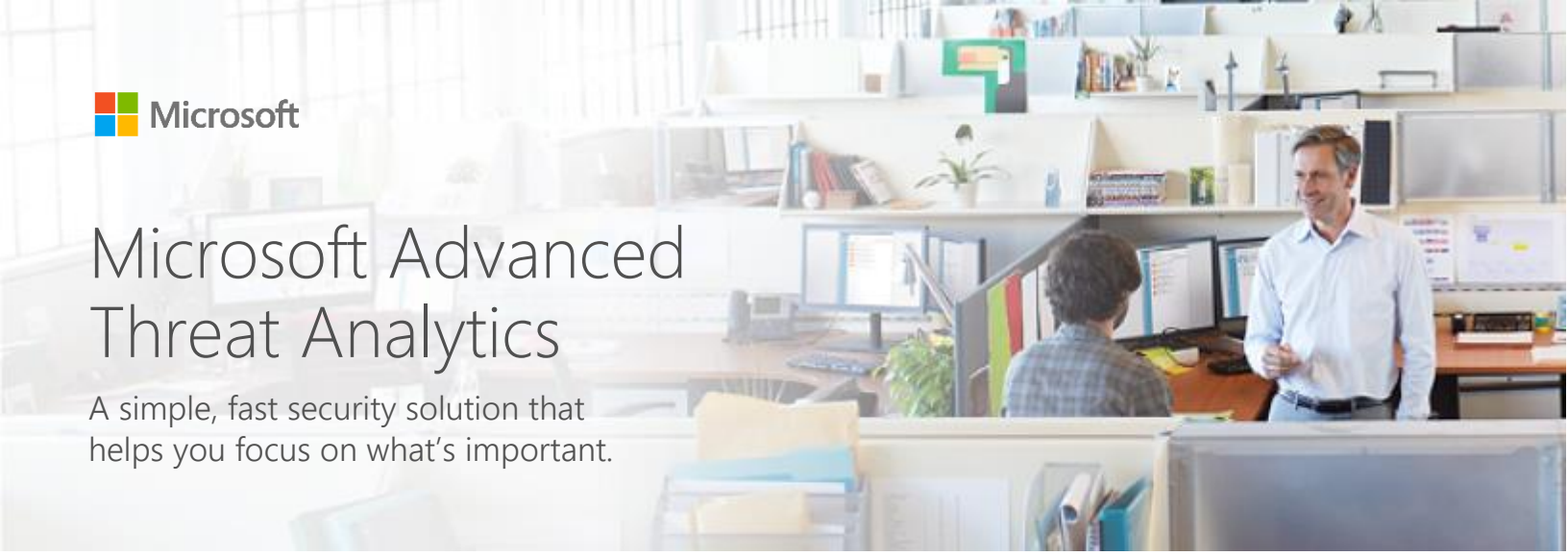


Microsoft

Microsoft Advanced Threat Analytics

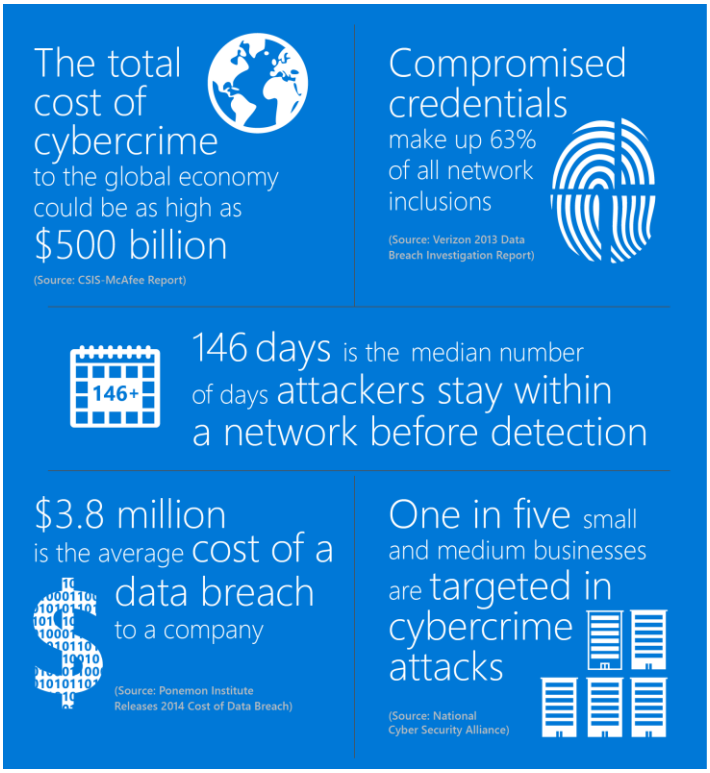
A simple, fast security solution that helps you focus on what's important.

Changing nature of cyber-security attacks

Today, the topic of cyber-security has moved from IT and the datacenter to the highest levels of the boardroom. Attacks and threats have grown substantially more sophisticated in frequency and severity. Attackers reside within a network an average of eight months before they are even detected. In the vast majority of attacks, they compromise user credentials and they are increasingly using legitimate IT tools rather than malware.

You are now working under the assumption of a breach. How do you find the attackers—before they cause damage?

Sobering statistics: the enterprise at risk



Microsoft Advanced Threat Analytics

Traditional IT security tools provide limited protection against sophisticated cyber-security attacks when user credentials are stolen. Initial set up, creating rules, and fine-tuning are cumbersome and may take years. Every day, you receive several reports full of false positives. Most of the time, you don't have the resources to review this information and even if you could, you may still not have the answers, since **these tools are designed to protect the perimeter, primarily stopping attackers from gaining access.** Today's complex cyber-security attacks require a different approach.

Microsoft Advanced Threat Analytics (ATA) provides a simple and fast way to understand what is happening within your network by identifying suspicious user and device activity with built-in intelligence and providing clear and relevant threat information on a simple attack timeline.

Microsoft Advanced Threat Analytics leverages deep packet inspection technology, as well as information from additional data sources (Security Information and Event Management and Active Directory) to build an Organizational Security Graph and detect advanced attacks in near real time.

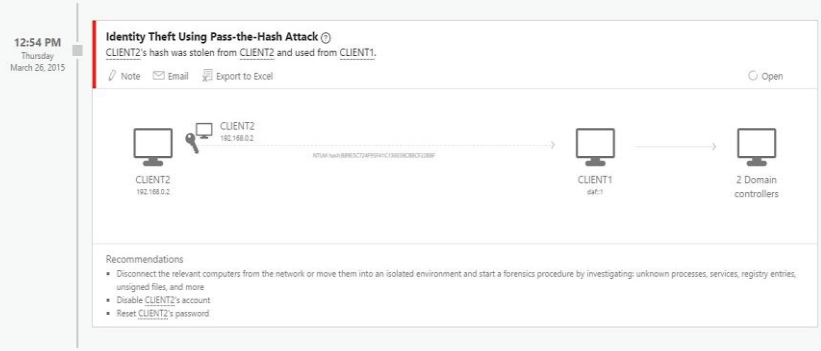
What is Microsoft Advanced Threat Analytics?

ATA is an on-premises platform to help you protect your enterprise from advanced targeted attacks by automatically analyzing, learning, and identifying normal and abnormal entity (user, devices, and resources) behavior.

Malicious attacks

ATA detects known malicious attacks almost as instantly as they occur.

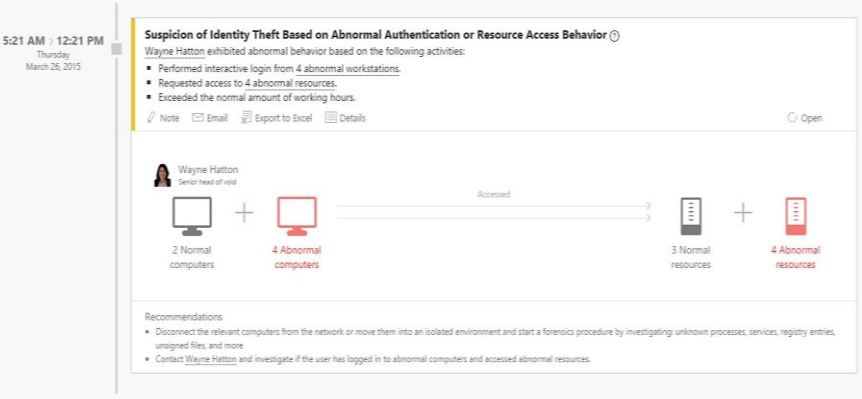
- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Malicious replications
- Reconnaissance
- Brute Force
- Remote execution
- Malicious DPAPI



Abnormal behavior

Behavioral analytics leverage Machine Learning to uncover questionable activities and abnormal behavior.

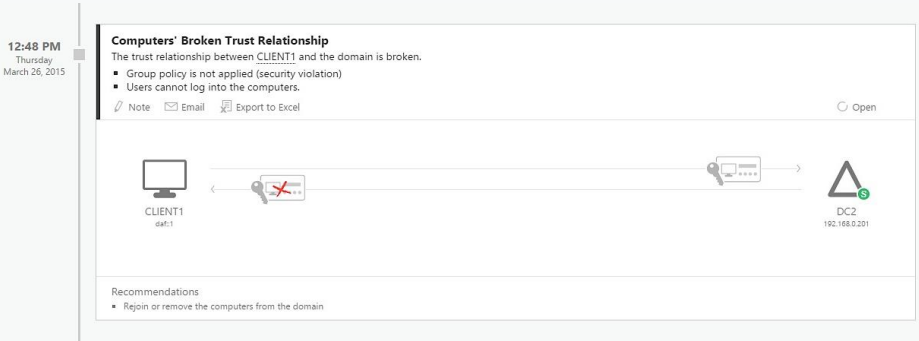
- Anomalous logins
- Unknown threats
- Password sharing
- Lateral movement



Security issues and risks

ATA identifies known security issues using world-class security researchers' work.

- Broken trust
- Weak protocols
- Known protocol vulnerabilities



Benefits

Detect suspicious activities and malicious attacks with behavioral analytics
Using its proprietary algorithm, Microsoft Advanced Threat Analytics works around the clock to help you pinpoint suspicious activities in your systems by profiling and knowing what to look for. No need for creating rules, fine-tuning, or monitoring a flood of security reports, since the intelligence needed is built in. ATA also identifies known advanced attacks and security issues.

Adapt to the changing nature of cyber-security threats
ATA continuously learns the behavior of organizational entities (users, devices, and resources) and adjusts itself to reflect the changes in your rapidly-evolving enterprise. As attacker tactics get more sophisticated, ATA helps you adapt to the changing nature of cyber-security threats with continuously-learning behavioral analytics.

Focus on what is important with a simple attack timeline
The constant reporting of traditional security tools and sifting through them to locate the important and relevant alerts can get overwhelming. The attack timeline is a clear, efficient, and convenient feed that surfaces the right things on a timeline, giving you the power of perspective on the who, what, when, and how. ATA also provides recommendations for investigation and remediation for each suspicious activity.

Reduce false positive fatigue
Traditional IT security tools are often not equipped to handle the rising amounts of data, turning up unnecessary red flags and distracting you from the real threats. With ATA, these alerts happen once suspicious activities are contextually aggregated to its own behavior, as well as to the other entities in its interaction path. The detection engine also automatically guides you through the process, asking you simple questions to adjust the detection process according to your input.

Key features

Behavioral analytics
ATA begins to understand entity behaviors while also automatically adjusting to known and approved changes in the enterprise. For instance, certain users have access to a specified set of servers, folders, and directories and the system learns their activity from the tools and resources they normally use.

Simple, actionable attack timeline
ATA's attack timeline makes your job easier and security measures better by listing questionable activities as they occur, accompanied with recommendations based on the specific activity alert.

Mobility support
No matter where your corporate resources reside—within the corporate perimeter, on mobile devices, or elsewhere—ATA witnesses authentication and authorization. This means that external assets like devices and vendors are as closely monitored as internal assets.

Organizational Security Graph
ATA builds an Organizational Security Graph, which is a map of entity interactions representing the context and activities of the users, devices, and resources.

SIEM Integration
ATA works seamlessly with SIEM after contextually aggregating information into the attack timeline. It can collect specific events that are forwarded to ATA from the SIEM. Also, you can configure ATA to send an event to your SIEM for each suspicious activity with a link to the specific event on the attack timeline.

Email Alerts
You can configure ATA to send an email to specific users or groups in your organization when it detects a suspicious activity. Each email will include a link to the specific attack in the ATA attack timeline, keeping the appropriate people up to date on the security issues in your organization, even when they do not monitor the attack timeline.

Easy deployment
ATA can be deployed either as an out of band solution by utilizing port mirroring without effecting the existing environment. ATA can also be deployed directly on the domain controllers without the added overhead of additional servers.
Once deployed ATA automatically starts analyzing and detecting suspicious activities.

For more information, please visit www.microsoft.com/ata

For trying and evaluating Microsoft Advanced Threat Analytics, please visit www.microsoft.com/en-us/evalcenter/evaluate-microsoft-advanced-threat-analytics