security white paper IDG

THE ANSWER TO NEXT-GENERATION SECURITY THREATS

Fresh research shows that enterprises are using old tools to combat new security dangers that only a more advanced breed of security solution can successfully address

THE MORE THINGS CHANGE, the more they stay the same. In IT security as in so many other aspects of life, it's truer than ever these days. The security landscape may have changed significantly in recent years, but the technologies people use to protect themselves all too often haven't.

And make no mistake, the security landscape has grown more perilous. Hackers today are exploiting new threat vectors to launch increasingly sophisticated attacks in steadily climbing numbers. According to security researcher Ponemon Institute LLC, the average enterprise's chances of experiencing a data breach involving 10,000 or more records over a 24-month period currently stands at approximately 22 percent.

Yet as an exclusive new study from IDG Research Services reveals, most companies are fruitlessly attempting to address complex and proliferating new security risks with old and increasingly overmatched countermeasures—ranging from network firewalls and anti-virus software to simply throwing more people at the problem by adding employees or hiring consultants. Worse yet, the new survey shows that IT executives at those companies know those strategies are ineffective, but continue using them anyway.

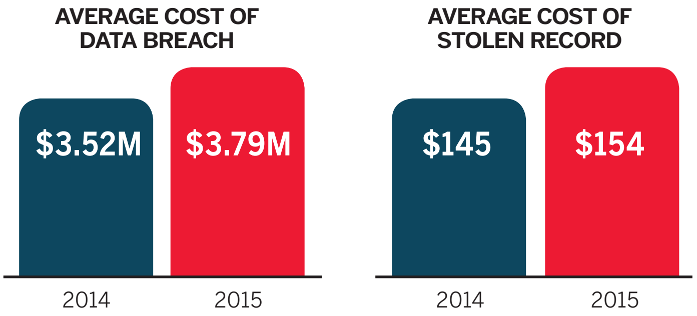
There is a better way forward, however. Faced with an expanding array of next-generation security threats, leading-edge vendors are introducing next-generation security offerings that use cryptographic identifiers, network micro-segmentation, and other powerful and innovative technologies to enforce a "zero trust" IP communications model with radical implications for safeguarding the enterprise. When equipped with state-of-the-art orchestration software, this new breed of security solution empowers businesses not only to defend themselves more effectively from ever-evolving risks, but to do it in a way that requires dramatically less time and effort as well.

EXPANDING ATTACK SURFACE

The need for such solutions has never been greater, because security breaches are not only more numerous than before but more expensive too. Indeed, the average cost of a data breach rose in 2015 from $3.52 million to $3.79 million, according to Ponemon Institute data. The firm also found that the average cost for each lost or stolen record containing sensitive information increased from $145 to $154.

THE RISING COST OF LAX SECURITY

Source: *Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC



A wide range of relatively new security hazards is making that kind of financial liability all too common. The rise of smartphones, tablets, and cloud computing, for example, has rendered the whole notion of the defined, firewall-protected network perimeter all but obsolete.

"In the past, architectures were very easy to control because they were geo-

TEMPERED NETWORKS

graphically bound in most cases," says Marc Kaplan, vice president of security architecture at next-generation security vendor Tempered Networks. Today, however, employees, business partners, and customers are accessing network resources from an endless variety of devices and locations, often over shared public connections. The emerging "Internet of Things" and machine-to-machine communications is only making matters worse by introducing massive amounts of Web-enabled devices and equipment. That includes things like windfarms, tractors, oil drills, freight trucks, etc., that often do not have native security built in, or that run older and "unpatchable" operating systems. Companies are frequently connecting to these devices over cellular communications, without using encryption.

"We've got an expanding attack surface area in the form of a lot more IP-enabled devices," observes security expert Doug Cahill, of analyst firm Enterprise Strategy Group.

Behind the firewall, meanwhile, data centers are rapidly implementing flatter network architectures. Designed to handle increasing volumes of "east-west" traffic between workloads and distributed architecture components more efficiently, those new topologies are also creating convenient new avenues for malware to spread through enterprise infrastructures. "In a flat network that's easily permeable by someone with the right permissions, once an exploit gets inside it can spread like wildfire," Kaplan says.

Unfortunately, he adds, most businesses are combatting these new risks with outdated security tools. "The attacks have grown more complicated and the network has grown more dynamic, but the security solutions have essentially stayed the same. Addressing the crux of the issue requires more than adding new product features to existing products," Kaplan notes. What's more, those systems usually come from multiple vendors so they rarely integrate smoothly. Worse yet, many of them rely on IP address-based trust mechanisms that are vulnerable to "spoofing" attacks.

Managing them all, furthermore, is a complex, labor-intensive nightmare requiring manual updates every time technicians perform moves, adds, and changes in the data center. "It's really hard to keep firewall rules current," observes Adrian Sanabria, a senior security analyst at 451 Research Inc.

This is especially true for IT departments that have more to do than ever these days yet less time, money, and people to do it with, Kaplan adds. Skilled security specialists cost more than many businesses can afford, and overworked network generalists simply can't spare the time required to keep close tabs on firewall rules and security events.

"The people who typically manage security these days have day jobs," Kaplan observes. "They can't go through millions of lines of logs every day to see if there's some problem hidden in the noise created by every policy change someone made."

SERIOUS CHALLENGES

Data from the new IDG study reveals just how badly businesses are struggling to cope with today's demanding security pressures. For example, 62 percent of poll respondents called misconfiguration of security policies and other forms of human error extremely or very challenging, while 55 to 57 percent said the same of bolted-on traditional security safeguards, increased dependence on security personnel with advanced skills, and having too many manual processes versus too little automation.

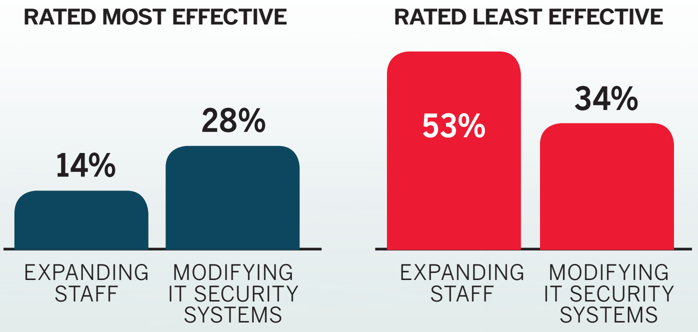
What's more, 60 percent of survey participants called IT security complexity extremely or very challenging, an equal 60 percent blamed security complexity for impeding their agility to at least some extent, and another 14 percent said complexity is hindering their agility to a great extent. "Networks are so hard to set up and manage and lock down," Sanabria says. "You just get stuck in constantly making changes."

IDG's data also confirms that many companies are responding to new security challenges in old-fashioned ways. When asked what techniques they use to keep up with security configuration changes and updates, for example, 69 percent of poll respondents cited traditional IT security solutions, 50 percent named hiring IT security consultants, and 38 percent named hiring or assigning additional technical staff.

Surveyed IT leaders are under no illusions about the effectiveness of those measures either. Fully 53 percent of them called hiring or assigning more IT staff one of the least effective approaches to keeping up with configuration requirements, and 34 percent said the same of modifying traditional IT security systems. By contrast, just 14 percent and 28 percent of survey participants, respectively, called hiring additional staff and modifying traditional tools one of the most effective techniques.

SECURITY COUNTERMEASURES:
UPGRADE STAFF OR TECHNOLOGY?

Source: *Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC



STAYING SAFE BY GETTING HIP

Though less widely known and used, certain next-generation security solutions are more powerful and actually more cost-effective than the techniques most companies are utilizing to keep critical IT assets safe at present.

The key to their power is a little-known but immensely important technology called the Host Identity Protocol, or HIP. Successfully deployed for over 10 years in some of the world's most demanding and frequently targeted IT environments, and recently declared a global standard by the Internet Engineering Task Force, HIP provides an advanced encryption method using unique cryptographic identities and a trust model based on whitelisting, rather than "spoofable" IP addresses to identify endpoints. This results in a far more reliable basis for trust.

"It's sort of like deciding whether or not a stranger is who they claim to be by examining a sample of their DNA rather than asking them their name," Kaplan says.

"IT'S SORT OF LIKE DECIDING WHETHER A STRANGER IS WHO THEY CLAIM TO BE BY EXAMINING A SAMPLE OF THEIR DNA."

MARC KAPLAN VP SECURITY ARCHITECTURE, TEMPERED NETWORKS

Next-generation security solutions hide network resources behind HIP-based appliances (which can be physical or virtual) that exchange traffic only with an approved whitelist of other HIP-enabled appliances bearing known and verified identity keys. For ultimate security, these appliances communicate only with other HIP-based appliances bearing a unique embedded certificate to create an end-to-end encrypted communication channel. "The certificate is like a fingerprint, so in addition to checking a host's DNA you're checking its fingerprints too," Kaplan adds.

That arrangement offers significant advantages over older security methodologies. First, it prevents attackers from viewing a company's servers, and therefore from targeting them as well. "If someone compromises your core routing infrastructure all they're going to see is encrypted traffic between HIP-based appliances," Kaplan observes. "They won't know if there's two or 2,000 devices behind those appliances." They won't be able to read any of that HIP traffic either, because next-generation security solutions use AES-256 encryption and SHA-2 message authentication to render network communications indecipherable to outsiders.

Meanwhile, HIP-based appliances redefine IT agility and deliver unprecedented ease and control by enabling IT staff to reallocate network resources as often as they want without changing trust relationships. That's so long as a HIP-enabled appliance makes the move along with them. "Your DNA stays with you wherever you go and so do your fingerprints. The same is true with HIP-enabled appliances," Kaplan says.

HIP-based appliances offer protection from denial-of-service (DoS) attacks as well. Such assaults slow back-end infrastructures to a crawl by bombarding them with transactions that require little capacity to generate but lots of capacity to process. The HIP protocol levels the playing field by requiring host devices to solve a resource-intensive cryptographic puzzle before submitting traffic.

"An attacker has to put a strain on their own servers before they can put a strain on yours," Kaplan says, making the infrastructure requirements associated with a successful DoS strike unacceptably expensive. HIP-enabled appliances add further resilience on top of that by hiding network resources from a DoS host's view. "If you can't see it, you can't target it," Kaplan notes.

HOW TEMPERED NETWORKS CAN HELP

NEXT-GENERATION SECURITY TECHNOLOGIES are the answer to next-generation security challenges, and Tempered Networks is uniquely qualified to help organizations harness the power of such technologies.

The core elements of the Tempered Networks solution are the HIP-enabled security appliances and their centralized orchestration engine. Drawing on a cutting-edge implementation of the Host Identity Protocol, HIP-based appliances hide, or cloak, critical network resources from would-be attackers by ensuring that only devices on a trusted whitelist can view, query, or detect them. The highest level of encryption available secures all traffic between Tempered Networks appliances.

Tempered Networks' hardened security appliances are available in a variety of both physical and virtual form factors suitable for any environment, including branch offices, kiosks, drilling rigs, production facilities, and other remote sites that communicate over public or private shared networks. The company's industry-leading orchestration engine makes configuring and administering any number of HIP-based appliances a snap. And that means companies can create micro-segmented, identity-based overlay networks in minutes.

"It's incredibly easy to establish trust relationships among devices, because the system abstracts all the minutiae out of that process," explains Marc Kaplan, Tempered Networks' vice president of security architecture.

The orchestration engine also automates ongoing administration and maintenance, enabling network and security managers to focus their time on more strategic projects and initiatives instead. Through its intuitive management interface, IT staff have centralized, single-pane-of-glass control over the entire solution and can easily and rapidly provision secure overlay networks to departmental users. "It's truly a very easy product to use," Kaplan says.

Managing remote access rights is easy with the Tempered Networks solution as well. Administrators can give employees, contractors, and vendors access privileges to individual devices or groups of them in minutes, and revoke them just as swiftly.

Best of all, the Tempered Networks solution preserves and in some cases improves the value of legacy network and security investments; it fully integrates with VLANs, VPNs, firewalls, and other existing IT assets.

To learn more about the Tempered Networks solution and experience its elegant approach with yourself own eyes, check out this video demo. Then contact Tempered Networks to set your company's journey to the next generation of enterprise security in motion.

TEMPERED NETWORKS®

“THE REALITY IS YOU’RE GOING TO BE BREACHED EVENTUALLY. WHEN IT HAPPENS, YOU WANT TO MITIGATE THE DAMAGE. **THE ONLY WAY TO DO THAT IS TO SEGMENT YOUR NETWORK PROPERLY.”**

MARC KAPLAN VP SECURITY ARCHITECTURE, TEMPERED NETWORKS

SEGMENTATION ON STEROIDS

HIP-based appliances play a key role in an important feature of next-generation security solutions: identity-based overlay networks. Software-defined subsets of a larger physical infrastructure, overlays are basically networks-within-a-network separated from one another by impenetrable virtual borders. HIP-enabled appliances use whitelists to determine which devices belong to which overlay network based on their IP and MAC address, and then direct traffic accordingly. Packets admitted to one overlay network can neither see nor access any of the others.

According to Kaplan, overlay networks help companies significantly limit the after-effects of the successful security attacks they’re sure to suffer sooner or later. “The reality is you’re going to be breached eventually,” Kaplan says. “When it happens, you want to mitigate the damage, and the only way to do that is to segment your network properly.”

The best next-generation security solutions take network segmentation even further using “micro-segmentation.” Sort of an overlay network on steroids, micro-segmentation gives especially high-value or vulnerable endpoints an additional layer of protective isolation. “Think of it almost like an Ethernet cable between two devices,” Kaplan says. “No one else on or off the network can see the traffic between those hosts.”

REMOVING PAIN BY HIDING COMPLEXITY

Encouragingly, given benefits like that, the new IDG Research Services study shows that businesses have begun supplementing their outdated security defenses with next-generation solutions. In fact, when asked what techniques they use to keep up with security configuration changes and updates, 53 percent of survey participants named next-generation IT security technologies. In addition, 30 percent of respondents said they’re using micro-segmentation now and another 22 percent plan to do so in the future. Of those companies, moreover, 77 percent agreed that micro-segmentation helps isolate business-critical endpoints and 51 percent said it helps reduce available attack surfaces.

Still, the IDG data also indicates that companies face multiple barriers on the road to adopting micro-segmentation. When organizations neither using nor planning to use micro-segmentation were asked to explain that decision, 47 percent cited both the complexity of mapping existing security controls to different segments and increased security management difficulty. Another 35 percent named high deployment complexity.

Those figures have a familiar ring to many veterans of the network security scene. The basic principles behind segmentation, whitelisting, and many of the other techniques used in next-generation security solutions are nothing new, they say. Until now, though, implementing them was a time-consuming, manual process that quickly overwhelmed even the best-run IT departments. “The concept of ‘least privilege’ has been around forever,” Sanabria notes. “The traditional methods have just been way too difficult to manage.”

TAKING PAIN OUT OF NETWORK SECURITY

That’s why a next-generation security solution’s most critical feature may well be orchestration software. Businesses will never be able to tap into the power of technologies like micro-segmentation if they must configure and maintain them by hand. Kaplan therefore advises IT leaders to look for products that automate not just micro-segmentation, but device discovery, trust relationships, overlay network management, and other complex yet essential tasks.

“Best-in-class solutions enable you to build and maintain incredibly large, complicated networks in a few clicks without having to manage passwords, trust models, or routing and switching rules,” he says. “What was really painful to do previously suddenly becomes simple.”

Ultimately, next-generation security solutions—or those worth adopting, at any rate—are all about taking the pain out of protecting the enterprise by hiding the complexity of that task. The tools businesses need to hold today’s constantly shifting and multiplying threats at bay are available now. All IT leaders need do is make the choice to start using them.