TANIUM

ARTIGO TÉCNICO

Confrontando a maior superfície de ataque já vista com o gerenciamento convergente de endpoints (XEM)

Resumo executivo

Os ataques de ransomware são uma das ameaças cibernéticas de mais rápido crescimento na história recente. O número de ataques aumentou mais de 140% no terceiro trimestre de 2021, apesar de as organizações gastarem mais de US$ 160 bilhões em segurança cibernética no ano passado.

Você já se perguntou por que esse problema de alta prioridade está recebendo mais dinheiro e atenção do que nunca, e ainda assim o problema está piorando?

Isso porque a abordagem do setor à segurança é falha.

Cada provedor de segurança e gerenciamento de TI oferece apenas uma pequena parte da solução necessária para proteger nossos ambientes. E para exacerbar ainda mais a situação, essas diversas ferramentas são frequentemente implantadas em silos nas organizações.

Os diretores de TI e de segurança de informação são forçados a comprar várias soluções, juntá-las e tomar decisões com base em dados obsoletos, imprecisos e incompletos.

Para piorar as coisas, essas ferramentas não têm visibilidade em tempo real. Na verdade, em 94% das empresas, as ferramentas podem não estar vendo até 20% dos endpoints que exigem proteção. As soluções pontuais criam lacunas que os hackers podem explorar e apenas aumentam a complexidade de uma área de superfície de ataque em constante crescimento.

Pare por um minuto. Quando foi a última vez em que você se perguntou?

- Quantos endpoints temos?
- Quais aplicativos são executados neles?
- Quais usuários têm acesso administrativo desnecessário?

Para responder a essas perguntas, você teve que explorar várias soluções pontuais, depois centralizar, normalizar e analisar os dados de cada solução?

É hora de terminar este ciclo por meio de uma abordagem totalmente diferente: implantar uma plataforma de gerenciamento de endpoints convergente.

Uma única plataforma que fornece visibilidade e remediação.

Uma única plataforma que fornece dados em tempo real e tem impacto em tempo real.

Essa plataforma gerencia e protege todos os tipos de endpoint, de laptops a contêineres na nuvem, sensores e internet das coisas (IoT), permitindo que as equipes trabalhem juntas, reunindo dados de operações de TI, segurança e gestão de risco e conformidade. Ao adotar essa abordagem de plataforma em vez de montar diversas soluções pontuais, você poderá ver que é possível interagir com cada endpoint em segundos, independentemente da escala e complexidade da rede.

As organizações agora têm uma plataforma de gerenciamento convergente de endpoints em que podem confiar e continuar a expandir e ampliar. É possível eliminar rápida e sistematicamente a enorme quantidade de soluções pontuais legadas acumulada e substituí-las por uma única plataforma.

A evolução da tecnologia e da sociedade

Estamos em um momento dinâmico, em que vemos mudanças na tecnologia e na sociedade como um todo que afetam a forma como trabalhamos e vivemos. Todas as organizações estão lidando com essas três grandes mudanças:

Transformação digital

A transformação digital está mudando a forma como as empresas operam e agregam valor em todos os setores que atendem. O que costumava ser controlado centralmente por perímetros cercados evoluiu para uma ampla rede de serviços de software, infraestruturas de nuvem e serviços de aplicativos descentralizados.

As empresas agora gastam US$ 700 bilhões anualmente em projetos de transformação digital, de acordo com a empresa de pesquisa Futurum. A pesquisa também mostra que é comum uma empresa ter mais de 200 aplicativos usados ativamente, e 60% desses aplicativos são entregues a cada dois anos. Esse ritmo de transformação digital está apresentando um grande desafio para a segurança cibernética.

Trabalho em qualquer lugar

O aumento do trabalho remoto causado pela pandemia criou um perímetro dinâmico em constante mudança.

Antes da pandemia, a maioria das organizações adotava a abordagem de segurança cibernética chamada "castelo e fosso". Os firewalls corporativos protegeram redes empresariais, garantindo a segurança de dispositivos, sistemas e dados locais.

Essa abordagem não funciona tão bem como antes. Muitos recursos de TI agora operam fora do fosso, ou firewall, e são vulneráveis a ameaças cibernéticas de todos os tipos.

Se as organizações não têm a capacidade de gerenciar a segurança nesses dispositivos, independentemente de onde estejam, elas estão se abrindo para uma grande superfície de ataque e enorme risco.

Explosão de endpoints

Por fim, a combinação de transformação digital e trabalho em qualquer lugar está impulsionando uma explosão em dispositivos de endpoint, expandindo a borda com dispositivos móveis, IoT, contêineres de nuvem e sensores, todos os quais são possíveis entradas para invasores.

Enquanto isso, ataques cada vez mais sofisticados, como phishing, comprometimento de e-mail comercial, ransomware e outros, criam um desafio de gerenciamento de endpoint muito mais difícil do que nunca.

Respondendo a essa pressão, as equipes de TI continuam a adquirir cada vez mais ferramentas, e essas aquisições são muitas vezes isoladas por equipe. O estudo de lacunas de visibilidade da Tanium em 2020 revelou que uma empresa média usa aproximadamente 43 operações de TI e ferramentas de segurança, embora isso varie amplamente conforme o tamanho da empresa.

Mas, apesar de mais ferramentas e orçamentos de segurança crescentes, a lacuna de vulnerabilidade não está melhorando. Na verdade, está piorando. As organizações estão gastando bilhões em segurança cibernética. Enquanto isso, 20% dos endpoints estão ficando indetectáveis e desprotegidos, e a cada 11 segundos ainda ocorre um ataque de ransomware.

Hoje, é mais difícil do que nunca para diretores de informação e de segurança de informação garantir e proteger as operações.

Mais complexidade, mais desafios

As organizações estão lidando com circunstâncias extraordinárias. É fácil gerenciar endpoints quando a superfície de ataque não está crescendo ou liderar a transformação digital quando ela não precisa acontecer da noite para o dia.

Então, como você possibilita tecnologias novas e emergentes e facilita a transformação digital nesses tempos desafiadores?

1. Modernize plataformas, abordagens e ambientes legados.
2. Gerencie as exigências regulatórias e de conformidade contínuas.
3. Gerencie melhor as ameaças de segurança e a superfície de ataque crescente.

Não se engane: à medida que nos tornamos mais conectados, as ameaças se tornam mais reais. Com uma área de superfície maior, as ameaças estão se tornando cada vez mais complexas e difíceis de defender. E os bandidos, que são frequentemente patrocinados pelo Estado, estão usando essas mesmas tecnologias emergentes para fazer uma guerra altamente sofisticada contra nós.

Precisamos de uma convergência.

Por que cada organização precisa do XEM

As soluções convergentes unem ferramentas e dados em uma solução unificada. Uma solução convergente é um sistema que permite a convergência: atua como a espinha dorsal para que todas as interações cruciais entre dados, ferramentas e equipes ocorram. Ela está na interseção dos domínios nas Operações de TI, Segurança, Risco e Gestão de Conformidade. As soluções convergentes atraem uma ampla gama de usuários, permitindo que os líderes de TI e funcionários colaborem.

A mudança e o crescimento devem ser gerenciados

As empresas precisam de uma solução que resolva a explosão de endpoints, a proliferação de ferramentas e a modernização de TI de todos os endpoints, fluxos de trabalho e equipes.

Dada a infinidade de mudanças que afetam a TI, é fundamental que as organizações priorizem soluções que forneçam visibilidade em todos os endpoints, controle desses endpoints e confiança na qualidade dos dados gerados. É primordial que as empresas combatam a expansão e a fadiga de ferramentas que servem apenas para aumentar a exposição ao risco de uma empresa e reduzir a produtividade dos funcionários por meio da consolidação de ferramentas. Os silos dentro das organizações podem ser eliminados usando ferramentas comuns que combinam operações de TI, risco e conformidade e segurança em uma plataforma convergente.

Uma plataforma convergente como a descrita deve abranger três coisas:

- Todos os endpoints. A visibilidade em toda a gama de endpoints por meio de um único painel é essencial; seja laptop, desktop, celular, contêiner, ou sensor, todos os tipos de endpoints devem ser conhecidos, gerenciados e protegidos.
- Todo o fluxo de trabalho. O potencial de agir e construir qualquer fluxo de trabalho de que uma empresa precise deve ser habilitado por meio de uma plataforma: cada módulo (sejam operações de TI, segurança ou risco e conformidade) é meramente um fluxo de trabalho que depende dos mesmos recursos subjacentes da plataforma.
- Todas as equipes. O alinhamento entre as equipes em torno de uma única fonte de verdade, os mesmos dados e o mesmo conjunto de ferramentas comuns é uma necessidade básica para quebrar silos.

As plataformas convergentes abordam o enigma “tecnologia, processo e pessoas”

Uma plataforma unificada que permite uma tomada de decisão mais rápida, dados de alta fidelidade e vários recursos em um local substitui processos manuais tediosos. Combinar o alcance das operações de TI, segurança, risco e conformidade em um local permite o que várias soluções de pontos legados não conseguem. As equipes podem se concentrar no que importa, fazendo o trabalho de forma multifuncional, produtiva e segura, fornecendo a resposta mais eficaz a um ambiente onde os invasores estão mais agressivos do que nunca e os clientes exigem mais do que nunca. Então, como você possibilita tecnologias novas e emergentes e facilita a transformação digital nesses tempos desafiadores?

Resultados do XEM

Essa abordagem convergente capacitará os clientes em quatro áreas essenciais:

Visibilidade: Com visibilidade completa, as organizações podem identificar riscos digitalizando o ambiente de endpoints em minutos. Isso é vital quando você pensa no perímetro em constante mudança onde os dispositivos estão indo e vindo, ou quando você está adicionando dispositivos ou sensores de IoT.

Alinhamento: Do ponto de vista do alinhamento, é possível criar uma linguagem comum entre as equipes de operações, segurança e risco, tudo com um conjunto de dados comum.

Capacidade de resposta: Por meio da capacidade de resposta, é possível corrigir vulnerabilidades e abordar a conformidade com um clique, um console, em segundos.

Controle: É possível mover o perímetro das operações, segurança e conformidade para onde a rede realmente começa e termina: a borda.

Caso de uso do XEM: Log4j

Não há melhor caso de uso do XEM (gerenciamento convergente de endpoints) do que a vulnerabilidade mais crítica do setor, o Log4j. Com uma plataforma convergente, os clientes puderam realizar descobertas detalhadas e completas em tempo real, avaliação detalhada, priorização e remediação independente do sistema operacional entre plataformas.

Uma solução de XEM pode encontrar indicadores de vulnerabilidade, detectar sinais de exploração, remediar e fortificar o ambiente e relatar exposições contínuas. Todas essas peças trabalhando juntas diferenciam a plataforma XEM de qualquer outra coisa no mercado.

Definição de recursos

As plataformas convergentes resolvem o problema tecnológico para que as empresas possam se concentrar no problema organizacional.

As soluções técnicas devem transcender a tecnologia. Elas precisam habilitar uma solução de negócios. Ao permitir uma melhor comunicação entre as equipes e fornecer visibilidade dos ativos, controle desses ativos e confiança nos dados que afetam esses ativos, as equipes podem tomar decisões mais rapidamente e de maneira mais informada. Historicamente, a responsabilidade tem sido limitada devido ao isolamento de ferramentas e equipes, mas esse não é mais o caso com o advento das ferramentas convergentes. Já se foram os dias de ferramentas não confiáveis e processos separados que trazem resultados incompletos.

As plataformas convergentes mudam radicalmente a mentalidade ultrapassada de produto

Em vez de serem centradas na ferramenta, as plataformas convergentes são centradas no dispositivo. Em vez de aplicar ferramentas ao endpoint, as plataformas convergentes consideram tudo de que o endpoint precisa e fazem do endpoint o foco. As plataformas convergentes resolvem tudo o que é necessário na jornada ou ciclo de vida de um dispositivo. As equipes de produtos que desenvolvem plataformas convergentes adotarão uma mentalidade geral que descreve roteiros que abordam as diversas necessidades do endpoint, desde o ponto de vista operacional ao de conformidade e de proteção.

As plataformas convergentes unem ferramentas e dados em uma solução unificada

Os vários recursos centrais incluem plataformas convergentes, alojadas em um único painel de controle, que é um painel para ver, controlar e confiar em tudo o que está acontecendo no endpoint. Veja todos os dados recebidos de todos os endpoints em um só lugar:

1. **Gerenciamento de riscos e conformidade:** Monitore alterações de arquivos e registros; cumpra as regulamentações e práticas de privacidade. Verifique a rede em busca de ativos não gerenciados; localize lacunas de conformidade; avalie os computadores em relação aos benchmarks do setor.
2. **Gerenciamento de clientes:** Forneça patches de forma consistente e rápida. Mantenha todos os sistemas em funcionamento e atualizados com patches automatizados e tempo de inatividade mínimo; simplifique, centralize e aplique as configurações essenciais.
3. **Busca de ameaças:** Emita alertas sobre comportamento suspeito e restauração de endpoints de volta ao estado estável. Identifique contas e sistemas de alto risco; encontre e corrija vulnerabilidades em escala; execute remediação automatizada por meio de ações priorizadas nos endpoints.
4. **Descoberta e inventário de ativos:** Faça um inventário completo dos ativos de hardware e software. Identifique todas as máquinas em uma rede, incluindo qual software elas têm e como são usadas.
5. **Monitoramento de dados confidenciais:** Rastreie e gerencie dados confidenciais para que os invasores não o façam. Pesquise rapidamente dados confidenciais e revele a localização deles para agir. Localize alterações não autorizadas de eventos em caminhos de arquivos, escopo para exposição de dados e possível risco e sistemas de arquivos de índice.
6. **Gerenciamento de serviços:** Permita que as equipes de TI ofereçam suporte aos funcionários e resolvam tíquetes de suporte técnico. Crie um fluxo de trabalho simplificado e de suporte técnico usando dados precisos e em tempo real.

As plataformas convergentes atraem uma ampla gama de usuários

Os diretores de informação escolhem plataformas convergentes para garantir que os endpoints sejam corrigidos em relação às vulnerabilidades mais recentes em horas e configurados adequadamente. Os diretores de segurança de informação escolhem plataformas convergentes para servir como a última linha de defesa para responder a violações. As equipes de infraestrutura usam plataformas convergentes para analisar migrações para a nuvem em semanas, em vez de meses ou anos. As equipes de compras usam plataformas convergentes para confirmar que não pagam por mais software do que usam. Os auditores usam plataformas convergentes para avaliar como está a conformidade das empresas com um patchwork de estruturas regulatórias e de conformidade. Os custodiantes de dados usam plataformas convergentes para encontrar e remover dados confidenciais em escala.

Claramente, as plataformas convergentes permitem que líderes e funcionários de TI, em diversas funções, gerenciem e protejam todos os ativos.

Olhar para o futuro

As tendências que moldam o mundo de TI de hoje só continuarão a acelerar

As tendências de trabalho remoto chegaram para ficar. A necessidade de gerenciar e proteger todos os tipos de endpoints (dentro e fora da rede) não está desaparecendo. De acordo com uma pesquisa do Gartner, 48% dos funcionários trabalharão remotamente pelo menos parcialmente após o término da pandemia; uma pesquisa do Pew Research Center revelou que 54% dos funcionários dos EUA preferirão trabalhar remotamente quando a pandemia acabar, e um relatório da Gallup mostrou que 6 em cada 10 gerentes planejam permitir que os funcionários trabalhem remotamente com mais frequência do que antes da pandemia. A partir dessas estatísticas, fica claro que uma força de trabalho distribuída futura significa que as equipes de TI continuarão gerenciando e protegendo endpoints fisicamente fora dos firewalls corporativos. As plataformas convergentes como a Tanium, que geram visibilidade, controle e dados confiáveis para as equipes de TI, continuarão a ser fundamentais em um ambiente de trabalho híbrido.

Em segundo lugar, a migração para a nuvem também continuará a evoluir, expondo dados confidenciais ao risco de serem acessados e usados para fins indesejados. Apenas em 2022, os gastos do usuário final em serviços em nuvem devem aumentar em 22%, de acordo com o Gartner. E a nuvem é popular: O relatório anual State of the Cloud descobriu que 90% das organizações confiarão em alguma forma de solução de nuvem híbrida até o final de 2022. No longo prazo, até 2026, o Gartner prevê que os gastos com nuvem totalizarão pelo menos 45% de todos os gastos com TI empresarial. Assim, as empresas precisarão de soluções como a Tanium, que sejam compatíveis com a nuvem e que permitam operações seguras conforme migrarem de soluções locais.

Em terceiro lugar, a inteligência artificial (IA) e os algoritmos baseados em aprendizado de máquina (ML) se tornarão ainda mais cruciais no mundo dos endpoints. Adaptar políticas e funções de segurança a usuários individuais em tempo real com base no tipo de dispositivo, configuração do dispositivo, padrões de quando e onde tentam fazer login e outras variáveis será fundamental. A Tanium pode permitir que a verdadeira IA/ML notifique os usuários sobre comportamentos suspeitos e automatize a remediação devido à qualidade dos dados aos quais tem acesso e à velocidade com que pode devolver esses dados. As empresas continuarão investindo em soluções como a Tanium, que automatizam, adaptam e aprendem constantemente com as ameaças.

A plataforma de gerenciamento convergente de endpoints da Tanium está pronta para aproveitar essas tendências futuras

Com a Tanium, os clientes têm um conjunto convergente de módulos para tudo o que for necessário para um dispositivo se manter em funcionamento. Ferramentas convergentes em todo o espaço de operações de TI, segurança e risco e conformidade reúnem equipes: uma plataforma para dar visibilidade, controle e confiança na infraestrutura de TI.

A Tanium está construindo conscientemente a plataforma levando em conta o que é necessário para permitir o trabalho das equipes de TI (operações e segurança). Em meio a uma superfície de ataque em constante expansão, os líderes de TI podem ser proativos, invés de reativos, em relação à solução problemas. As equipes são mais capazes de se comunicar entre si, fazendo referência ao mesmo conjunto de dados e ferramentas; nenhum treinamento adicional é necessário entre as equipes; e é simples adicionar mais módulos porque cada um é simplesmente um fluxo de trabalho construído na mesma plataforma subjacente. As equipes precisam gerenciar menos aplicativos e ferramentas, enquanto experimentam um impacto positivo nos resultados de negócios por meio de maior colaboração.

Essencialmente, a Tanium é uma empresa de dados que ajuda a TI a escalar, convergindo o mundo das operações de TI, segurança, risco e conformidade para uma solução unificada. Esse é o poder da certeza.

Referências

https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf

https://venturebeat.com/2021/09/26/digital-transformation-spending-is-up-to-700b-per-year-but-results-lag/

https://federalnewsnetwork.com/federal-insights/2021/04/what-the-pandemic-driven-increase-in-it-complexity-means-for-federal-agencies/

https://www.retaildive.com/news/76-of-cios-say-it-complexity-makes-it-impossible-to-manage-performance/516065/

https://hbr.org/2021/10/does-your-team-really-need-another-digital-tool

https://www.businesswire.com/news/home/20170918005033/en/Information-App-Overload-Hurts-Worker-Productivity-Focus

https://securityboulevard.com/2021/06/proliferation-of-devops-tools-introduces-risk/

https://www.advsyscon.com/blog/break-down-silos-in-it/

https://blog.trello.com/tips-to-improve-cross-team-collaboration

https://www.beezy.net/blog/too-many-tools

https://jfrog.com/devops-tools/what-is-devsecops/

https://www.dynatrace.com/news/blog/top-eight-devsecops-trends/

https://www.maltego.com/blog/tackling-tool-fatigue-soc-teams-need-interoperable-tools/

https://explodingtopics.com/blog/remote-work-trends

https://www.parallels.com/blogs/ras/green-it-cloud-predictions-2022/#:~:text=Gartner%20forecasts%20a%20rapid%20global,enterprise%20IT%20spending%20by%202026

https://workforceinstitute.org/workers-globally-wish-for-better-technology/

https://www.formstack.com/resources/blog-software-interoperability#:~:text=The%20term%20%E2%80%9Csoftware%20interoperability%E2%80%9D%20refers,behind%2Dthe%2Dscenes%20coding

https://www.darkreading.com/edge-articles/security-considerations-in-a-byod-culture

https://site.tanium.com/rs/790-QFJ-925/images/WP-Visibility-Gap-2020.pdf

https://www.globenewswire.com/news-release/2021/05/04/2222642/0/en/GitLab-s-Fifth-Annual-Global-DevSecOps-Survey-Reveals-2020-Was-Catalyst-for-DevOps-Tool-Adoption.html