential threats.

### Real-time reporting and policy controls

The unified policy engine allows administrators to quickly configure a security policy, enforcement occurs immediately allowing policies to be tuned and tailored on the fly. Detailed insights can be viewed inside the Threat Defense portal or in a SIEM/SOAR dashboard via out- of-the-box integrations or a suite of APIs and datastreams.

### Conditional Access policies

Prevent business applications from being accessed by risky users or devices with Conditional Access. The permissions of managed corporate and unmanaged BYO devices are revoked until they are assessed as safe. Policies can be enforced natively within the Threat Defense network or via integration with Jamf or IdP.

### Unified operations and management

Integrating Threat Defense with a management solution like Jamf or IdP allows information about organizational user groups to be synced. This allows Threat Defense to be deployed quickly to devices and makes assigning user permissions easy. The integration also simplifies event monitoring and threat hunting for ThreatOps by adding human readable names to reporting.

## Powered by MI:RIAM

MI:RIAM is an advanced threat intelligence engine; it works in real time to identify the broadest range of known and zero-day threats. Built on the largest set of threat data, MI:RIAM collects information from 425 million sensors around the globe as input into its algorithms. MI:RIAM utilizes advanced data science to provide security leaders with real-time insight into the latest threat intelligence and active risks to the business.

To learn more about how Threat Defense can protect users, mobile devices and organizational data from malicious intent, please visit jamf.com.

wandera
a Jamf company