Petri IT Knowledgebase Resource
A BWW Media Group Brand

PETRI
WE GET IT

Petri Webinar Brief
March 18, 2020

How to Secure Teams From External Threats and Data Loss

How to Secure Teams From External Threats and Data Loss

Presenter: Matt Smith, Senior Solutions Architect at CoreView
Mike Otey, President of TECA, Inc.

Moderator: Brad Sams, Petri IT Knowledgebase, Executive Editor at Petri.com

Overview

Microsoft Teams is arguably the most powerful workplace productivity tool on the market. But with such a robust solution comes a myriad of potential vulnerabilities that could affect your day-today business. In fact, both Gartner and Forrester report that 80% of SaaS breaches stem from misconfiguration, inappropriate user behaviors, or incorrectly allocated user permissions.

In the webinar, Mike and Matt discussed:

- The latest features and updates to Teams
- Best practices on keeping threats out and people productive
- Common Office 365 specific vulnerabilities you can mitigate against
- How to improve response time to hacker attempts by 500%

The full webinar dives deep into each section to help the listener better understand the best-practices of the industry. This tech brief will provide an overview of everything Matt and Mike discussed.

What is Microsoft Teams?

Microsoft Teams is the newest application from Microsoft that brings a unified chat, calling, meeting and collaboration hub to every user of Office 365 for small businesses up to enterprise operations; there is also a free version available as well.

The application has seen substantial growth with 44 million daily active users, this is up from 20 million in Nov 2019. Nearly every single Fortune 500 company is now using the application and Microsoft reports that they have several customers with more than 100,000 users of the platform.

Teams has become the central tool of the Office 365 ecosystem and with the significant rise in remote work, Teams is the application that is enabling this work-scenario with little overhead to IT shops.

Challenges for Remote Workers:

The rise in remote work is enabling new challenges for IT who are provisioning VPN tokens and remote hardware at levels that have rarely been seen before. This means making sure your users know how to use VPNs, Teams, webcams, Bluetooth peripherals and updating their software, and a lot more, is critical to your operational success. In controlled environments, this is not a significant burden but in remote scenarios, the complexity increases.

With more employees working from home, the increase of sophisticated attacks are on the rise. Emails that contain phishing links related to COVID-19 are successfully tricking users into releasing their credentials as many emails are disguised to look like emails from Microsoft or an employee at your company.

These phishing attacks are growing in their success rate thanks to mixing personal and work devices and using multiple email services on devices that connect to corporate networks.

Challenges for Remote Workers:

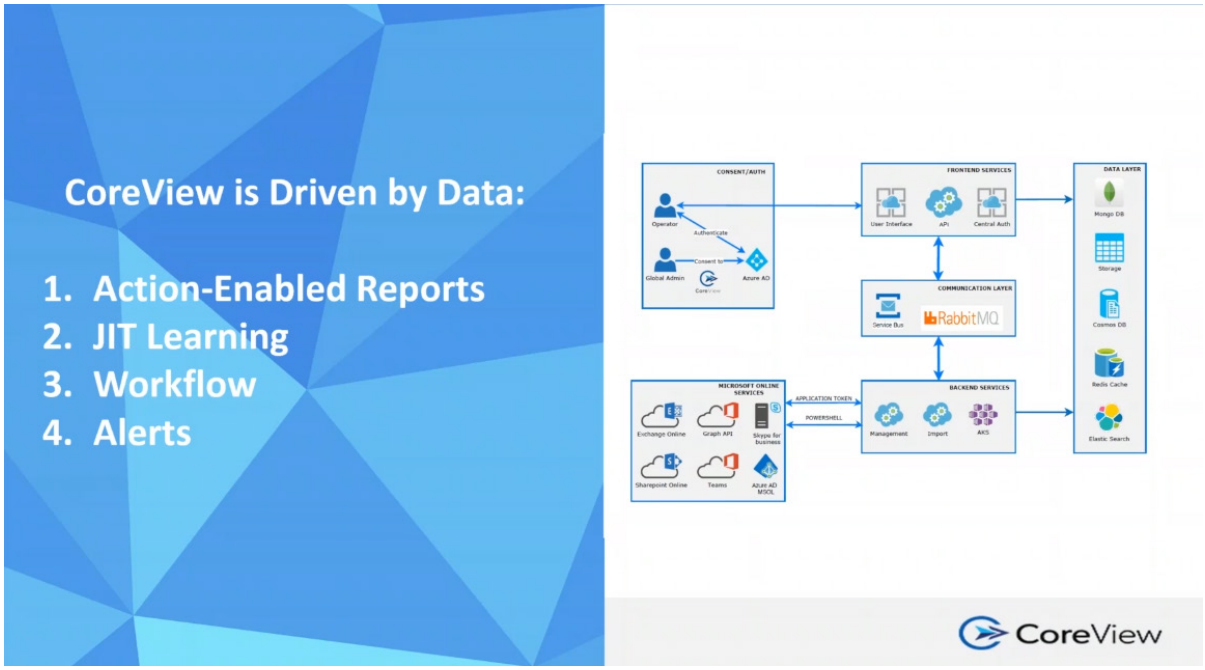
To help protect users, there are basic configurations you can use to help keep your data and environment protected.

A best practice is to enable strong passwords but more importantly, multi-factor authentication (MFA). Further, it's important to monitor Teams usage and look for outliers of activity including suspicious login attempts by volume or location.

One of the most important steps is user education. Making sure that the user knows what a phishing attempt looks like, to never share credentials, and to how MFA operates, is your best first-line defense.

CoreView's Office 365 Solution:

Coreview is a SaaS management platform for Microsoft Office 365 that allows you to gather, report, and act on data monitored from an Office 365 tenant. This includes auditing, workflow automation, administration, role-based access control, policy management, and licenses management.



The CoreView software connects to all the available API endpoints to help create a security view that you cannot find any other way than through these connections.

By collecting all of the data, CoreView is able to provide a significant level of insight into how, where, and what a user is doing and the hardware they are using to complete these tasks. And crucially, if the user that is connecting to your tenant is secure and what security policies are in place to protect the user and your data.

The key is being able to see the right information, at the right time, but not be overwhelmed with false-positive alerts. With CoreView's workflow and alerts, you can help users stay updated with the correct policies and also make sure your environment remains protected.

In the webinar, Matt dives deep into how all the information CoreView is able to surface through its platform can make IT administrators more productive, your environment more secure, and help users be more productive as well.

In the webinar, Matt details five killer features of the platform that are outlined below:

1. **BYOD Configuration Management**
    - **a.** Report on who owns what device, with what OS, and which device management policies (if any) have been applied.
2. **User Training and Adoption Campaigns**
    - **a.** See all applications a user is using and reporting of what features are being used to identify additional training opportunities.
    - **b.** Drive user to 1800 Just-in-Time learning videos that are context specific and uniquely designed for CoreView's platform.
    - **c.** Identify, set up, and track adoption campaigns so that users can learn easily.
3. **Audit of all Office 365 Activities**
    - **a.** Provides 12 months (or longer) data retention (instead of Microsoft; s 3 months)
    - **b.** Ability to run e-discovery to highlight actions taken on responsive items.
    - **c.** Audit file access and email forwarding after a malware/ransomware attack.
    - **d.** Audit access when a user on/offboards.
    - **e.** Create security responsive plans for FINRA and other regulatory requirements
4. **Desired Configuration Management Alerts**
    - **a.** Alerts when a service account logs in.
    - **b.** Alert when partner or application is added to the company.
    - **c.** Alert when a member is added to a critical security group.
    - **d.** Alert when delegated admin performs actions that incur costs.
5. **Secure Delegation**
    - **a.** Exposes all management actions at a granular level with a single UI
    - **b.** Deploys in minutes
    - **c.** Delegate based on Azure AD properties like "Department" or SMTP domain
    - **d.** Delegate admins can manage Teams Call queues, auto attendants etc.

CoreView's solution helps you take command and control of your Office 365 tenant. CoreView pulls everything into a single pane of glass view, so you can manage application policies, delegate and automate responsibilities, take corrective action and track application usage from one efficient and illuminating vantage point.

Additional Information

Coreview offers demos and more for its solutions, check out their resources to learn more.

CoreView