

University of Cordoba Secures Its Campus Data Center with Hillstone intelligent NGFW

## The Customer

The University of Córdoba is one of the top public colleges in Colombia. It offers a broad range of undergraduate programs underpinned by world-class research, including the field of basic sciences, associated agro-industrial production, engineering, social sciences, social, education and health. It has more than 12,000 students, supported by more than 550 academic staff.

## The **Challenge**

Like many educational institutions, the University of Córdoba balances academic freedom and flexible network access with security and resource consumption concerns. It is continually under attack from hackers, DDoS, and malwares. In the past, most malware has effectively tried to bring down the network just to make noise and provide distraction, but there has been a shift from 'disruptive malware' aimed at causing problems to networks to 'criminal malware' aimed at generating profit for criminals.

With traditional firewall protection, the IT team was unable to keep pace with security needs. "We have to protect the campus network of the university against various attacks, including advanced threats. In addition, we have to provide full protection for critical assets such as servers that support, for instance, education management system and databases," says the IT manager. "Another critical requirement was visibility and control of user traffic to ensure security as well as Quality of Service." Due to these issues, the IT team had to find a way to protect its research, personal, and financial data, as well as restrict and control access to data and networks.

## University of Cordoba Secures Its Campus Data Center with Hillstone intelligent NGFW

## The **Solution**

The Hillstone Networks T3860 Intelligent next-generation firewall (iNGFW) was deployed at the university's data centers perimeter. The solution delivers NGFW features, including IPS, AV, URL, QoS, as well as intelligent features, including ATD (Advanced Threat Detection) and ABD (Abnormal Behavior Detection).



Figure 1: Application-Based Visibility Interface

The university IT team was impressed by the breadth of application-based visibility (Figure 1) offered by the Hillstone solution, as well as the user-based dashboards that provided executive level as well as granular details for administrators. "We could instantly see what was traversing our network, what people are using, and where they're going on the Internet," says the IT manager. The Hillstone iNGFW provides visibility into every stage of an attack and detected security breaches within a matter of minutes or even seconds, so that the administrator could take proper action to prevent network casualty.

The IT team learned that the solution prioritizes hosts with the greatest security risks and provides

contextual information about the threat for maximum visibility. The security administrators were able to drill-down into the attacks, including packet captures, to analyze all threat details and resolve the issue to prevent it from recurring.

In addition to the traditional NGFW features, the Hillstone ATD engine analyzes close to a million "known" malware samples, and provides an accurate method for identifying unknown malware, helping administrators detect advanced threats, which cannot be detected by traditional signature based anti-virus. Figure 2, below, illustrates that 67 critical threats were detected by ATD within 24 hours.

A TABLE OF THE OF MILLION CONTRACT OF THE	lonkor Folicy Chipel Hud	work System							
Ap Field Q Trived Q Milphile			-	_					
			0	Float 67 High 45 Medium 34	Lew 31 Incoming Th	reat Map			
Criterie .									
Citta									
140				-			1. 10		
							<ul> <li>(4)3</li> </ul>		
Medum .									
Ltw -		an	•	• •					
		√ Scan	☆ AtteX □ 0x5	O Motiong O Spans O Ma	bare				13 -
Within: Last 24 Hours w Detected by: Advanced Thread D w	+ Fiter	♡ ścin	⊙ ATHA [] De5	⊖ Moting ⊖ Span ⊖ Ha	hare				
the second secon	+ Fiter		o Attack De5 c	Destination	Detected at	Count	Detected by	Status	
~							Detected by Advanced	Status	
me MAL/NARE User Agent (Farfux) - Possible Trojan Downloader	Type	Severity Certain	y Source	Destination	Detected at	12		Status	
ne MALTUAR: User-Agent (Fantos) - Possible Trigen Downloader MALTUAR: User-Agent (Fantos) - Possible Trigen Downloader	Type Scan - Web Applica .	Severity Certain	y Source	Destination	Detected at 2016/15/06 16:44.21	12	Advanced	Status Detected	Admin Ad
ne MIA/TURRE Uver-Agent (Fanlor) - Possible Trojen Downlader MIA/TURE Uver-Agent (Fanlor) - Possible Trojen Downlader MIA/TURE Uver-Agent (Fanlor) - Possible Trojen Downlader	Type Scan - Web Applica - Scan - Web Applica - Scan - Web Applica - Scan - Web Applica - Malware - Trojan	Severity Certain Monum 1009 Monum 1009 Monum 1009 Color 1075	y Source	Destination	Detected at 2016/15/08 18 44.21 2016/15/08 18 43.28	12	Advanced		Admin Ad
Construction     C	Type Scan - Vivb Applica . Scan - Vivb Applica . Scan - Vivb Applica . Scan - Vivb Applica . Melware - Tribon Milakare - Tribon	Severity Centae Minime 1009 Minime 1009 Minime 1009 Coloral 00%	y Source	Destination	Detected at 2016/0100 10.4421 2016/0100 10.44221 2016/0100 10.4428 2016/0100 10.4428 2016/0100 10.4152 2016/0100 10.10.20	7	Advanced Advanced Advanced		Admin Ad
Construction     C	Type Scan - Vivb Applica . Scan - Vivb Applica . Scan - Vivb Applica . Scan - Vivb Applica . Melware - Tribon Milakare - Tribon	Severity Certain Monum 1009 Monum 1009 Monum 1009 Color 1075	y Source	Destination	Detected at 2016/11/08 18.44.21 2016/11/08 18.43.28 2016/11/08 18.33.21 2016/11/08 15.41.52	10 7 1 3 2	Advanced Advanced Advanced Advanced		Admin Ad
Monte User Apert (Partics) - Possible Trajes Downlader     MOLONIAR User Apert (Partics) - Possible Trajes Downlader     MOLONIAR User Apert (Partics) - Possible Trajes Downlader     MOLONIAR User Apert (Partics) - Possible Trajes Downlader     montestation     montestation	Type Scan - Web Applica Scan - Web Applica Scan - Web Applica Mahare - Singin Mahare - Singin Mahare - Singin	Severity Centain Manuer 1009 Manuer 1009 Cellical 00% Cellical 00% Cellical 00% Cellical 00%	y Source		Defected at 2016/11/08 18:44:21 2016/11/08 18:43:28 2016/11/08 15:41:52 2016/11/08 15:41:52 2016/11/08 15:41:52 2016/11/08 15:41:52	12 7 1 3 2 1	Advanced Advanced Advanced Advanced Advanced	Detected	Admin Ad
Alexandrometry and a second seco	Type Scan. Web Applica. Scan. Web Applica. Scan. Web Applica. Moharer - Snipin Moharer - Snipin Moharer - Snipin Moharer - Snipin	Severity Centair Issues 1000 Centair 1000 Centair 1000 Centair 1000 Centair 1000 Law 27% Tagin 66% Centair 80%	9 Source 20 20 20 20 20 20 20 20 20 20 20 20 20	Destrutor	Detected at 2016/11/08 16.44.21 2016/11/08 16.43.28 2016/11/08 16.43.28 2016/11/08 15.43.22 2016/11/08 15.43.23 2016/11/08 15.43.29 2016/11/08 15.44.24	12 7 1 3 2 2 1 2 2 1 2 2 1	Advanced Advanced Advanced Advanced Advanced Advanced Advanced	Detected Detected Detected	Admin Ad Open
Alexandrometry and a second seco	Type Scan - Web Applica Scan - Web Applica Scan - Web Applica Mahare - Singin Mahare - Singin Mahare - Singin	Severity Contain Manuer 1009 Manuer 1009 Calkard 1009 Calkard 00% Unit 20% Dage 00% Dage 00%	9 Source.	Cristitution	Detected at 2016/11/08 16.45.21 2016/11/08 16.43.28 2016/11/08 16.33.28 2016/11/08 16.35.23 2016/11/08 15.41.52 2016/11/08 14.45.28 2016/11/08 14.43.26 2016/11/08 14.43.25	12 7 1 3 2 2 1 2 2 1 2 2 1	Advanced Advanced Advanced Advanced Advanced Advanced	Detected	Admin Ad Open
Compared Service (and Proceedings Pro	Type           Scan - Web Applica           Scan - Web Applica           Scan - Web Applica           Scan - Web Applica           Moharer - Trajin           Moharer - Trajin	Severity Centau Inner 1900 Inner 1900 Celluid 90% Celluid 90% Celluid 90% Celluid 90% Celluid 90% Celluid 90% State 90%	9 Searce.	Crestrutos	Detected at           2016/11/68 18:4421           2016/11/68 18:4322           2016/11/68 15:4152           2016/11/68 15:4152           2016/11/68 15:4152           2016/11/68 15:4152           2016/11/68 14:4251           2016/11/68 14:4251	12 7 1 3 2 2 1 1 2 2 1 1 2 1 1 1 2 1 1 1 2 1 2	Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced	Detected Detected Detected Detected Detected	Admin An Open Open Open Open Open Open
Comparing a second	Type Scan - Web Applica. Scan - Web Applica. Scan - Web Applica. Motores - Trage Motores - Trage Motores - Trage Scan - Veb Applica. Motores - Trage Scan - Veb Applica.	Severity Contain Severity Contain Selection 1999 Selection 1997 Collection 297% Collection 297% Collection 297% Selection 297%	5 Source.	Destination	Detected at           2016/01/00 16.44.21           2016/01/00 16.44.21           2016/01/00 15.43.22           2016/01/00 15.43.22           2016/01/00 15.43.22           2016/01/00 15.43.24           2016/01/00 15.43.25           2016/01/00 14.43.01           2016/01/00 14.43.25           2016/01/00 14.22.51           2016/01/00 14.23.25           2016/01/00 14.23.25	12 7 1 3 2 2 1 1 2 2 1 1 2 1 1 1 2 1 1 1 2 1 2	Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced	Detected Detected Detected Detected	Admin An Open Open Open Open
The control of the second seco	Type           Scan - Web Applica           Scan - Web Applica           Scan - Web Applica           Scan - Web Applica           Moharer - Trajin           Moharer - Trajin	Severity Centau Inner 1900 Inner 1900 Celluid 90% Celluid 90% Celluid 90% Celluid 90% Celluid 90% Celluid 90% State 90%	9 Searce.	Crestrutos	Detected at           2016/11/68 18:4421           2016/11/68 18:4322           2016/11/68 15:4152           2016/11/68 15:4152           2016/11/68 15:4152           2016/11/68 15:4152           2016/11/68 14:4251           2016/11/68 14:4251	12 7 1 3 2 2 1 2 1 2 1 1 1 1 1 1 1 1 1 1 1 1	Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced	Detected Detected Detected Detected Detected	Admin An Open Open Open Open Open Open
New Control Con	Type Scan - Web Applica. Scan - Web Applica. Scan - Web Applica. Motores - Trage Motores - Trage Motores - Trage Scan - Veb Applica. Motores - Trage Scan - Veb Applica.	Severity         Contast           Severity         Contast           Severity         Solow           Solow         Solow           Solow         Solow           Colland         Solow           Select         Solow           Solow         Solow	5 Source.	Destination	Detected at           2016/01/00 16.44.21           2016/01/00 16.44.21           2016/01/00 15.43.22           2016/01/00 15.43.22           2016/01/00 15.43.22           2016/01/00 15.43.24           2016/01/00 15.43.25           2016/01/00 14.43.01           2016/01/00 14.43.25           2016/01/00 14.22.51           2016/01/00 14.23.25           2016/01/00 14.23.25	12 7 1 3 2 1 1 2 1 1 1 1 1 1 1 1 1	Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced	Detected Detected Detected Detected Detected Detected	Open Open Open Open Open

Figure 2. Threats detected by ATD engine

Due to deploying Hillstone Networks T3860 Intelligent next-generation firewall (iNGFW), the University of Córdoba resolved issues related to network visibility, as well as security against advanced threats. "The comprehensive capabilities of the Hillstone solution enables us to secure and more fully support our academic mission," concluded the IT manager.



 Americas: +1-408-508-6750
 |
 APAC: +65-6678-7660

 Europe: +420-721-125-070
 |
 MEA: +971-4557-1493

 Request a Demo or Free Trial: inguiry@hillstonenet.com