cohesivenetworks

White Paper

Guarding Against Enterprise Attacks: Application Segmentation and Security

January 2015

Copyright Cohesive Networks

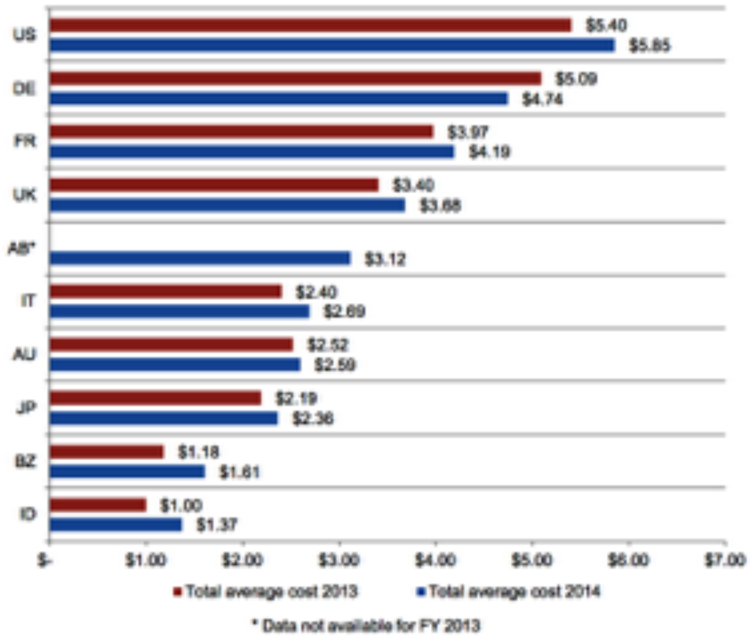
The major data breaches of 2014 should be clear warning signs for all network administrators and application owners: attackers have become professional.

Organizations now face potential exploitation by hackers, criminal gangs and foreign governments. 2014 saw more than 697 separate data breaches in the U.S., according to an October report from the Identity Theft Resource Center (ITRC). The organization estimates the 2014 attacks exposed over 81,443,910 personal records of customers, patients, partners and employees.

Data breaches across industries and verticals demonstrate that any company can be a potential target. Wall Street Journal reporter Jennifer Smith writes, “law firms, accounting firms and other contractors are increasingly common targets for cyberattackers looking to grab valuable information such as intellectual property or details on pending deals.”

Malevolent groups of hackers do not use particularly sophisticated means to access infrastructure. Hackers can compromise any corporate application “on a wire” within a network after they breach the perimeter. Once inside a corporate network attackers are able to move “east-west,” or laterally, between computers and servers within the organization to wreak havoc on an enterprise. The domino effect within a network allows hackers to easily access valuable data for an average of 229 days before IT teams detect a breach.

Figure 3. The average total organizational cost of data breach over two years
Measured in US$ ($000,000 omitted)



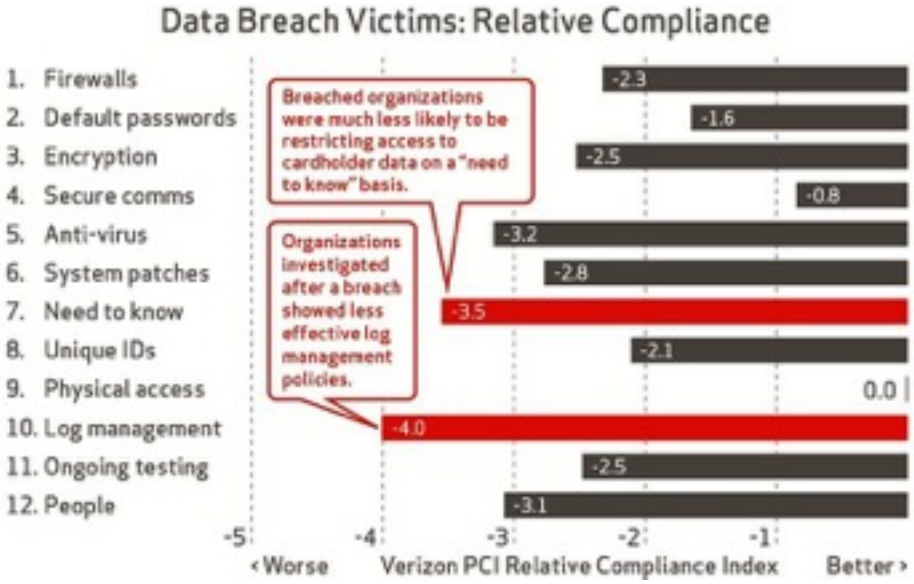
Source: Ponemon 2014 Cost of Data Breach Study

Enterprises must rethink security in 2015.

What 2014 has taught us about enterprise security

With serious attackers targeting a variety of industries, the cost to investigate, notify, and respond to a data breach can potentially destroy an organization. The global average cost of a data breach was $3.5 million in 2014, according to the 2014 Ponemon Institute report. The report estimates that enterprises have to pay an average of $145 per lost or stolen record, up from $136 in 2013 or a nine percent increase in just one year. All the while, enterprises face increasing regulatory implementation costs and reporting demands.

A staggering 43% of companies worldwide have reported being breached in the past year, according to the Ponemon Institute report. Hackers are out to profit from and disrupt corporations, and are causing increased regulatory and financial harm. Early estimates predict the Sony hack will cost over $100M to correct, not including lost revenues, falling stock prices, lost contracts with actors and directors, lawsuits, and personal losses. Another study from PwC estimates the worst cost of a security breach for small businesses cost between £65,000 and £115,000 on average; while large firms can reach up to £1.15m.



Source: Verizon 2014 PCI Compliance Report

One month before the Sony hack, in October 2014, the FBI released a warning that Chinese government hackers are running an ongoing campaign to steal valuable data from U.S. enterprises and government agencies. The group gains access to a targets' perimeter and then attacks "laterally" inside the system, according to a Washington Post article.

Causes: Traditional security approaches do not work for modern infrastructure
Historically, cybersecurity best practices involved rigid exterior defenses including firewalls, intrusion detection systems, and access control at the edge of the data centers. This approach is a continuation of the era of physical security, when data center servers were hardwired to a physical network and connections between partners ran over dedicated circuits. This perimeter defense mode used to adequately protected the enterprise.

Today's more complex and distributed networks can create a much more porous perimeter and expose potential weaknesses. Nearly 85 percent of insider attacks or "privilege misuse" attacks used the target enterprises' corporate local area network (LAN), according to a 2014 Verizon security report.

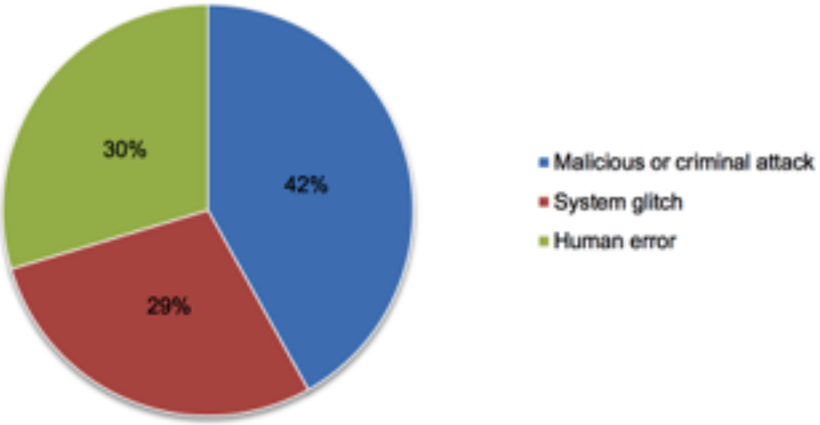
Causes: More traffic moving within data centers as well as to cloud
More than 7.7 zettabytes of annual cloud traffic will be outside owners' control by 2017, according to the 2013 Cisco Cloud Index.

To put the data center level security risks into perspective, Martin Casado, Senior Vice President of VMware's Networking and Security business unit, recently observed:

> …more and more traffic stays within the data center. We call this east-west traffic. So, in an average data center about 80% of the traffic never leaves. It turns out, Mr. Customer, that 80% of your security spend is on the north-south border, so you're spending 80% percent of your dollars on 20% of your traffic.

Causes: Compliance falls short
Roughly 25 percent of companies studied in a 2014 Verizon PCI compliance report still use factory defaults in point of sale devices and hardware. Details emerged after the 2013 Target hack that their FireEye network security and Symantec antivirus systems both detected the breach, yet features to automatically destroy malware were disabled.

Figure 5. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=314)



Source: Ponemon 2014 Cost of Data Breach Study

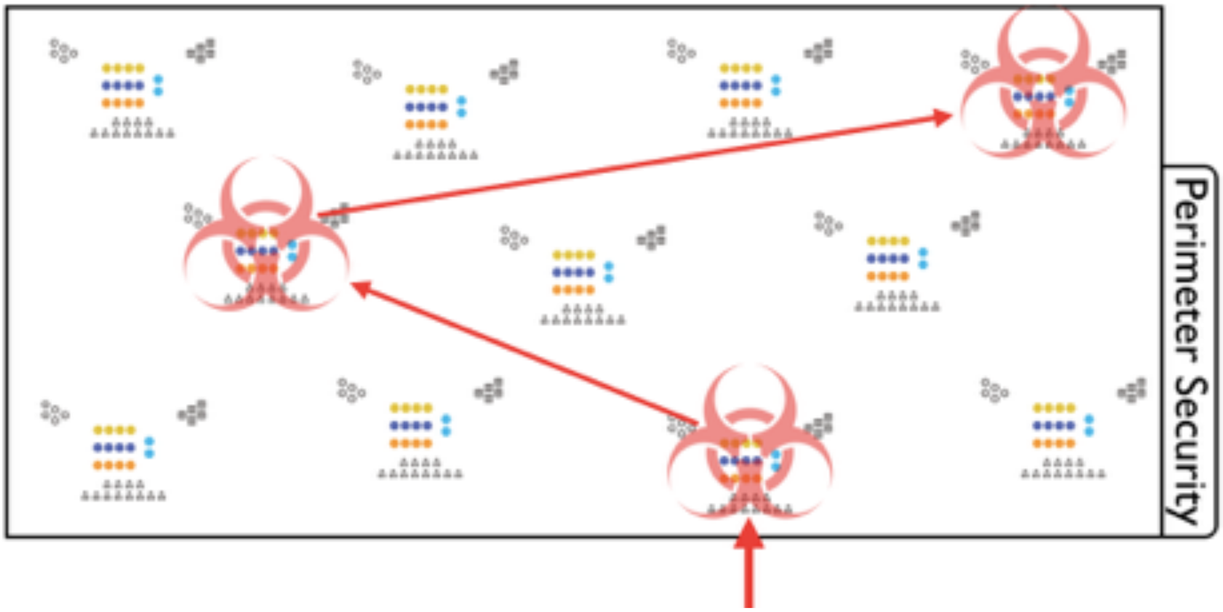
The Mandiant 2014 Threat Report notes that the average time it takes for an enterprise to detect breaches is 229 days; unfortunately this is 4 percent slower than reported in 2012. As an example, in the December 2013 Target breach, the security team reportedly did not react until federal investigators warned the organization a full two weeks after the initial breach. Clearly, security solutions are failing IT teams by either by not detecting malicious attacks inside the network or creating too many false positives.

Current solutions: Weak enterprise security with just core hardware and virtual layer
There are three possible layers where enterprises can use network security today: the core network hardware, the virtualization layer, or on each application's virtual local area network or VLAN.

In data center core hardware, refrigerator-sized boxes provide some application security functions, but the focus has been on keeping these boxes physically isolated. The standard data center perimeter or “demilitarized zone” (DMZ) model focuses most of the security efforts on protecting the outside, with little to no security features inside.

In the virtualization layer, multi-tenant hypervisor rules can provide some logical isolation, so that secure applications do not share the same virtual resources. The “logical segmentation” allows network and application administrators to keep applications isolated even if they might share the same multi-tenant infrastructure. Keeping applications isolated in layers 2 and 3 does save cost and operational complexity, but force security protections on the entire network rather than individual applications.

The perimeter-based security approaches still have not evolved to meet the modern application-focused enterprise. Hardware and virtualization layer defenses allow application teams far too much access to core mission critical controls and force teams to write overly permissive controls to accommodate overlapping use cases. Because of the large overlaps, the conflicts between different application security rules trigger too many false positives, similar to the Target breach scenario. The weaknesses of the perimeter-based approach are apparent in the east/ west attacks on Sony, Target and in the September 2014 attack on Home Depot.



Application and network teams are not to blame, though. The application sprawl across an enterprise can be very difficult to manage and secure. Enterprises cannot assume network and virtualization administrators will become experts in every application and security rule.

Security Improvements: Compliance for the modern world
2014 also saw some hope for enterprises looking for cures for the common data breach: more government agencies and compliance groups are updating security standards to match modern cybercrime.

The National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce, has created some of the most comprehensive security documentation. The first NIST Framework for Improving Critical Infrastructure Cybersecurity, published in February 2014, created voluntary standards for organizations to better identify, protect, detect, respond and recover from data breaches. The Framework offers both guidelines and measures for all organizations to manage access control and data security, and explicitly data at rest and data in motion.

In the European Union, the European Banking Authority (EBA) recently created a new set of minimum security requirements for payment services providers in the EU. The standards will create a framework for managing risks and increase requirements for incident reporting and consumer authentication. The standards are likely to adopted by August 1, 2015.

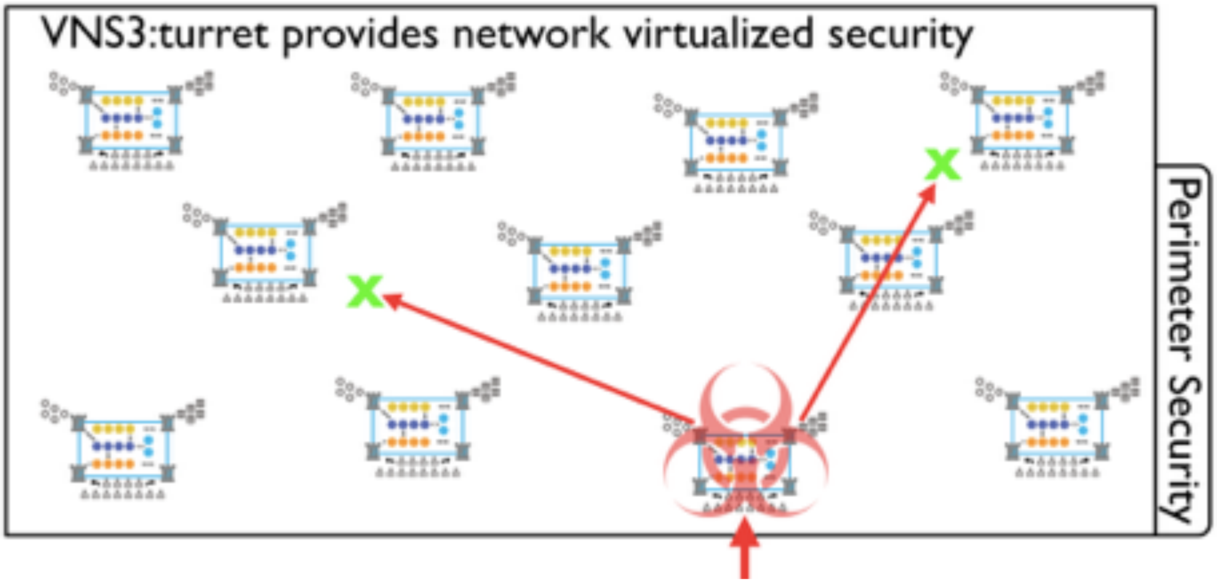
Another regulatory shift in 2015 is the Payment Card Industry (PCI) Data Security Standard 3.0. PCI regulations apply to any enterprise that stores, processes or transmits payment card information. The updated standards went into effect on 1 January 2015 and include requirements aimed at third party providers and stress security as a shared responsibility.

Application Security Control: Layers of protection
To guard and quarantine an application, enterprises can force all servers and applications to go through secure switches at every layer within a data center network, all but eliminating malicious east/west movement. In order to gain control over all incoming and outgoing traffic for each application, enterprises can use “micro-perimeters” to break the secure network into smaller, tightly controlled overlay networks.

Application security controllers can add security within the network layers to strengthen existing core networking hardware and virtualization layer security. Installing full function network security appliances for each application can improve network security without changing existing network or security infrastructure.

Just like the physical segmentation at the core hardware layer and logical segmentation at the virtualization layer, application layer security provides “application segmentation.” With application segmentation, enterprises can dictate what traffic travels to each application server.

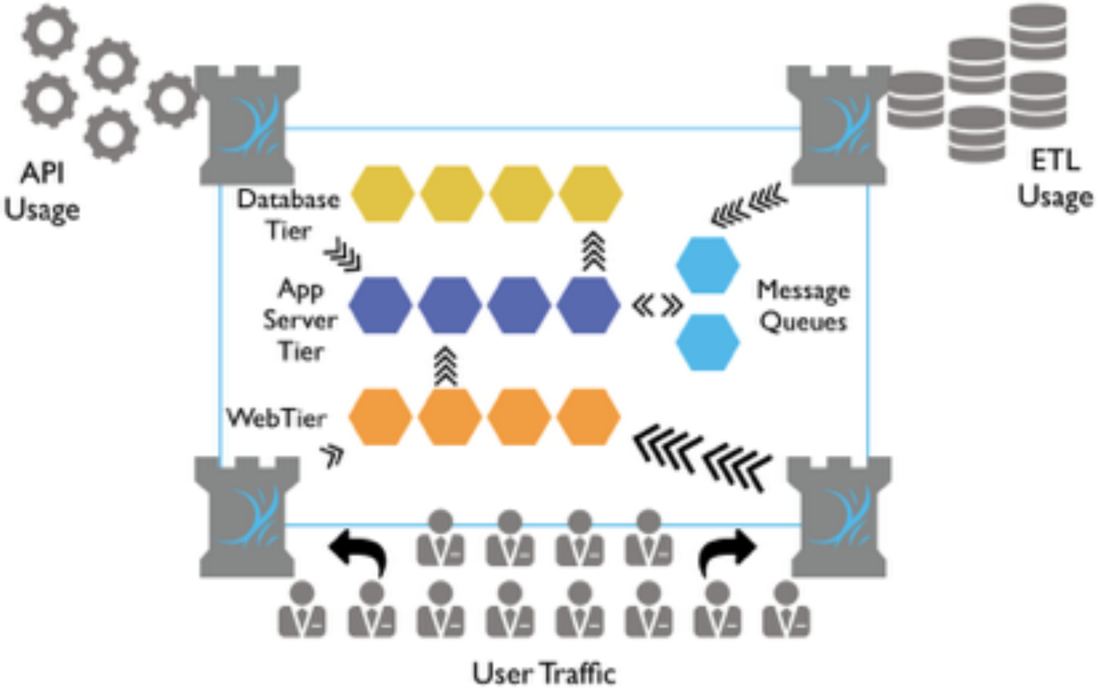
For example, an enterprise can determine that an application's web server can only initiate traffic out to an application server through an encrypted switch. The application server cannot initiate traffic into the web server layer, and the database layer cannot initiate traffic to the application server or web server layers. In this example, the message queue layer cannot talk to the web server layer.



Because all data must pass through an encrypted switch, enterprises can mediate security and segmentation. User traffic then gets isolated to flow through the application's secure edge. Even with only basic interior firewall rules, this enterprise can protect themselves from an east/west exploit.

VNS3:turret - Application segmentation creates secure micro-perimeters
VNS3:turret is an application security controller. You can deploy as encrypted, clustered virtual appliances, creating a micro-perimeter around your mission critical applications. The micro-perimeter works as a secure, redundant network combined with dataflow and compliance tools. This "application segmentation" provides the most comprehensive application security model available today.

VNS3:turret is deployed as clustered software-only virtual appliances that create a micro-perimeter to secure your mission critical business systems in any network. The application segmentation allows each application's developer team to take a proactive role in cybersecurity in any public, private, hybrid or virtualized environment.



Availability
VNS3:turret is available on all Public Clouds, including: Amazon Web Services EC2, Amazon Web Services VPC, Google Compute Engine (GCE), HP Helion, IBM SoftLayer, Terremark vCloud Express, ElasticHosts, CloudSigma, Flexiant, Rackspace, InterRoute, Abiquo, BigStep, and Century Link.

VNS3:turret is available on major private cloud environments, including: Openstack, Flexiant, Eucalyptus, and Abiquo, as well as most virtual infrastructures including VMware, Citrix, Xen, and KVM. Licensing for VNS3:turret is on an annual subscription basis and only requires a 12 month commitment. The annual license fee is for up to ten critical applications.

Get in touch with the Cohesive Networks team to see how VNS3:turret can secure your private cloud environments:

- Email us: **sales@cohesive.net**
- US toll free: +1 (888) 444-3962
- UK phone: +44 208 144 0156

Learn more about VNS3:turret and the VNS3 Product Family:

- Blog: **cohesive.net/blog**
- Twitter: **twitter.com/cohesivenet**

Security Framework References:

NIST Framework: http://goo.gl/PWhctF
Payment Card Industry (PCI) Data Security Standard version 3.0: http://goo.gl/0M1fgY
European Central Bank Recommendations for the Security of Internet Payments: http://goo.gl/8M8C6D

Referenced Studies and Articles:

"Why the JPMorgan Hack Is Scary." Bloomberg View, 6 October 2014; http://www.bloombergview.com/articles/2014-10-06/why-the-jpmorgan-hack-is-scary
"Data Breach Reports." ITRC Data Breach Report, 23 December 2014. http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf
Smith, Jennifer. "Banks Ramp Up Cybersecurity Requirements For Outside Lawyers." The Wall Street Journal Law Blog, 27 October 2014. http://blogs.wsj.com/law/2014/10/27/banks-ramp-up-cybersecurity-requirements-for-outside-lawyers/
"Survey: 80 Percent of IT Security Professionals Say They Can Detect a Data Breach on Critical Systems Within a Week." Tripwire, 11 August 2014. http://www.tripwire.com/company/news/press-release/survey-80-percent-of-it-security-professionals-say-they-can-detect-a-data-breach-on-critical-systems-within-a-week/
"Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis." Ponemon, 5 May 2014. http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
Richwine, Lisa. "Cyber attack could cost Sony studio as much as $100 million." Reuters, 9 December 2014. http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209
Miller, Andrew; Home, Richard; and Potter, Richard. "2014 Information Security Breaches Survey." PwC and U.K. Department for Business, Innovation and Skills (BIS), 2014. http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf
Nakashima,Ellen and Soltani, Ashkan. Washington Post, 15 October 2014. http://www.washingtonpost.com/world/national-security/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b-f6333e2c0453_story.html
"2014 Data Breach Investigation Report." Verizon Enterprise, 2014. http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf
Vaughan-Nichols, Steven J. "Cisco projects data center-cloud traffic to triple by 2017." ZDnet, 15 October, 2013. http://www.zdnet.com/article/cisco-projects-data-center-cloud-traffic-to-triple-by-2017/
"Verizon 2014 PCI Compliance Report." Verizon Enterprise, 2014. http://www.verizonenterprise.com/resources/reports/rp_pci-report-2014-executive-summary_en_xg.pdf
Dix, John. "VMware's Casado talks about evolving SDN use cases, including a prominent role for security." Network World, 6 October, 2014. http://www.networkworld.com/article/2691482/sdn/vmwares-casado-talks-about-evolving-sdn-use-cases-including-a-prominent-role-for-security.html?nsdr=true
Leyde, John. "Target IGNORED hacker alarms as crooks took 40m credit cards – claim." The Register, 14 Mar 2014. http://www.theregister.co.uk/2014/03/14/target_failed_to_act_on_security_alerts/
Baert, Christoph. "New Security Measures for Payments in the European Union." Mastercard Security Matters, 2014. http://arm.mastercard.com/securitymatters/2014-issue/new-security-measures-payments-european-union/

About the Authors

Patrick Kerpan, CEO

Mr. Kerpan is responsible for directing product, technology and sales strategy. Mr. Kerpan brings more than 20 years of software experience to the role of CEO and was one of Cohesive's founders in 2006. Previously he was the CTO of Borland Software Corp which he joined in 2000 through the acquisition of Bedouin, Inc., a company that he founded. Mr. Kerpan was also the vice president and general manager of the Developer Services Platform group at Borland, where he was instrumental in leading the Borland acquisition of StarBase in 2003. Before founding Bedouin, Inc., Mr. Kerpan was a managing director responsible for derivatives technology at multiple global investment banks.

Ryan Koop, Director of Products and Marketing

Mr. Koop is responsible for product development and manages teams for public relations, international events, and content marketing. His role spans the technical product development, customer support, business development and thought leadership needs of a growing company. Previously, he worked at a trading platform software company in the US Derivative Markets.

Copyright Cohesive Networks