wavex

# Are Security Visibility Gaps Increasing Your Risk of Data Breaches?

Microsoft Tier-1 Cloud Solutions Provider

Microsoft Partner
Microsoft
Gold Security
Gold Cloud Productivity
Gold Collaboration and Content
Gold Data Analytics
Gold Datacenter
Gold Cloud Platform

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2018

UKAS ISO 27001 INFORMATION SECURITY MANAGEMENT

WINNER Azure Partner of the Year 2018

CYBER ESSENTIALS PLUS

IT EUROPA EUROPEAN IT & SOFTWARE EXCELLENCE AWARDS 2019 FINALIST

# 1 The Equifax breach: cybersecurity complacency and lack of visibility

As one of the major credit reporting agencies, Equifax maintains a vast amount of sensitive personal and financial information, making the company a highly attractive target for cybercriminals. The Equifax data breach in 2017 was one of the largest in history, with 148 million people affected. And it should never have happened.

Equifax acknowledged on Wednesday, Sept. 13, that a patch for the Apache Struts CVE-2017-5638 vulnerability—exploited by cybercriminals as a gateway in — was available in March, well before the attacks began. However, Equifax had not updated the vulnerable software at the time of the breach, more than two months later.

As a result, criminals were able to exploit the vulnerability and gain access to Equifax files from mid-May through July of this year, more than four months after the vulnerability had been disclosed publicly.

Equifax was arguably brought down due to poor IT visibility; the Apache flaw was left unpatched because incomplete lists of IT assets hid the vulnerability from the security team. If the company had invested in regularly auditing its IT estate and monitoring patch levels, the security department could have patched it earlier, potentially avoiding the breach.

Not only does keeping an up-to-date dashboard of everything in your tech stack allow you to accurately monitor threats, it also helps prevent 'license creep' - when businesses end up footing licensing bills for software that they're not even using.

**Do you know what your security posture is?**

# 2 You can't secure what you can't see

You cannot monitor or protect devices and information you can't see. One of the first steps that any organization must take to reduce risk and improve overall security is to understand the activity that is taking place on their networks and computer systems.

To establish and align a security program with controls and technology applied correctly, organizations need to have complete security visibility.

# 3 The added value of security visibility

> Nearly **60%** of CISOs and decision-makers consider lack of visibility a major threat to their cloud infrastructure, according to Help Net Security.

Before security teams can do anything to protect their environment, they need to see and understand what is happening or about to happen.

This is precisely the why a single, visual dashboard is so important for event analysis, threat monitoring and mitigation - to ensure full-spectrum visibility into threats across the entire perimeter and beyond.

Having an understanding of their IT data allows organizations to manage it in line with internal business requirements. Organizations will benefit from:

### Enhanced security

Organizations can visualize key security metrics and have an informed understanding of vulnerabilities and risk. They can highlight the security risks to prioritize and apply appropriate remediation actions, avoid misconfigurations, and rectify compliance gaps.

### Improved efficiency

Having full transparency of their security data enables stakeholders to define holistic strategies focused on it. IT security metrics also help align IT investment to business strategy, customer experience, and cloud optimization, helping leaders determine the value of technology and building confidence in IT performance.

# 4 Comprehensive insights into your security posture

The APEX Security dashboard provides superior security visibility so you can understand the true scope of the risks and vulnerabilities your organisation faces and maximize the effectiveness of your efforts to protect it. Through continuous monitoring, broad measurement, and detailed security recommendations, APPEX lets you make data-driven decisions on how to better manage your resources and protect your organization.


## 1. Vulnerabilities

Data collected from APEX Secure provides you an overview of vulnerabilities across your network. The APEX Secure scan runs periodically (normally monthly).

Most cyber-attacks exploit vulnerabilities within software or devices therefore having visibility of these vulnerabilities is critical in determining your level of risk and plan appropriate remediation.

## 2. Public Identity

A major risk within any organisation is staff whose access to the system is generally managed with username/password and multi-factor authentication. However, many staff use their corporate credentials (email/passwords) when creating accounts on other 3rd party web sites. Many of these 3rd party organisations subsequently get hacked which provides hackers the logon details of your staff. The Wavex public identify platform checks exploited databases for the details of your staff. Staff whose details are within many exploited databases will be subjected to more cyber-attack attempt.

## 3. Office 365 & Azure

As most organisations move their data to the Cloud, they require greater visibility into cyber-crime.

IBM 2021 report stated most organisations take 212 days to detect a cyber-crime. Wavex Advanced Threat Detection (ATD)

is designed to dramatically reduce this by providing greater visibility of cyber-attacks and quickly validating the threat with staff.

This report shows risky behaviours which could constitute a cyber-attack attempt.

## 4. Data Loss Prevention

This report is designed to provide you an overview of breached data-loss-prevention (DLP) policies. For instance, you may restrict the use of credit-card numbers stored in documents. This provides you an overview of the breaches and APEX ATD will notify individuals should they infringe on a policy also.

## 5. IT Risk Register

Wavex maintain a risk register for areas where we have detected IT risks associated with your organisation. These are then reviewed within regular review meetings.

## 6. Patching Compliance

This report provides an overview of the patching levels across the organisation. Patching data comes from the APEX Remote Security Management platform.

## 7. Threats

This provides an overview of threats detected by your anti-virus solution across your end-points.

## 8. Phishing

To provide you a way to assess the susceptibility of staff to phishing emails. By populating the form an email will be sent to the specified recipients and a report will be sent to you list those individuals that engaged with the fake phishing email.

## 9. Security Recommendations

To provide you a way to assess the susceptibility of staff to phishing emails. By populating the form an email will be sent to the specified recipients and a report will be sent to you list those individuals that engaged with the fake phishing email.

**If you'd like to know more about our services please get in touch:**


 **www.wavex.co.uk**  **020 7030 3210**  **tellmemore@wavex.co.uk**