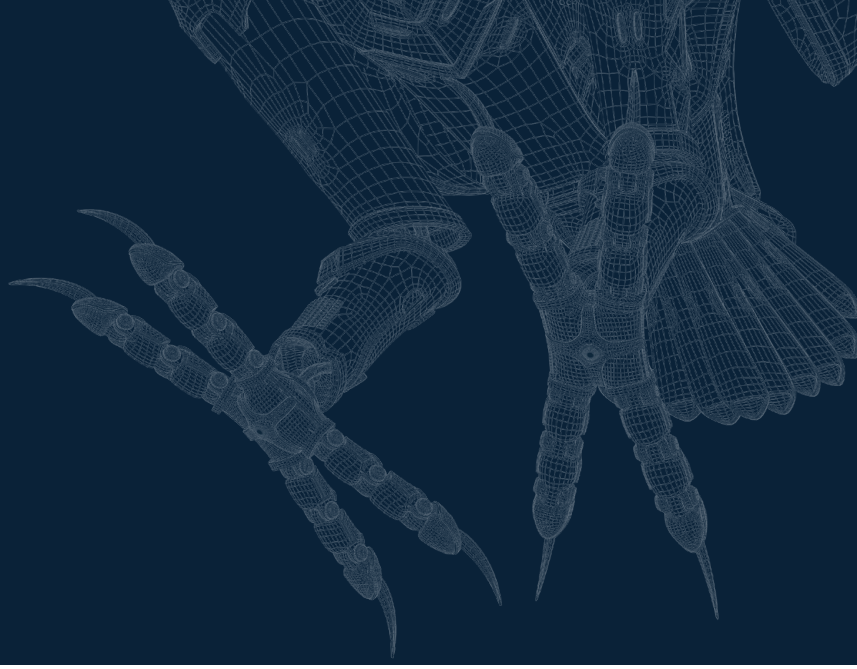
cybereason | CASE STUDY

TX GROUP



COMPANY

TX Group

INDUSTRY

Media

NUMBER OF ENDPOINTS

6000 (3,700 employees)

USE CASE

Secure anywhere, anytime access for agile development and collaboration

THE CHALLENGE

- Need for a security partner that can handle multiple agile companies
- Support remote workers accessing critical applications
- Need a security partner for 24/7 monitoring and incident response

SOLUTIONS

- Reduced the attack surface for remote workforce (½ the incidents)
- Real-time protection, detection, and response across all endpoints
- Fused context across endpoints, **Google Workspace, Okta, AWS, and Digital Shadows**

The Challenge

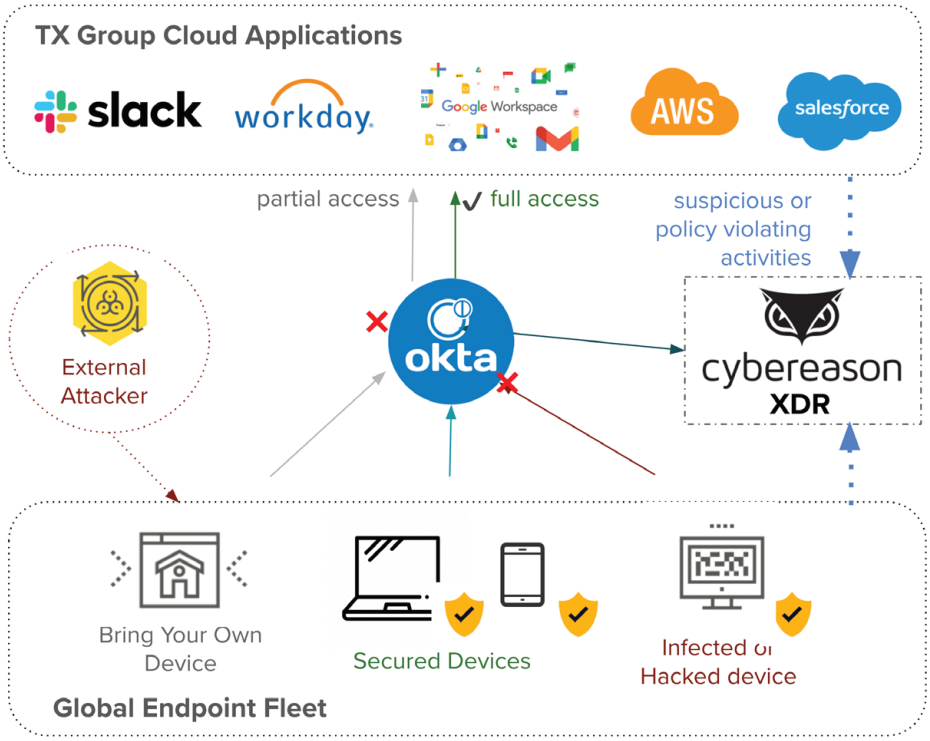
Andreas Schneider, Group CISO at TX Group, is tackling one of the greatest unsolved problems in cybersecurity today: "How can we thoughtfully automate our security team?"

This is a tall order, especially in light of our ever-evolving world. The pandemic has not only changed the face of remote work, but have forced nearly every company today to reevaluate their development, IT, and security strategies. Adversaries are launching more attacks with automation and have become ruthless with data theft and extortion to achieve ransom demands.

Since 2018, TX Group has worked to be a cloud-first company, adopting a **zero trust framework and an agile security strategy**. This means instead of a hardened perimeter with firewalls and VPN, users should be able to access all of their business applications from any device, any time, and anywhere.

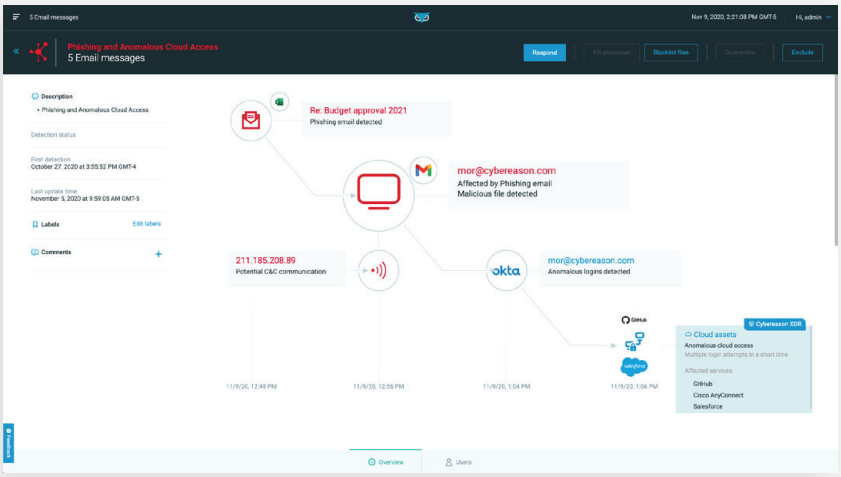
In order to secure a work anywhere environment, Andreas wanted a solution that not only provided direct visibility into global endpoints, but could monitor and understand access to critical applications across cloud and on-premises. For example, if an unknown or bring your own device (BYOD) is being used to access an application, always require two-factor authentication. Or, if malicious operations have been detected on an asset, automatically limit the associated user's access to critical applications.

In the past, Andreas and his team had used multiple security information and event management (SIEM) tools. The data lake approach didn't meet their needs: there were visibility blind spots, manual work when reconciling events, and there wasn't a reduction in mean time to respond (MTTR). TX Group **didn't want to centralize log data in a single place**—they wanted a **threat detection technology that could secure their zero trust** deployment and more importantly, take automated responses.

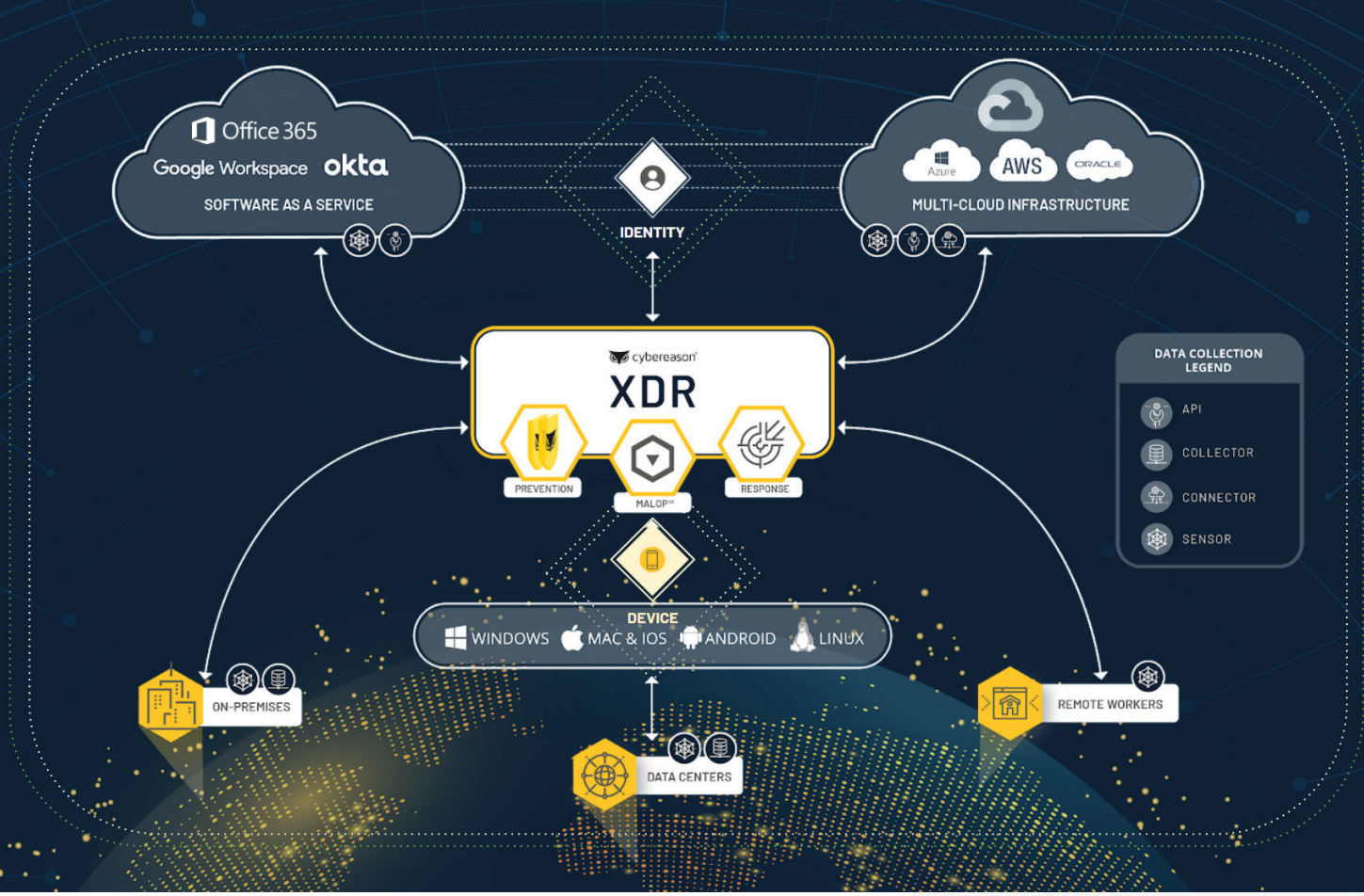


The Solution

Since 2018, TX Group has looked to Cybereason EDR to protect Windows, Mac, and Linux endpoints across the company and their subsidiaries. Cybereason was originally chosen for its flexible support for **on-premises and air-gapped environments**, strong pre-built detection coverage, and because Cybereason exposes Malops (malicious operations), a fully correlated narrative and deep context about an attack as opposed to individual alerts and alarms for each detected behavior.



The two teams worked closely together to extend TX Group's detection and response capabilities across cloud services and infrastructure. With the direct integrations with **Okta, Google Workspace, Digital Shadows, Fortinet and AWS**, Cybereason XDR automatically surfaces anomalous user behavior, insider threats, and makes it easy to understand the full attack story behind any incident.



The Outcome

Since expanding to XDR in Summer 2020, the team has gained more visibility, identified multiple suspicious behaviors including MFA bypasses and other Okta intrusion attempts, and have already set up a first Slack notification and response bot to reduce remediation time and efforts. **Unlike SIEM tools, Cybereason correlates endpoint telemetry against user identities and access behaviors.** This approach detects threats that would otherwise be overlooked as weak signals and greatly accelerates incident triage and investigation times.

Andreas continues to update the board at TX Group on the implementation of their agile, zero trust security strategy. Because they chose cloud-first, the TX Group team **reduced their overall attack surface, friction to end-users, and even their number of incidents**—in spite of the pandemic and rise in cyber attacks. Instead of investigating individual alerts and tools, the team is focused on the broader mission: "Which of my users and assets are at risk? Did our user click on a phish and enter credentials or download malware? If yes, automate the response where best feasible." Both teams are looking forward to expanding the XDR deployment across more TX Group brands and adding new use cases that enable focusing on the relevant chain of events.

"Cybereason is a trusted security partner who is continuously evolving to stay future-ready. XDR allows us to understand beyond our endpoints by monitoring user identities and access. This extended detection and response has already revealed risky behaviors and allows us to focus on the most relevant threats."

ANDREAS SCHNEIDER
Group CISO, TX Group

Learn more at Cybereason.com →

cybereason