

テレワークやリモートワークをサイバー脅威から守る最新のソリューションが新登場！

世界初！

テレワークやリモートワークに使われるパーソナルデバイスを
セキュリティ保護してリスクを低減



※フロリダキーズ大学は、フロリダ州
キーウェストにあるコミュニティカレッジ
です。

Vicarius社は、新しいWFH(work-from-home:在宅勤務)パラダイムにとって重要である迅速且つ効率的な
“SaaS型”リスク軽減対策ツール(TOPIA)をカレッジ・オブ・ザ・フロリダキーズに提供しました。

“Vicarius社のプロアクティブなソリューションは、他のどのソリューションよりも良く且つ迅速に
組織全体にわたるリスクを低減することができました！”

Michelle Adam氏、IT担当VP、College of the Florida Keys

● 課題

当カレッジ・オブ・ザ・フロリダキーズでは教師及び学生にZoomで勉強することを強いるWFHパラ
ダイムシフトに伴い、リモート資産を保護する方法を必要としていました。リスクにさらされることは
ネットワーク境界に接続されたあらゆるデバイスにわたって広がるので、最新のパッチ適用機能
を備えたクラウドベースのソリューションを見つけることが重要でした。

加えて、臨機応変的なループの中で作業することは、何が来るかを同カレッジのチームが予測
できない時にリスクを低減することを非常に困難にしていました。カレッジ・オブ・ザ・フロリダキ
ーズにとっては、学生のプライバシーが常に一番大事であり、学生のプライバシーを保護するこ
とが主な優先事項でした。しかし、同カレッジは、先だってリスクの解析及び軽減を提供するソ
リューションを必要としていました。そこに現れたのがVicarius社でした。

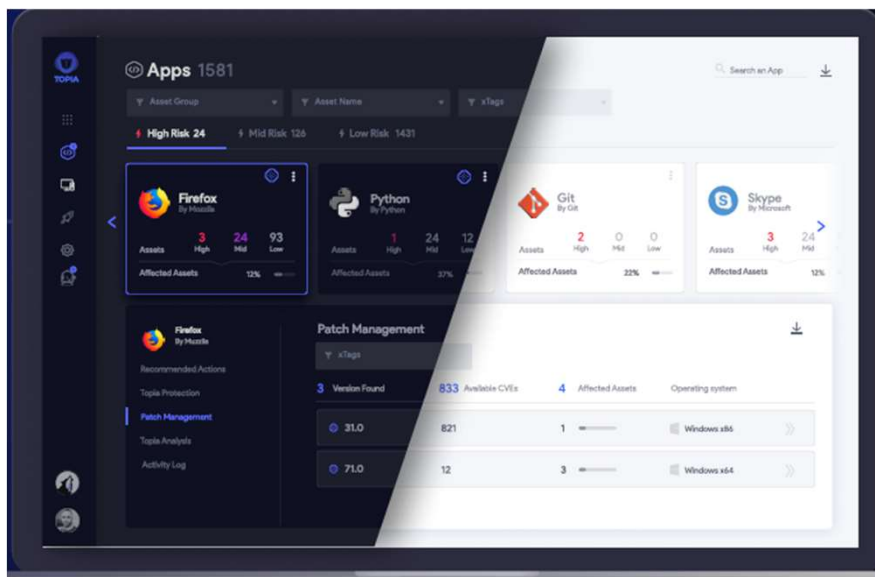
● 結果

- TOPIAのリスク解析エンジンは、カレッジ・オブ・ザ・フロリダキーズがエクスプロイトの対象になり
易い複数の高リスクのアプリケーションを特定するのに役立ちました。
- 2週間以内に、カレッジ・オブ・ザ・フロリダキーズは、TOPIAの脆弱性管理ツールによってリス
クレベルを大幅に低減しました。
- TOPIAにより、カレッジ・オブ・ザ・フロリダキーズは、リスク低減の取り組みに対してリアクティブ
ではなくプロアクティブなアプローチを取ることができるようになりました。

- Vicarius社のパワフルなソリューションは、コンプライ
アンスやミタリグレードのサイバー保護を確実な
ものにします。

TOPIAの脆弱性管理サイクル

- 1) 資産と脆弱性の検知と解析
- 2) 環境からデータ収集しコンテキストベース化
- 3) クリティカルな脆弱性の優先付け
- 4) 脆弱性に対する対策の提供



**脅威や攻撃から保護された「安全なエージェント」を用いた
テレワーカーやリモートワーカー、支店、グループ企業を守る最新の「SaaS型」サイバーセキュリティソリューション！**

xTags Summary

Dynamic exploit factors are being detected by exploitation tags (xTags). Each xTag designed to highlight unique factors across the entire organization, which may result in a potential breach.

Organization Top xTags

xTags Name	Affected Apps	Affected Assets
#attack_surface	58	14
#known_vulnerability	31	11
#has_patch	32	9
#availability_impact_if_exploited	25	11
#has_exploit	24	11

272 Installed Apps



Top 10 Risky Apps

ID	Versions	Assets	0-Day	CVE	Risk Level
Sudo	2	4	0	6	High
Anydesk	1	1	19	1	High
Tcpdump	2	5	0	28	High

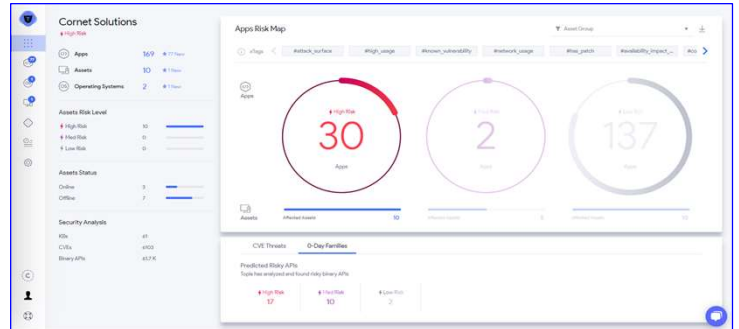
Apps Summary

272 Installed Apps



Top 10 Risky Apps

ID	Versions	Assets	0-Day	CVE	Risk Level
Sudo	2	4	0	6	High
Anydesk	1	1	19	1	High
Tcpdump	2	5	0	28	High
Sqllite	1	1	0	23	High
JRE	2	2	515	6	High
Bluez	2	2	0	5	High



- **CVEやバイナリレベルの脅威を検出するTOPIAは、公式のCVEなしに脆弱性について専用アプリケーションまでも解析することができる世界初の「SaaS型」オールインワン脆弱性管理ソリューションです！**
- **業界初のパッチレス脆弱性管理(再起動は不要です！)**
TOPIAのPatchless Protection™機能は、「パッチ後の再起動などによりシステムを止められないケースや、ミッションクリティカルなインフラ」などに、ベンダーが提供するパッチを適用しなくても、ミッションクリティカルなインフラストラクチャを安全に保つことができます。高リスクの脆弱性のあるアプリをブロックし、迅速且つ安全に脅威から資産を守ります。



信頼できる唯一の情報源

組織は、サードパーティのソフトウェアセキュリティ管理に2~3の製品を使用しています。これらのシステムはほとんど単独で動作し、連携しないため、脅威を見つけて優先順位を付けるセキュリティチームと、パッチのインストールを使用して脅威を軽減するITチームとの間にギャップが生じます。

TOPIAを使用すると、企業は、緩和策が正常に伝達されると更新される1つのビューを持つことができます。



クラウドファーストプラットフォーム

従来の脆弱性スキャナーはオンデマンドのネットワークスキャンを実行し、優先順位付けソリューションは境界ベースのログを収集し、現在のパッチ管理プラットフォームは内部ネットワーク内に展開されます。

TOPIAは、スケーラビリティ、パフォーマンス、及び分散ネットワーク向けに設計されたクラウドファーストプラットフォームです。在宅勤務(WFH)の時代に最適です。



次世代のコンテキスト化 リスクスコアリング

今日の脆弱性管理プロセスには、組織的なコンテキストが欠けています。先進企業は優先順位付けソリューションを使用しますが、収集されるデータは限られており、スキャン結果に結び付けられていません。

TOPIAは、ゼロデイ脆弱性予測、実行ベースの悪用スコアリング、及びメモリ防御などの次世代機能を使用して、リスク管理プロセスにコンテキストを追加します

● Vicarius (本社イスラエル、設立:2016)

Vicarius社は、CISO、MSSP及びIT管理者向けに設計された**世界初の「SaaS型」オールインワン脆弱性管理プラットフォーム**により、重要なアプリ及び資産を保護するのを支援します。Vicarius社のパワフルなソリューションは、規制コンプライアンス及びトップレベルのミタリグレードのサイバー保護を確実なものにします。